INTERNATIONAL GUIDE TO EXPORT CONTROLS AND ECONOMIC SANCTIONS

Second Edition

Kay C. Georgi, Paul M. Lalonde, and
Douglas N. Jacobson, Editors

ABA
AMERICANBARASSOCIATION
International Law Section

INTERNATIONAL GUIDE TO

EXPORT CONTROLS AND ECONOMIC SANCTIONS

Second Edition

Kay C. Georgi, Paul M. Lalonde, and
Douglas N. Jacobson, Editors

ABA
AMERICANBARASSOCIATION
International Law Section

Cover design by Amanda Fry/ABA Design

A catalog record for this book is on file with the Library of Congress.

Discounts are available for books ordered in bulk. Special consideration is given to state bars, CLE programs, and other bar-related organizations. Inquire at Book Publishing, ABA Publishing, American Bar Association, 321 N. Clark Street, Chicago, Illinois 60654-7598.

www.ShopABA.org

Dedications

To my wife, Magda, and our children, Claire and Yonas. And to my parents, Claire and Marc Lalonde, who still show me the way.

— Paul M. Lalonde *To the memory of my parents, Jay and Marion Georgi, and to my husband and son, Paolo and Ugo Nascimbeni.*
— Kay C. Georgi

To my wife, Emily Jacobson, for all her amazing support.

— Douglas N. Jacobson

Contents

13 Export Controls and Economic Sanctions in Australia

18 Export Controls and Economic Sanctions in Hong Kong

22 Export Controls and Economic Sanctions in Japan

About the Editors and Authors

Editors

Paul M. Lalonde is the leader of the National Regulatory Practice Group at Dentons Canada LLP. He has over 30 years of experience in international trade law, including import/export controls, international sanctions, anti-dumping and countervail, customs, trade and investment treaty disputes, and international anti-corruption law. Paul has been recognized as a leading practitioner in international trade and procurement law by several directories, including *Lexpert*, *Chambers*, *Legal 500*, *Legal Post*, *World's Leading Lawyers* (Legal Media Group), *Who's Who of Public Procurement Lawyers*, *Who's Who Legal Canada*. He has held numerous leadership positions in the ABA International Law Section, the International Bar Association, and the Canadian Bar Association, and is past chair and president of Transparency International Canada. He is called to the Bars of Québec (1990) and Ontario (1992) and is fluently bilingual in English and French.

Kay C. Georgi has more than 33 years of experience advising clients on all aspects of international trade, with particular capability in the areas of export control and sanctions, Foreign Corrupt Practices Act (FCPA), and import (customs) matters. Ranked as one of the leading "International Trade: Export Controls & Economic Sanctions" lawyers by *Chambers USA* and *Chambers Global*, and as a leading international trade practitioner by *Legal 500* and *Expert Guides*, Kay served two three-year terms as co-chair of the ABA Export Controls & Economic Sanctions Committee.

Kay has been a lead auditor in International Traffic in Arms Regulations (ITAR) audits conducted pursuant to the Directorate of Defense Trade Controls (DDTC) of the U.S. Department of State consent agreement/directed disclosures and served as an expert witness in international arbitrations. She attended Cornell University for her undergraduate and law school studies, earning her BA with distinction in Classics and archeology and her JD summa cum laude with a concentration in international legal affairs. Kay is fluent in Italian.

Douglas N. Jacobson is the founding partner of the Washington, DC-based international trade law firm of Jacobson Burton Kelley PLLC. Doug has over 30 years of experience representing a wide range of U.S. and non-U.S. companies on compliance with U.S. and multilateral regimes governing the export of dual-use items, software, technology, defense articles, and humanitarian products. He also represents companies and individuals in enforcement actions brought by BIS, DDTC, and OFAC. Doug served as the outside auditor in one of the largest criminal and civil export controls and sanctions enforcement cases brought by OFAC and BIS.

Doug is a frequent author, speaker, and commentator on export controls and sanctions matters and is an adjunct professor of sanctions and export control law at American University's Washington College of Law in Washington, DC. Doug is ranked in the *Chambers and Partners' Global and USA* guides as a leading export controls and sanctions attorney. He is also listed in *Who's Who Legal* as a leading international trade attorney. Doug received a BA in government from the University of Texas at Austin and a juris doctorate from American University's Washington College of Law, where he was an editor of the *American University Law Review*. He is a member of the District of Columbia and Maryland Bars and is admitted to practice before the U.S. Court of International Trade and the U.S. Court of Appeals for the Federal Circuit.

Authors

Evan Abrams is an attorney with Steptoe & Johnson LLP where he counsels financial institutions, multinational corporations, and individuals on a variety of international regulatory and compliance matters. He regularly advises clients on issues related to anti-money laundering (AML),

economic sanctions, export controls, foreign anti-corruption, the Committee on Foreign Investment in the United States (CFIUS), and the Defense Counterintelligence and Security Agency (DCSA).

Kala Anandarajah practices in competition (merger control, cartels, etc.), trade (export controls, FTAs, sanctions, etc.), and consumer protection. *Chambers* notes that she is lauded by clients as having "unrivalled knowledge and understanding of the law and [is] uniquely . . . able to understand very complicated businesses and their likely reactions," a "business-focused and client-oriented attorney who balances her expertise with practical experience," with a "solid, can-do attitude . . . [who] is very good at working *out a strategic solution to a legal problem . . . one of the few practitioners who is truly at the cutting edge*." On trade specifically, her practice is the only one in Singapore with a *Chambers* global ranking. She has been involved in advising multinational corporations on trade agreements, including the WTO, RTAs, and FTAs (TPP, AEC, etc.); deals with setting up a business and structuring logistics flows to benefit from RTAs and FTAs; advises extensively on ROOs and COOs; handles export controls involving strategic and controlled goods; advises and assists with voluntary disclosure programs; and deals with product liability and product recalls.

In 2022, Kala was named one of the ten most innovative practitioners in Asia Pacific by *Financial Times*, recognized as one of the most highly regarded in Southeast Asia by *Who's Who Legal* (also in 2021), recognized clients' choice counsel by *Lexology*, and named top 50 employment lawyers in the world. In 2021, she was awarded the Highly Commended Lawyer in Private Practice at the Legal 500 Southeast Asia Awards (one of only two) and the Outstanding Achievement by Women in Business Law Awards Asia. She is also cited as top 100 women competition lawyers in the world by *Global Competition Review*. In 2022, she was awarded the Public Service Star (Bintang Bakti Masyarakat), and, in 2014, she was awarded the Public Service Medal (Pingat Bakti Masyarakat), both of which are conferred by the president of Singapore, for her contributions to public service.

John Boscariol is a partner in the Litigation Group at McCarthy Tétrault LLP and leader of the firm's International Trade and Investment Law

Group. He specializes in investigations, enforcement, disputes, and compliance regarding economic sanctions, anti-corruption law and policy, export, brokering and technology transfer controls, blocking orders (Cuba), government contracts, national security, and other trade and customs measures. He has developed a recognized expertise in advising on the intersection of Canadian economic sanctions, export and technology controls, and anti-corruption measures with those of the United States, the European Union, the United Kingdom, and other jurisdictions. John is ranked by *Who's Who Legal* among a small number of attorneys as a global thought leader in investigations and as a global leader and a national leader in the international sanctions and trade & customs categories. Recently, he was also named by *Expert Guide's Best of the Best (Global)* as one of the world's top 30 international trade attorneys and by *Best Lawyers* as the 2019 and 2021 international trade and finance law "lawyer of the year" in Toronto. *Martindale-Hubbell* rates John as "AV Preeminent," their "highest level of professional excellence" and *Chambers Global* ranks him in Band 1 for WTO/International Trade. He is adjunct faculty at the University of Western Ontario Faculty of Law where he designed and teaches *Anti-Corruption Law and Its Application in International Business*. John has also been active in the leadership of the American Bar Association International Law Section and is past co-chair of the ABA Export Controls and Economic Sanctions Committee. In October 2021, John received the Ontario Bar Association Award of Excellence in International Law.

Tomer Broude is dean of the Faculty of Law at the Hebrew University of Jerusalem, and associate professor and Bessie and Michael Greenblatt, Q.C., Chair in Public and International Law at the Faculty of Law and Department of International Relations. He has formerly served as academic director of the Minerva Center for Human Rights at the Hebrew University of Jerusalem, and vice-dean of the Faculty of Law. He specializes in public international law and international economic law, particularly international trade and investment, human rights, dispute settlement, development, and cultural diversity. He is the author and editor of several books and numerous articles that have appeared in top-ranked publications such as *International Organization*, *University of Pennsylvania Law Review*, *European Journal of International Law*, *Leiden Journal of International Law*, *Vanderbilt Law Review*, *Virginia Journal of International Law*,

International Journal of Cultural Property, *Journal of World Trade*, *World Trade Review*, and the *Journal of International Economic Law*. He is an editor of the *Journal of International Dispute Settlement* and a general editor of the Cambridge University Press book series on International and Economic Law (CITEL). He is one of the founders of the Society of International Economic Law and a former member of its executive council, and currently a member of the executive council of TradeLab, an international network of university pro bono clinics and practica.

Tomer has taught at numerous law schools around the world, such as the University of Toronto, University of Virginia, University of California-Los Angeles, Fordham Law School, Hong Kong University, Melbourne Law School, University of British Columbia, and Gujarat National Law University. He was a distinguished fellow at the Munk School of Global Affairs and Public Policy at the University of Toronto (2020–2022). He has been appointed to the indicative list of governmental and nongovernmental panelists to hear WTO disputes and to the list of Israeli arbitrators under the Israel-MERCOSUR Free Trade Agreement. In 2018, he was appointed by the government of Canada to the roster of NAFTA Chapter 19 (Trade Remedies) Panelists (now USMCA). He is a member of Israel's Trade Remedy Advisory Board.

Raphael Brunner is a partner at MME Legal | Tax | Compliance, a Zürich-based international law firm. He advises and litigates for clients on national and international commercial and contract law. His focus is on international trade, distribution, logistics, shipping, and transport law, including customs law, free trade agreements, and export compliance. Raphael also forays into public procurement law and international insolvency law, and often represents clients with complex internal and external investigations.

Raphael is vice president of the Swiss Association for the Law of the Sea, a regular speaker at international conferences, and a lecturer at the Lucerne University of Applied Sciences and Arts and the Swissmem Academy. He also regularly publishes on topics in his field. Raphael leads MME's trade practice covering export compliance and sanctions. The team advises equally the exporting and importing industry and trading industry as well as logistic service providers and insurers.

Ali Burney is a partner at Steptoe & Johnson LLP based in Hong Kong SAR. His practice focuses on representing U.S. and non-U.S. clients in the Asia-Pacific region on matters related to U.S. economic sanctions, export controls, the U.S. Foreign Corrupt Practices Act (FCPA), and anti-money laundering (AML) laws. Ali has extensive experience representing clients in front of the U.S. Department of Justice, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), and the U.S. Department of Commerce's Bureau of Industry and Security (BIS). His experience includes conducting cross-border investigations, filing voluntary self-disclosures, responding to subpoenas, obtaining OFAC licenses, conducting risk assessments, and representing individuals and companies seeking removal from OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) and the BIS Entity List. He also frequently advises companies investing in high-risk sectors and countries on sanctions, anti-bribery and corruption, and export control–related pre-acquisition due diligence and post-acquisition compliance program implementation.

Michael L. Burton is a partner at Jacobson Burton Kelley PLLC and former co-chair of the ABA's Committee on Export Controls and Economic Sanctions and AAEI's Committee on Export Compliance and Facilitation. He has 25 years of experience representing U.S. and foreign clients on a wide range of issues related to compliance with and enforcement of U.S. export controls (Export Administration Regulations and International Traffic in Arms Regulations), economic sanctions administered by the Office of Foreign Assets Control (OFAC), anti-boycott, the Foreign Corrupt Practices Act, anti-money laundering, CFIUS/FIRRMA, and import laws. He counsels clients on complex trade controls issues, designs and audits corporate compliance programs, and has obtained numerous U.S. government licenses authorizing transactions under these controls. Michael is ranked in the *Chambers and Partners' Global and USA* guides as a leading export controls and sanctions attorney. Michael graduated, magna cum laude, from Brown University and Georgetown University Law Center.

Alexander Bychkov is a partner at Melling, Voitishkin & Partners. He heads the International Trade, Customs and Sanctions Practice Group and actively participates in the Tax Practice Group, and the Compliance and Investigations Practice Group. He is also a member of the Healthcare &

Life Sciences Practice Group. Alexander focuses his practice on advising clients on the broad array of international trade and compliance matters, as well as indirect tax and general commercial matters, with a particular emphasis on Russian distribution structuring, customs regulatory matters, product valuation and classification, VAT, U.S./UK/EU/Swiss and Russian trade compliance, import and export control requirements and sanctions, WTO and anti-dumping issues, internal investigations and dispute resolution in the spheres of trade compliance, customs, anti-bribery, and corruption (including representation of clients in related administrative and criminal investigations).

Since 2006, Alexander has been consistently recognized as one of the leading professionals in the tax field within Russia and across the CIS. His practice is recognized by *Chambers and International Tax Review*. He was also mentioned in 2018, 2019, and 2020 in *World ECR* as one of the leading trade compliance experts.

Simone Cadeddu is a partner at Bird & Bird, leading the Italian Regulatory & Administrative Practice, with a strong focus on export controls, sanctions, foreign direct investment, and military procurement. An LLM graduate of Georgetown University Law Center, Simone obtained his JD from Sapienza Università di Roma, where he also earned a PhD in public administration.

Jessica Cai is a partner at JunHe LLP and focuses on trade compliance, customs investigation, and trade remedies. Jessica has substantial experience in assisting Chinese clients in handling issues related to U.S., EU, and Chinese sanctions and export controls. She also has extensive experience in trade remedy cases, helping clients deal with anti-dumping and countervailing and anti-circumvention investigations in China, the United States, the EU, Canada, Australia, and other countries, involving various industries such as solar cells, steel, chemical, and textiles. Besides providing guidance in handling and responding to customs affairs and assistance in preparing documents related to sales, production, and accounting for Chinese enterprises, Jessica provides advice on long-term strategic plans, establishing strategic response mechanisms, and reshaping business structures.

Kuok Yew Chen is a corporate M&A lawyer with a specialization in regulatory and trade law and technology, media, and telecommunications law at Christopher & Lee Ong. He regularly advises on cross-border transactions, mergers and acquisitions, telecommunications projects, trade, and general corporate and regulatory matters. His expertise in the corporate space extends to advising private equity funds, multinationals, and public and private companies on these areas of law, and he is familiar with the various regulatory authorities for competition, telecommunications, and trade.

Yew Chen was recently featured on The Asia Pacific Legal 500 TMT Hall of Fame, which highlights individuals who are at the pinnacle of their profession and have received constant praise from their clients for continued excellence. He is also recognized as a Distinguished Practitioner for Corporate M&A by *Asialaw Profiles* and is ranked as a Tier 1 Corporate M&A Lawyer by *Asia Pacific Legal 500*.

Michael Cheung is a Hong Kong practicing lawyer at Melinda Lee & Co. in association with Sam Zhang & Co. The firm has years of experience in the area of international trade and export controls. His practice also covers corporate and commercial law, mergers and acquisitions, and foreign direct investment in the People's Republic of China. He is a China-appointed attesting officer, appointed by the PRC Ministry of Justice.

Maura Décosterd is a trade policy consultant with government, private sector, and academic expertise covering Europe, SE Asia, and Africa. Her current work with the Zürich-based firm MME focuses on export controls and sanctions compliance. She publishes, lectures, and speaks on trade policy and economic integration. She currently advises clients on regulatory compliance, and designs policies and strategies to facilitate the observance of Swiss and EU regulations in the field.

Ashok Dhingra is founder and senior partner of Ashok Dhingra Associates and leads the White-Collar Crimes, Investigations and Regulatory Laws Group in the firm. Ashok has more than 46 years of three-dimensional experience working with Indian Customs, including DRI, Big 4 consulting firms, and law firms. He assists clients in conducting audit and investigations under the Foreign Corrupt Practices Act, UK Bribery Act,

and Indian Prevention of Corruption Act, investigations of wrongdoing or fraud or ethical violations by management or employees of multinational companies. Ashok also assists clients in options to deal with noncompliance and making self-disclosure to the authorities.

Ashok has assisted clients in investigation and adjudication under the Prevention of Money Laundering Act and Black Money (Undisclosed Foreign Income and Assets) and the Imposition of Tax Act. He regularly advises clients during raids or investigations by tax, trade, and regulatory authorities like DRI, ED, and SFIO. Ashok advises clients on key issues under the Foreign Exchange Management Act and assists in compounding of offences by Reserve Bank of India. Ashok also advises clients on issues under the Information Technology Act, data security, data privacy, data retention, encryption and movement of data across jurisdiction, and regulatory laws. Ashok regularly appears before departmental adjudication and appellate authorities, Tax Tribunal, High Court, and Supreme Court as an arguing counsel in tax, customs, and trade matters. Ashok is fluent in English, Hindi, and Punjabi.

Anthony Eskander is a London-based barrister specializing in financial crime, export controls and sanctions, regulatory law, and commercial litigation. He advises domestic and international clients, including solicitors and corporate clients, on a broad range of issues, including criminal liability, forfeiture and confiscation, bribery and corruption issues, and sanctions. He provides representation for clients in courts, including the Court of Appeal, and is on the panels of both the Crown Prosecution Service and the Serious Fraud Office. Prior to practicing as a barrister, Anthony was in the financial crime team at KPMG, advising KPMG and the firm on his area of expertise. Anthony was also an analyst in the Operations Division at Goldman Sachs. His responsibilities included ensuring the investment bank’s compliance with domestic and international financial regulations. During his time at Goldman Sachs he gained expertise in the fields of international fraud, bribery, money laundering, and counterterrorism financing laws. Anthony is frequently asked to write articles for newspapers and magazines, and is frequently quoted in the media.

Diego Fissore is an attorney with G. Breuer. His practice areas are general corporate and commercial law and trade law, and he has extensively advised clients in these areas at national and international levels. Diego graduated from the University of Buenos Aires with honors in 1987, then earned an LLM at Harvard Law School in 1995. He is admitted to the bars of Buenos Aires, Argentina, and New York, USA. Diego has been adjunct professor of civil law at the University of Buenos Aires, School of Law, since 2004, and adjunct professor of civil law at the Universidad Argentina de la Empresa (UADE, Buenos Aires) since 2003. He is also a postgraduate professor at UADE and teaches "Business Law in Latin America," in English, in which trade law is a major part of the syllabus.

William E. Fork is a partner at Pillsbury Winthrop Shaw Pittman LLP, where he is an internationally recognized advisor to multinational companies and governments involved in nuclear development projects. Areas of advice include nuclear vendor procurement structures and agreements for the construction, operation, and fueling of nuclear power units. Among other representations, he has served as the general counsel of the implementing company of a civil nuclear power program during its development phase. He has served as an international nuclear law instructor for the International Atomic Energy Agency (IAEA) and OECD Nuclear Energy Agency (NEA). He also serves as a member of the board of directors of the International Nuclear Law Association (INLA), the association for the international nuclear law bar.

Peter Gjortler has been an Of Counsel at Grayston & Company since its creation in 2007. He is a Danish qualified lawyer who has practiced EU law for more than 30 years in private practice, public administration, judicial service, and universities. His professional experience includes time spent at the Danish Ministry of Justice and High Court of Appeal; as a legal advisor to the Danish government; and at the European Court of Justice, the University of Copenhagen, and Riga Graduate School of Law.

Geoffrey M. Goodale is a partner in the Government Contracts and International Trade Practice Group of Duane Morris LLP. For over 20 years, he has assisted U.S. and non-U.S. companies of all sizes in numerous industries develop and implement strategies to accomplish their

international business goals. His practice focuses on export controls, economic sanctions, import compliance, trade litigation, international intellectual property rights protection, foreign direct investment, cybersecurity, and compliance counseling to government contractors.

Geoffrey has served as co-chair of the ABA International Law Section's Export Controls and Economic Sanctions Committee, Customs Law Committee, International Trade Committee, and National Security Committee. In addition, he has been co-chair of the D.C. Bar's International Law Section and chair of the Virginia State Bar's International Practice Section, and he has served as a member of the Advisory Committee on Rules of the U.S. Court of International Trade. He received his BA in government with honors from the College of William and Mary and his juris doctorate from the George Washington University Law School, where he was notes editor of the *AIPLA Quarterly Journal*.

John Grayston is a Belgian avocat and an English qualified solicitor. He has been based and practiced EU law in Brussels for more than 20 years. John has specialized in advising clients on EU trade and customs laws, including both export control and sanctions issues. In 2007, he and colleagues founded the law firm Grayston & Company (www.graystoncompany.com).

Sonia Gupta is founder and managing partner of Ashok Dhingra Associates and leads the Customs and Trade Group. Sonia is a chartered accountant and attorney with over 20 years of experience of assisting clients in customs and trade laws, export controls, sanctions, foreign trade policy, regulatory laws, and money laundering laws, providing both advisory and litigation services. Sonia advises clients on varied issues under export control laws and sanctions, assisting clients in drafting internal compliance programs, training of employees, audit of internal processes, issues arising out of inadvertent export of restricted goods, software and technologies, and investigations by regulatory authorities to close the matter causing least disruption to business. Sonia also advises clients on classification and rate of duty under customs tariff; applicability of exemption notification; country of origin rules; availability of drawback on export or re-export of goods and services; investigation by Special Valuation Branch of Customs to determine arm's length price in case of transaction with associated

enterprises; and trade remedial measures such as investigations for levy of anti-dumping duty, safeguard duty, and countervailing duty. Sonia assists clients on options to deal with noncompliance and making self-disclosure to the authorities; and during raid and investigations by tax and regulatory authorities like Directorate of Revenue Intelligence (DRI), Enforcement Directorate (ED), and Serious Fraud Investigation Office (SFIO).

Sonia regularly appears before departmental adjudication and appellate authorities, Tax Tribunal, High Court, and Supreme Court as an arguing counsel in tax, customs, and trade matters. Sonia is fluent in English, Hindi, and Gujarati.

Martha Harrison is a partner at McCarthy Tetrault LLP in the International Trade and Investment Group. She is a specialist in international trade law, including trade remedies and controls, import/export controls and related programs, customs and trade agreement compliance, economic sanctions, cross-border goods regulatory regimes, and product distribution laws. She also advises on government relations and procurement, and international investor-state arbitration. She is recognized as an expert in her field by a variety of legal organizations and publications, including *Chambers Global*, *Chambers Canada*, *The Legal 500*, *Canadian Legal Lexpert Directory*, *Who's Who Legal*, *Best Lawyers in Canada*, and *Expert Guides*.

Andrew Hudson is a partner at Rigby Cooke Lawyers and leads the Customs Trade Practice with significant expertise across international trade law and customs. Andrew is a trusted, highly regarded advisor to businesses, industry associations, peak bodies, and government, and regularly consults on legal and trade developments that affect Australian and international businesses. Andrew specializes in all areas of trade, including international trade conventions, dispute resolution and arbitration, trade financing options, commodity and freight contracts. He represents his clients' best interests during inquiries or prosecutions by government agencies, in matters involving dumping and alleged underpayments of customs duty, breaches of license conditions by service providers, biosecurity, and defense control issues along with any associated litigation.

Andrew is a member of the board of directors of the Export Council of Australia (ECA) and the executive committee of the Food and Beverage

Importers of Australia (FBIA), and in these capacities is regularly involved to engage with the government agencies and peak industry bodies operating across Australian borders. He is also chairperson of the Private Sector Group NCTF, established by the ABF to implement the WTO Trade Facilitation Agreement, and a member of the Department of Foreign Affairs and Trade Rules of Origin Consultative Group.

Dainia Jabaji, associate in Winston & Strawn's International Trade Practice, investigates and provides counsel in complex cases involving OFAC-administered sanctions, the BSA, and other AML laws and regulations. She works with both U.S. and international clients, providing sanctions, AML, and other financial crimes compliance guidance at all stages, from proactive counseling to compliance assessments, to internal reviews, audits, investigations, remediation, and disclosures. Prior to joining Winston, Dainia worked at one of the world's largest financial institutions as a BSA/AML regulatory analyst, and then as a vice president of U.S. Economic Sanctions Investigations. There, she researched, identified, and analyzed BSA and AML matters pertaining to large, globally operating corporate customers and financial institution clients. Dainia has also investigated multi-jurisdictional sanctions cases, recommended and implemented appropriate remediation, and drafted regulatory disclosures.

Peter Jeydel is Of Counsel with Steptoe & Johnson LLP, where his practice focuses on U.S. export controls and sanctions compliance counseling, along with transactional advice, licensing and opinions, jurisdiction and classification assessments, disclosures, and enforcement actions. He has experience in a variety of other international regulatory compliance areas as well, such as anti-corruption and foreign investment national security reviews. His previous experience was with the Office of the Secretary of Defense for Policy (OSD-P).

Vera Kanas is head of TozziniFreire's International Trade Practice Group. She has more than 15 years of experience in the area, assisting Brazilian and foreign companies in a number of issues related to trade remedies, customs law, and trade compliance. She also represents clients in relevant aspects of structuring import and export operations and their supply chain, as well as in issues related to the rules and procedures of the World Trade

Organization and other international agreements. Vera holds a master's degree in international economic law from the Université de Paris-I Panthéon-Sorbonne, France (2002), and PhD in international law from USP (Universidade de São Paulo) (2004). Vera is a WTO Panelist (DS 578, July 2021).

Glen Kelley is a partner in the New York office of Jacobson Burton Kelley PLLC. Glen advises U.S. and non-U.S. companies and financial institutions on economic sanctions, export controls, anti-bribery and anti-money laundering laws, and U.S. foreign investment laws. He served as an attorney-advisor at the U.S. Department of State. Glen represents clients across a broad range of business sectors in transactional and compliance matters, and licensing and negotiations with U.S. government agencies.

Jiatong Li is an associate in the trade compliance team at JunHe LLP. She is particularly very experienced in transaction tracing and data reconciliation, supply chain mapping, and forced labor compliance. Jiatong also helps clients on a number of high profile anti-dumping and countervailing investigations, and circumvention investigations, in various industries.

Zixuan Li is an associate in the trade compliance team at JunHe LLP. She has assisted in conducting thorough due diligence and research, KYC screening, product classification, as well as risk assessment and compliance programs and practical guidelines and training for many clients in different sectors. Zixuan also has assisted in customs investigations and defending clients in criminal smuggling cases.

Greta Lichtenbaum is a partner in the Washington, DC office of O'Melveny & Myers LLP, specializing in compliance with U.S. laws that govern international business transactions and trade, including U.S. economic sanctions, export controls, anticorruption, foreign investment, money laundering, anti-boycott, and customs laws. In addition to advising clients on the application of these laws, Greta assists in all aspects of managing compliance with these laws, including developing corporate compliance programs, conducting internal investigations relating to potential violations of these laws, and representing companies before the

relevant agencies in connection with enforcement proceedings, clearances, license requests, and government inquiries.

Greta has repeatedly been recognized as a leading lawyer in the area of export controls and economic sanctions by *Chambers USA* (Band 1), *Chambers Global* (Band 1), and *The Legal 500 US*. She is a frequent speaker on topics related to international trade and has written extensively on these topics as well. Greta is a longtime leader of the Washington, DC trade controls bar, having served for many years as the leader of the "OFAC Practitioners Group"—a group of private lawyers who interact with OFAC, the State Department, and other key policy makers on the frequently evolving area of economic sanctions law and policy.

Roy Liu was an associate in the trade compliance team at JunHe LLP and is now with a global law firm. She is experienced in trade compliance and customs matters.

J. Scott Maberry is a partner in the Washington, DC office of Sheppard Mullin Richter & Hampton LLP. He specializes in export controls, economic sanctions, customs, and anti-bribery. He advises U.S. and multinational companies and their directors, officers, and boards in transaction due diligence, compliance counseling, licensing, internal investigations, company-to-government advocacy, and white collar criminal defense.

Daniel Martin is the head of HFW's Global Regulatory Group, as well as the Sanctions and Export Control Practice. Daniel advises traders, shipowners, freight forwarders, insurers, and brokers on a host of regulatory and compliance issues, including international trade sanctions, export controls, customs, and anticorruption legislation. He advises on all aspects of the EU and UK sanctions legislation, and he is also familiar with the application of US. sanctions to non-U.S. persons. He provides detailed, practical advice that is tailored to clients in the commodities, shipping, logistics, and marine insurance sectors. In addition to advice on regulatory compliance (including ways to engage effectively with OFSI and other regulators), Daniel advises on compliance procedures and controls that traders, shipowners, logistics companies, banks, insurers, and brokers should adopt to minimize risk. *Acritas Star Lawyers* describes Daniel as

“down to earth, commercially minded, understands my business and thinking outside the box.”

Thaddeus R. McBride is the head of the International Trade Practice at Bass Berry & Sims. Thad advises U.S. and non-U.S. companies and individuals on compliance matters and investigations involving export and import controls, economic sanctions, the Foreign Corrupt Practices Act, matters in front of the Committee on Foreign Investment in the United States, and other trade regulations and laws. Thad is based in Washington, DC.

Oksana Migitko is an associate in the International Trade & Investment Law Group at McCarthy Tétrault LLP. She maintains a general trade practice that includes advice across a wide range of export controls, customs, anticorruption, sanctions, regulatory, and compliance matters. Prior to joining McCarthy Tétrault LLP, Oksana practiced law in Russia for more than ten years.

Fumiko Oikawa is a partner at Atsumi & Sakai and the vice manager of the firm’s International Trade team. She has practiced law for 19 years and has extensive experience in cross-border transactions ranging from banking and finance to international trade. She has advised and represented both government and private sector companies on EPA matters, anti-dumping cases, and regulatory compliance matters including economic sanctions, export controls, and customs. She has been featured by *Best Lawyers* in the practice area of trade law in 2020, 2021, 2022, and 2023.

Turenna Ramirez Ortiz is the managing partner for Sánchez Devanny’s Mexico City office and joined Sánchez Devanny to head the firm’s International Trade and Customs Group. She has more than 20 years of experience advising multinational companies on cross-border transactions related to international trade and customs, ranging from strategic planning, preventive and reactive audits by the Mexican IRS, to defense and litigation before the government and the federal courts. Turenna has a diverse client base, including automotive, retail, chemical, petrochemical, luxury goods, pharmaceuticals, software, cosmetics, electronics, maquiladoras (IMMEX), and trading companies. Turenna advises on foreign trade, multilateral treaties, and anti-dumping laws. Her experience includes the design and

implementation of business strategies, NAFTA origin verifications and tariff classification, rules of origin, export controls, import/export regimes, bonded facilities structure and management, and wide knowledge of tariff and non-tariff regulatory issues. She has participated in complex, high-visibility matters and in international trade negotiations with the secretary general of the World Customs Organization in a program against forgery and piracy.

Anthony Pan is Of Counsel, Integrity Compliance Specialist at the Integrity Compliance Office of the World Bank Group's Integrity Vice Presidency (INT). Anthony is a former associate at Steptoe & Johnson, where he advised clients on U.S. economic sanctions, export control, and anti-bribery and corruption laws and regulations. Anthony has experience in government and internal investigations for multinational corporations and state-owned enterprises, and he has trained in and provided compliance advice to clients in the telecommunications, financial services, commodities, aviation, and logistics sectors.

Andrew Park is a partner in the Seoul, Korea, office of Dentons. Having practiced law for more than 30 years in the United States and Korea, Andrew is uniquely positioned to counsel clients on today's national and cross-border transactions. He blends his knowledge in the laws of both jurisdictions and his deep business networks to successfully advise clients and to close deals. Andrew's practice is multidisciplinary and includes a focus on international commercial transactions such as acquisitions and joint ventures, international trade, antitrust, anti-dumping, labor, and intellectual property. His clients cut across a number of business sectors, including automobile, chemical, electronics, and fashion. Andrew served as chair of the Intellectual Property Rights Committee of the American Chamber of Commerce. In this role, he advised officials from the U.S. Department of State, the Office of the U.S. Trade Representative, the U.S. Embassy in Korea, and other public officials and multinational companies. Mr. Park is also an active panel member of the World Intellectual Property Organization (WIPO) and served on both the INTA's Internet Committee and the Domain Disputes Committee.

Jeffrey Rashba is a partner specializing in corporate law and international transactions in the Israeli firm of S. Friedman, Abramson & Co. Law Offices (Tel Aviv, Haifa, and Jerusalem). Jeffrey's professional mission is to help his clients, and their counterparties, navigate the legal, regulatory, and business ecosystems in which they operate in order to achieve their objectives, and that most often involves close interaction with Israeli clients venturing out globally, and with international clients active in the Israeli market. Though his practice is primarily transaction-driven, Jeffrey has developed a subspecialty in international trade, and he and his colleagues have represented some of the world's largest technology companies with their Israeli trade, customs law, and dual-use technology issues. Jeffrey has taught law courses for the Israeli Bar Association, and has lectured globally on international corporate law issues (U.S., Germany, Japan). Jeffrey has degrees in history (Columbia University), Islamic studies (University of Chicago), and law (University of Connecticut).

Meredith Rathbone is a partner with the law firm of Steptoe & Johnson LLP where she heads the International Trade and Regulatory Compliance Group and co-chairs the firm's Export Controls and Economic Sanctions Practice. She counsels clients on compliance with U.S. export controls and economic sanctions laws, United Nations sanctions and arms embargoes, and the U.S. government's regime targeting forced labor. Her experience includes assisting clients in resolving politically sensitive matters under the joint administration of various government agencies. Meredith is experienced in supporting clients with internal investigations, voluntary disclosures and subpoena responses, export and technology transfer authorizations, and undertaking product classification and jurisdiction assessments, and establishing compliance programs. She is recognized as a leading export controls and sanctions lawyer by *Chambers USA* and *Chambers Global*. She earned her undergraduate degree in international relations from the Georgetown University School of Foreign Service, and her law degree from Georgetown University Law Center, and has been an adjunct professor teaching international law courses at both institutions. She has also served on the U.S. Department of State's Advisory Committee on International Economic Policy, Sanctions Subcommittee.

Danielle Regev is a judicial law clerk at the Israeli Supreme Court, working for the honorable Justice Daphne Barak-Erez. Danielle is an LLM student at the Hebrew University of Jerusalem, specializing in public and international law. She received her LLB and BA in international relations, also from the Hebrew University of Jerusalem.

Bärbel Sachs heads the International Trade and Investment Controls and the Regulatory and Governmental Affairs Practice Groups at Noerr. She has been advising clients in all areas of German, European, and international trade law, including export controls, sanctions, and customs law, since 2006. Bärbel's practice focuses on advice concerning trade compliance programs and investigations of complex matters in the past. She also advises on foreign investment reviews by the German Federal Ministry for Economic Affairs and Climate Action.

Mark E. Sagrans is trade and compliance counsel with DuPont de Nemours. Mark has over 20 years of experience in export controls. Most of those have been in the private sector, though he has also worked at the Office of Export Enforcement in DDTC at the Department of State and in the Chemical and Biological Controls Division in BIS at the Department of Commerce. In addition to working in export controls, he also worked as a lobbyist in Washington, DC for alternative fuels and aerospace interests.

Anca Sattler is senior associate general counsel at Global Payments, Inc., a global financial technology company based in Atlanta, GA, where she is leading the privacy and data protection compliance programs, primarily for Europe and Canada. Prior to joining Global Payments, Anca was counsel for Dentons Canada, practicing in international trade and investment law, as well as privacy. In her trade practice, Anca represented large multinational companies in a variety of trade-related matters, guiding her clients through a wide range of critical issues, including customs, import and export controls, safeguard measures, anti-dumping and countervailing measures, procurement, international sanctions, and the controlled goods program. Anca advised both private parties and governments in international and domestic trade law and represented her clients in matters before the Canadian International Trade Tribunal and the Federal Court of Canada. Anca earned her JD, cum laude, from the University of Ottawa, where she

specialized in international law. Currently, Anca is pursuing an advanced master's degree in privacy, cybersecurity, and data management with Maastricht University.

Hena Schommer is the Global Trade counsel at Hewlett Packard Enterprise (HPE). As Global Trade counsel she is responsible for advising HPE on compliance with global trade controls, including export controls, sanctions, and other trade controls. Hena serves as the global internal legal advisor to the HPE Global Trade Organization, HPE business units, and other stakeholders at HPE, working to develop and implement compliance solutions, manage global trade-related investigations, and advise on licensing issues and customs requirements. Hena works on global trade legal issues in the United States, European Union, Singapore, Russia, and other jurisdictions in which HPE operates. Hena has spent over a decade working on U.S. export controls, sanctions, customs, and other trade controls issues. Prior to HPE, Hena was Of Counsel with Steptoe's International Trade & Regulatory Compliance Practice Group.

Cari N. Stinebower, chair of Winston & Strawn's International Trade Practice, counsels clients on compliance with U.S. economic sanctions, Bank Secrecy Act and AML laws and regulations, export, controls, and anticorruption/anti-bribery laws and regulations. She works with financial institutions and multinational corporations to develop compliance programs, conduct AML and OFAC risk assessments, conduct internal investigations, respond to government investigations, and address potential conflicts of law arising from non-U.S. data privacy and "blocking" laws and regulations. She served as counsel and as a programs officer for OFAC, where she advised on sanctions and anti-terrorism legislation, and drafted United Nations Security Council Resolutions and related executive orders, as well as agency counsel in Treasury's defense of a number of challenges to OFAC's authority, whether in litigation related to enforcement actions or in response to congressional investigations.

David Tang is a partner at JunHe LLP and has over 20 years of experience in international trade. David has deep understanding and extensive expertise in global economic sanctions and export controls. He advises many multinational clients on Chinese sanctions and export controls and helps

numerous Chinese companies in matters related to global sanctions and export controls, such as risk assessment, compliance program, on-site verification, internal and external audit and investigation, delisting and contingency planning. David has years of a track record in representing clients in high-profile inbound and outbound anti-dumping and countervailing cases. He is also experienced in various customs issues, from daily advisory work to audits, compliance work, and smuggling investigations. Clients often seek out David's unique investigative and auditing expertise in finding facts for the purposes of internal investigations and government investigations, and his strategic and artful thinking in navigating difficult conflicts and sensitive issues.

Elina Teplinsky is a partner and deputy leader of the Energy Industry Group at Pillsbury Winthrop Shaw Pittman LLP. She is also a leading member of the firm's International Nuclear Projects and Hydrogen teams. Elina is a trusted advisor to nuclear owner-operators, reactor and equipment suppliers, investors, architect-engineering companies, and technical consulting firms on complex nuclear transactional and regulatory matters. She has worked on transactions in more than 30 countries and serves as lead outside counsel on new build projects, equipment and fuel procurements, M&A transactions, and joint ventures in the nuclear sector.

Elina has vast experience in nuclear export control matters and is currently advising dozens of U.S. and global companies on all aspects of compliance with nuclear export control regimes across multiple jurisdictions, including U.S. Department of Energy regulations and the U.S. Department of Commerce Export Administration Regulations. Her work includes structuring and implementation of export compliance programs and addressing potential violations and securing licenses and advisory opinions.

Elina has been ranked as a leading nuclear energy practitioner by *Chambers Global* and *Chambers USA*. She is co-chair of the World Nuclear Association's Law Working Group and is a frequent lecturer at the World Nuclear University. She has been recognized as an expert nuclear advisor by the International Atomic Energy Association (IAEA), International Framework for Nuclear Energy Cooperation (IFNEC), and Nuclear Energy Institute (NEI). Elina is also a consultant to the Clean Air Task Force, a leading NGO focused on deep decarbonization, on nuclear energy strategy,

and global nuclear deployment. In addition, she serves as a member of the MIT-based Advanced Nuclear & Production Experts Group (ANPEG), a global consortium dedicated to developing low-carbon energy systems based on a “plug-and-play” nuclear microreactor.

Anahita Thoms heads Baker McKenzie’s International Trade Practice in Germany and is a member of the EMEA Steering Committee for Compliance & Investigations. Anahita is global lead sustainability partner for the Industrials, Manufacturing, and Transportation Industry Group. She served for three consecutive terms as co-chair of the Export Controls and Economic Sanctions Committee of the ABA and is an advisory board member of the Sustainable Finance Council of the German federal government. Anahita has won various accolades for her work, including 100 Most Influential Women in German Business (manager magazine).

Nicholas Turner is the managing associate general counsel in the Financial Crime Legal Advisory—Global Legal Function for HSBC. Prior to the publication of this book, Nick was Of Counsel in Steptoe’s Hong Kong office. He has worked with multinational financial institutions and corporations in the United States, the EU, China, Australia, and other jurisdictions on all aspects of economic sanctions, anti-money laundering, and anti-bribery and corruption compliance and investigations. Prior to joining Steptoe, Nick served as a regional sanctions compliance officer, seated in Hong Kong, for a U.S.-based multinational financial institution, after completing the bank’s two-year compliance management associate program in New York and California. In April 2020, *Global Investigations Review* named Nick on its list of “40 Under 40” investigations specialists.

Melisa Uremovic is the deputy managing partner of R&T Asia (Thailand) Limited, the Bangkok office of Rajah & Tann Asia. Melisa has more than 22 years of experience in Thailand and has a particular expertise in customs and trade matters, being one of only a small number of attorneys recognized in *The International Who’s Who of Business Lawyers—Trade & Customs* for Thailand. *Chambers and Partners*, in its 2022 Spotlight table, noted that Melisa “demonstrates a strong South-East Asia-focused trade practice from her base in Thailand. Her recent work spans anti-dumping and customs issues as well as WTO proceedings.” In addition, Melisa represents

multinational clients in a wide range of corporate and commercial work, as well as in complex regulatory matters involving competition, foreign investment, anticorruption, and technology, media, and telecoms laws.

Siyu Wang (Rain) is an associate in the trade compliance team at JunHe LLP. She specializes in the areas of sanctions and export control. She is very experienced in conducting due diligence and risk assessments, developing trade compliance programs for clients of different sizes and in a wide range of sectors, as well as developing contingency plans. Siyu has in-depth knowledge and experience in advising clients in the ICT industry and financial institutions.

Tracy Wong is a partner in the Corporate Practice Group in Christopher & Lee Ong, and spearheads the regulatory and trade practice. Tracy regularly advises multinational entities and foreign law firms on the regulatory requirements covering sanctions, WTOs, export controls, anti-dumping and safeguards, free trade agreements, rules of origin, amongst others. She also advises on corporate transactions, specifically in relation to mergers & acquisitions with a specialty in private equity transactions, and is also involved in general corporate and commercial transactions where she advises corporations on various matters ranging from the incorporation of a company to the regulatory aspects involved in the operations of a company. Tracy is listed as Who's Who Legal's Recommended National Leader for Southeast Asia Trade & Customs 2022.

Wendy Wysong leads the Hong Kong office for Steptoe & Johnson, focusing on regulatory compliance and white-collar defense of international laws, including the ITAR, EAR, OFAC sanctions laws and regulations and U.S. anti-boycott laws, as well as the FCPA. She is also the co-practice group leader for the Global Investigations and White Collar Practice. As a former assistant U.S. attorney in Washington and the deputy assistant secretary for export enforcement in the Department of Commerce's Bureau of Industry & Security (BIS), Wendy offers clients a unique combination of experience and insight as both a prosecutor and regulator before courts and agencies. Ranked as a Band 1 practitioner by *Chambers* in its Asia Pacific and Global guides, clients report that Wendy is "at the top of her game technically" and "brilliant at bringing to bear a global picture of how

regulators react." One insider noted that "she is the most experienced white-collar export lawyer that I know." Additionally, *Global Investigations Review* named her as one of 25 sanctions lawyers to have on speed dial. Her notable experience includes leading an international team that represented a Chinese telecommunications company charged with violating U.S. export controls and sanctions and securing the first ever "Temporary General License" enabling the company to stay in business during the multi-agency investigation. Wendy received her law degree from the University of Virginia School of Law, where she was a member of the University of Virginia Law Review.

Benson Yan is a member of the C.H.L.Y. and Partners, a law firm based in Taipei City, Taiwan. He received his LLB degree from the National Taiwan University School of Law in 1987 and his LLM (with distinction) from Tulane University Law School (New Orleans, USA) in 1994. He passed the New York Bar exam and was admitted to practice in the state of New York in 1995. He specializes in corporate and commercial work, in particular in the areas of joint ventures, foreign direct investments, corporate finance, mergers and acquisitions, international trade, and regulatory affairs.

Marco Zinzani is a member of the Bar of Milan, Italy. He joined Studio Legale Padovan in 2011 and he is the co-head of the firm's Trade Compliance Team. His practice focuses on international trade, export control, and international economic sanctions. Marco holds a law degree cum laude (2005) from Tor Vergata University of Rome and received an advanced master's degree in comparative, European, and international law (2007) and a PhD in European law (2012), both from Maastricht University (the Netherlands), where he subsequently taught EU law. Marco regularly speaks at professional and academic conferences and seminars on export control and international economic sanctions.

Acknowledgments

The idea for the first edition of this Handbook, which was originally published in 2013, originated at a breakfast meeting of the ABA International Law Section Export Controls and Economic Sanctions Committee during the Section's Spring Meeting in 2011.

Because of the significant changes to and expansion of export controls and sanctions during the past decade in the United States and globally, when deciding to move forward with the second edition, the editors felt it was important to expand the reach to as many countries as possible. This turned into a much larger task than we could have imagined, leading to a final version that is more than three times the size of the first edition, and covering export controls and sanctions from nearly 50 countries written by more than 60 authors from around the globe. This entire effort was further complicated by recent world events, which resulted in numerous changes in sanctions and export controls laws during the past year.

During the multiyear journey to the publication of the second edition, we were assisted by more people than we can possibly name here, and we are immensely grateful to everyone else who lent a hand along the way.

This book is the product of exemplary collaboration between members of the Section, and a testament to what can be achieved by its dedicated members around the world. It is, therefore, fitting that our first thanks go to the incredibly dedicated group of chapter authors who made this book possible. They were invariably good natured about the inevitable fits and starts involved in bringing together a collective work of this kind, and we could not be more grateful to each and every one of them.

We also wish to thank the staff at ABA Publishing, Lorraine Murray, who guided and supported us throughout the drafting, editing, and production process. Our gratitude also goes to the then chair of the ABA International Law Section who supported the book from the outset and to the members of the Section's Publications Committee who gave this project the green light to proceed.

We would also be remiss if we did not single out the following individuals who often went above and beyond the call of duty in supporting our work and who are not elsewhere identified in this book: from Dentons Canada LLP, Wilson Munoz, Maha Hebesh, and Sadaf Rahimi, and from ArentFox Schiff LLP, Corey Smith. We wish to thank the partners of Dentons Canada LLP, ArentFox Schiff LLP, and Jacobson Burton Kelley PLLC, as well as our families, who patiently supported us through this time-consuming endeavor.

Editing can be a thankless task but assembling the various parts of this book into a comprehensive, practical, and useful whole, and our collaboration with the authors, allowed us to deepen and broaden our understanding of this challenging and everchanging area of the law. We are immensely grateful for the experience. Finally, while we are deeply indebted to all those who assisted us, we take full responsibility for any errors or omissions that may remain.

Kay Georgi, Paul Lalonde, and Doug Jacobson *Co-editors*

Thank you to the firm and company supporters:

ArentFox Schiff LLP

Ashok Dhingra Associates Atsumi & Sakai

Bass, Berry & Sims PLC

Bird & Bird

CHLY & Partners

Dentons Canada LLP

Duane Morris LLP

DuPont de Nemours, Inc.

G. Breuer

Grayston & Company

HFW

Jacobson Burton Kelley PLLC
JunHe LLP
McCarthy Tétrault LLP
MME Legal | Tax | Compliance Noerr
O’Melveny & Myers LLP
Pillsbury Winthrop Shaw Pittman LLP
Rajah & Tann Singapore LLP
Raphaël Barazza
Rigby Cooke Lawyers
S. Friedman, Abramson & Co.
Sánchez Devanny
Steptoe & Johnson LLP
Studio Legale Padovan TozziniFreire Advogados Winston & Strawn LLP

Preface

Export controls and economic sanctions are more relevant now than ever for companies and organizations operating in a rapidly evolving and increasingly global business environment. The developments in the last year alone have demonstrated the complexities of compliance with these laws. Export controls and economic sanctions affect a wide range of transactions and activities engaged in internationally by companies and organizations of all sizes—supplier and vendor relationships, distribution arrangements, import/export activity, licensing agreements, humanitarian aid and relief operations, investments, leases and property acquisitions, commodities trading, hiring of multinational employees and contractors, banking and finance transactions in both the traditional and decentralized finance spaces, mergers and acquisitions, joint ventures, and the list continues. The field of export controls and economic sanctions is now widely recognized as a sophisticated area of legal practice. Compliance with these laws is crucial to ensuring one's standing as a reputable player in the global community, not to mention avoiding the significant monetary fines, criminal penalties, investigation costs, loss of export privileges, and debarment from government contracting that can result from a violation of these laws.

This book is a project of the ABA International Law Section Export Controls and Economic Sanctions Committee, which is dedicated to developing and delivering programs, publications, and advocacy in the areas of export controls and economic sanctions measures. This second edition of the book is triple the size of the first edition—a recognition of the

significant developments that have taken place in export controls and economic sanctions since publication of the first edition of the book a decade ago. This book is intended as an overview of this complex and dynamic body of law. While it should prove a valuable resource to both seasoned and novice practitioners, compliance professionals, and students, it is neither a substitute for—nor should it be relied upon as—legal advice in the context of specific transactions.

We extend our gratitude and felicitations to the patient and tenacious editors, Kay Georgi, Paul Lalonde, and Doug Jacobson and an all-star lineup of co-authors for this tremendous contribution to the field of export controls and economic sanctions. This book offers a thorough yet practical guide that will assist counsel and compliance professionals in identifying and navigating the many complex issues presented by export controls and economic sanctions laws.

Andrea Al-Attar & Alexandre Lamy *Co-chairs*, ABA SIL Export Controls & Economic Sanctions Committee 2022–2023

1

U.S. Economic Sanctions Law

Greta Lichtenbaum[1]

1.1 Overview

The United States imposes economic sanctions for a variety of foreign policy, national security, criminal enforcement, economic reasons, and humanitarian reasons. These measures generally seek to influence and alter behavior by restricting financial and commercial activities with targeted countries, governments, problematic activities, sectors, individuals, and entities. Economic sanctions can also be used to protect assets from depletion by perceived malign actors, such as autocratic governments.

Two broad categories of economic sanctions measures are "primary sanctions" and "secondary sanctions." There is some overlap, but, as a general matter, primary sanctions prohibit certain transactions with the targets of sanctions, with the goal of pressuring that target to stop problematic activity or thwarting the activity (e.g., human rights abuses, terrorism, narcotics trafficking). Secondary sanctions put economic pressure on "innocent" actors to incentivize them to stop defined activities with a primary Sanctions Target.

What is regulated: U.S. economic sanctions can restrict a wide variety of transactions involving targeted countries, governments, organizations, persons, and activities (hereinafter "Sanctions Targets"). They also penalize U.S. persons and, in defined circumstances, non-U.S. persons for engaging in or facilitating those transactions. These measures often block (i.e., freeze) property in which the sanctioned actor has an interest.

Where to find the regulations: While U.S. economic sanctions are promulgated pursuant to a number of laws, the statutory authority for most of these programs is the International Emergency Economic Powers Act (IEEPA).[2] U.S. economic sanctions regulations are codified in 31 C.F.R. chapter V. Some measures apply only pursuant to executive order, and others may be implemented through the Export Administration Regulations (EAR).[3]

Who is the regulator: The U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) is principally responsible for administering U.S. economic sanctions programs. The U.S. State Department plays a key role in developing economic sanctions policy, reviewing some license applications, and administering certain secondary sanctions. The U.S. Department of Commerce's Bureau of Industry and Security (BIS) also administers economic sanctions measures in the EAR that involve exports and re-exports from the United States.

This chapter discusses the statutory authority for U.S. economic sanctions, who must comply with them, and how they are implemented. This chapter also addresses core sanctions restrictions and country-based, list-based, and sectoral programs and their associated compliance risks; it also identifies key exemptions, licenses, and compliance approaches that may mitigate these risks. The chapter then discusses compliance expectations. The final sections of this chapter describe the consequences of violating U.S. economic sanctions and the potential for conflicts between U.S. economic sanctions and certain non-U.S. laws. In addition, this chapter's Appendices contain summaries of the various U.S. economic sanctions country programs, specific risk considerations for multinational companies, and significant court decisions affecting U.S. economic sanctions. Subsequent chapters separately cover U.S. export and re-export controls, which govern the actual or deemed transfer of regulated U.S. goods, software, and technology across international borders, and U.S. antiboycott laws, which counteract certain non-U.S. economic sanctions and non-U.S. export and re-export controls.

(a) Statutory Authority

IEEPA is the authority for most economic sanctions programs. Other key statutes are the 1917 Trading with the Enemy Act (TWEA)[4] and the United Nations Participation Act (UNPA).[5] From the time of World War I through the late 1970s, the primary statutory authority for U.S. economic sanctions was TWEA. Originally drafted as only a war power, this statute was amended in 1933 to authorize broad economic sanctions programs to target unfriendly countries and their governments, both in times of peace and war. However, only sections 5(b) and 16 of TWEA, which respectively address presidential emergency authority and penalties, remained applicable after the end of World War II. In December 1977, the United States enacted IEEPA to address concerns of presidential accountability in the peacetime exercise of TWEA emergency powers. At the same time, Congress amended TWEA and limited its application to times of declared war or, subject to an annual presidential finding that a continuation is in the U.S. national interest, to TWEA-based economic sanctions programs existing at that time.[6] Of these "grandfathered" TWEA-based economic sanctions programs, only the economic sanctions against Cuba still remain effective pursuant to this annual continuation process. IEEPA is accordingly the statutory authority for most U.S. economic sanctions adopted since 1977.

IEEPA authorizes the President to impose economic sanctions to address national emergencies arising from foreign threats to the national security, foreign policy, or economy of the United States. In order to exercise this emergency authority under IEEPA, the President must submit a separate justification to Congress for each national emergency declared.

This power is broad, and has rarely been successfully challenged. There are a few limitations on the authority, however. As discussed in greater detail later in this chapter, Congress amended IEEPA in 1988 and 1994 to limit restrictions on certain transactions related to travel and exchanges of information. Better known as the "Berman Amendments," these provisions bar the President from using IEEPA powers to prohibit or regulate, directly or indirectly, any trade between countries in most information and informational materials as well as any transactions related to travel between countries and its arrangement.[7] IEEPA also exempts personal communications that do not transfer anything of value and, in the absence of certain Presidential determinations, in-kind donations to relieve human suffering.[8]

Economic sanctions authorized under IEEPA may be terminated at any time by the President. IEEPA-based economic sanctions also automatically terminate after one year if they are not properly renewed under its "sunset" provisions or by congressional action. The 1976 National Emergencies Act (NEA)[9] also allows the President to continue to exercise certain enforcement powers related to economic sanctions even after the termination of the relevant national emergency.

Both the NEA and IEEPA impose additional procedural and reporting requirements on the President in connection with declared national emergencies. These reporting requirements oblige the President to provide initial, semiannual, and termination reports to Congress on each declared national emergency.[10]

The UNPA is the statutory authority for the President's implementation of economic sanctions mandated by UN Security Council resolutions. Unlike IEEPA, UNPA does not include exemptions for trade in information, travel, personal communications, or in-kind donations; nor does the UNPA include presidential reporting requirements to Congress, automatic "sunset" provisions, or renewal obligations. Furthermore, other statutes impose particular economic sanctions on countries or on activities, such as narcotics trafficking.

Finally, as discussed further later in the chapter and in the Country Summaries in Appendix A, in the past ten years, there has been a proliferation of new statutes focusing on imposing secondary sanctions on certain jurisdictions and activities, most notably in Iran and Russia.

(b) Role of Congress

Congress also plays an important role in the implementation of U.S. economic sanctions programs, both in terms of oversight and in terms of legislating. Congress accorded significant authority to the President to impose economic sanctions through IEEPA. Other statutes serve to limit presidential authority in this sphere, or impose new sanctions that the President is required to implement. The 1996 Cuban Liberty and Democratic Solidarity (Libertad) Act,[11] which is more commonly known as the Libertad Act or the Helms-Burton Act, is a key example of statutory limitations on the President's authority. Among other measures, that statute effectively precludes any wholesale lifting of the Cuban sanctions absent an

act of Congress or a determination by the President that a transition government in Cuba is in power. The Countering America's Adversaries through Sanctions Act (CAATSA) is an example of secondary sanctions imposed by Congress primarily targeting Russia. That statute requires the President in some circumstances to impose sanctions, and in other areas accords the President discretion to impose sanctions.

(c) Implementation

While there are numerous similarities between economic sanctions programs, the benefit of experience with one economic sanctions program does not necessarily transfer to other economic sanctions programs. In fact, most implementing regulations state that "[d]iffering foreign policy and national security circumstances may result in differing interpretations of similar language among [various economic sanctions regulations]."[12] The differences in each program's administration often arise from the legislation, executive orders, regulations, and regulatory guidance under which the program is implemented. Moreover, each economic sanctions program has special features arising from its unique foreign policy context and history. As policy instruments of the U.S. government, the application and interpretation of U.S. economic sanctions programs must be dynamic and capable of changing with U.S. policy objectives. These objectives can change as the result of world events, along with changes in administration. The latter was starkly illustrated when the Trump administration adopted a very different policy approach to Iran, Cuba, and China than the Obama administration. The Biden administration has made limited modifications to the Trump administration's approach.

The implementing language of an economic sanctions program—whether in presidential executive orders, OFAC regulations, or licenses—often is intentionally vague, and its literal interpretation may reach a very wide range of transactions. As a result, U.S. regulators have great latitude to "break new ground" and penalize U.S. persons—or even non-U.S. persons—for conduct that the U.S. government has not challenged historically.

Therefore, knowledge of the implementation and administration of each U.S. economic sanctions program is an essential part of understanding and interpreting these complex, dynamic, and often overlapping programs. This requires a good understanding of the statutory authority invoked and the

executive orders imposing the economic sanctions program, their implementing regulations, and relevant guidance promulgated by OFAC.

(d) Executive Orders

The vast majority of U.S. economic sanctions programs derive from executive orders. The President's authority to issue these executive orders can stem from a general statutory authority, such as IEEPA or UNPA. As noted earlier, the President's authority may also originate from a congressional mandate that the President implement specific economic sanctions. Examples of such congressional mandates include the 2010 Comprehensive Iran Sanctions, Accountability and Divestment Act (CISADA)[13] and the 2003 Syria Accountability and Lebanese Sovereignty Restoration Act.[14]

These executive orders generally declare new, or build upon existing, national emergencies, specify the threat that is posed, define the characteristics for designation of the targets of the economic sanctions, establish their effective date, and delegate authority for their implementation. In most cases, this administrative and enforcement authority is delegated to the Secretary of the Treasury, acting in consultation with the Secretary of State and other specified cabinet officials. In turn, this administrative and enforcement authority generally is delegated further to the director of OFAC.

(e) OFAC Regulations

OFAC administers and enforces dozens of economic sanctions regulations (codified at 31 C.F.R. chapter V) along with other economic sanctions programs for which regulations have not yet been issued. In connection with these programs, OFAC may promulgate implementing regulations, require reports relating to targeted transactions, issue licenses authorizing otherwise prohibited transactions, and take enforcement measures in connection with violations. As discussed later in this chapter, OFAC also identifies and adds new Sanctions Targets to its Specially Designated Nationals and Blocked Persons List (SDN List) and reviews requests for their removal. The SDN List is available online in various formats at https://ofac.treasury.gov/ofac-sanctions-lists.

The regulations implemented and enforced by OFAC are available online at https://www.ecfr.gov/current/title-31/subtitle-B/chapter-V. Summaries and other guidance related to the economic sanctions programs administered by OFAC are available on its website at https://ofac.treasury.gov/sanctions-programs-and-country-information. However, regular changes to U.S. economic sanctions programs necessitate that users of OFAC's website materials check their associated dates and use appropriate care to identify subsequent program changes.

OFAC has also increased its practice of issuing Frequently Asked Questions on its website. While these do not have the authority of regulations, they provide helpful guidance that is increasingly relied upon by the regulated community.

1.2 Jurisdictional Reach of U.S. Economic Sanctions Laws

All U.S. economic sanctions programs are intrinsically extraterritorial in nature. Indeed, OFAC's outward focus is evident from its stated mission of administering "economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to national security, foreign policy or economy of the United States."[15] The targets of U.S. economic sanctions laws are outside of U.S. territory and as a result cannot typically be reached by laws that govern domestic U.S. activity. As a consequence, U.S. economic sanctions laws inevitably restrict activities outside the United States, thereby impacting non-U.S. persons, including those that are not a target of the sanctions.

This extraterritorial effect can create challenges between U.S. and non-U.S. counterparties and within diplomatic channels. U.S.-based multinational companies seeking to comply with U.S. economic sanctions laws often face resistance from their non-U.S. counterparties; including, in some instances, a categorical rejection of proposed sanctions-related restrictions on commercial activity on the grounds that U.S. laws do not apply to non-U.S. counterparties. It can be helpful in such situations to explain the applicable bases for jurisdiction over the activity in question. All economic sanctions laws have a U.S. nexus that forms the basis for asserting jurisdiction, although that nexus differs among those laws and

depending on the circumstances at hand. This section describes the principal bases for jurisdiction, and briefly highlights areas of compliance risk that U.S. firms and their non-U.S. counterparties face as a result of the reach of these laws.

(a) Persons with Territorial or Nationality Ties to the United States

As noted earlier, IEEPA is the President's general legal authority for imposing economic sanctions measures targeting countries, regimes, individuals, and entities. With some exceptions (e.g., Cuba), this law is the authority underlying most existing U.S. sanctions programs. While economic sanctions programs promulgated under IEEPA can be applied to all persons "subject to the jurisdiction of the United States,"[16] in practice, most executive orders and regulations promulgated pursuant to IEEPA apply to the somewhat narrower class of "U.S. persons." That term is defined to include (1) entities organized under the laws of the United States, including foreign branches; (2) U.S. citizens and U.S. permanent residents; and (3) any persons located in the United States.[17] This definition is limited to persons with U.S. nationality or territorial ties to the United States and does not include foreign incorporated entities.[18]

While most U.S. companies are generally aware that economic sanctions regulations apply directly to them, they face more complicated compliance challenges in connection with their activities with non-U.S. business partners that may themselves engage in activities with Sanctions Targets. For example, foreign subsidiaries of U.S. companies are not U.S. persons and therefore not subject to sanctions under most IEEPA-based sanctions programs. A U.S. parent must be careful, however, not to facilitate the activities of foreign subsidiaries with Sanctions Targets, as such facilitation actions are themselves prohibited under most IEEPA programs.[19] This can be challenging, as many parent companies support foreign subsidiaries in a variety of ways, from IT support to human resources management to financial assistance. All of these support mechanisms can potentially facilitate specific business with Sanctions Targets.

Another compliance challenge that many multinational companies with complicated organization structures face in connection with territorial- or

nationality-based jurisdiction resides in their foreign branches. Unlike foreign subsidiaries, foreign branches of U.S. companies are "U.S. persons." Individuals employed by such foreign branches must be mindful of that fact. Conversely, some enforcement actions reveal that non-U.S. companies can also be caught unawares by the fact that their U.S. branches —incorporated outside the United States but operating in U.S. territory— are also directly subject to IEEPA sanctions programs.

All entities outside of the United States, whether U.S. subsidiaries or completely foreign companies, also need to be aware that U.S. citizens or permanent resident aliens are U.S. persons even when they are on foreign soil. Accordingly, entities outside the United States need to take care to ensure their U.S. person employees are not involved in sanctions-related transactions.

(b) Jurisdiction over the Item

Relying on the limited scope of the "U.S. person" definition, non-U.S. persons acting outside the United States often assume that they are never subject to the restrictions of IEEPA programs. The origin of the property involved in a particular transaction, however, provides an independent basis for jurisdiction under IEEPA, other sanctions laws, and export control laws.

U.S. economic sanctions laws (and parallel export control laws) restrict the export and re-export of U.S.-origin goods, software, and technology, including defined levels of U.S.-origin content in foreign-assembled products, to Sanctions Targets such as Iran, North Korea, and Syria.[20] These restrictions apply to U.S. and non-U.S. persons alike, although there can be some differentiation between U.S. persons and non-U.S. persons with respect to re-exports. Most notably, non-U.S. persons that are not owned or controlled by a U.S. person are not prohibited from re-exporting nonsensitive U.S. goods to Iran if those goods are in inventory outside the United States (though in certain circumstances engaging in such transactions could entail a risk of becoming a Sanctions Target through the application of secondary sanctions).

The courts have confirmed that IEEPA's authority extends to non-U.S. persons handling U.S.-origin goods, even where such persons are not in the United States. One First Circuit decision, for example, held that IEEPA clearly applies to non-U.S. persons where U.S. goods are involved.[21] That

case involved the conviction of a UK citizen for unauthorized exports to Libya. There have also been numerous Department of Justice (DOJ) criminal cases and OFAC and BIS civil enforcement investigations (the Commerce Department enforces the EAR) targeting non-U.S. persons involving unauthorized exports and re-exports of U.S.-origin goods to sanctioned countries and other destinations, even where such persons acted wholly outside the United States.

The consequence of this jurisdiction over originating items is that both U.S. persons and non-U.S. persons must be concerned about unlawful diversion to Sanctions Targets where U.S.-origin goods or technology is involved. The most commonly used compliance mechanism is a contractual geographical restriction, for example, in distribution arrangements, contracts for the sale of goods and software, or technology licenses involving U.S.-origin technology. OFAC and the Commerce Department also advise companies to conduct careful due diligence on overseas counterparties to ensure that such counterparties are aware of and will abide by economic sanctions and export control laws. With respect to non-U.S. counterparties that assert that such laws are inapplicable to their activities, it is worthwhile bringing to their attention that the United States is not alone in asserting jurisdiction over items originating in its territory. Most jurisdictions maintain and enforce export control laws.

(c) Causing a Violation by Dealing in Property in the United States or Procuring U.S.-Origin Services that Benefit Sanctions Targets

IEEPA also provides jurisdiction over dealings in all property "in the United States." In enforcement actions involving financial institutions, the U.S. government has taken the position that non-U.S. persons can be reached by IEEPA and other U.S. statutes even where such persons are acting outside the United States in a way that results in transactions involving property (including services) within the United States. Specifically, OFAC, DOJ, and bank regulators have successfully pursued non-U.S. financial institutions that allegedly used the U.S. banking system to facilitate activities in sanctioned countries. These cases, which have often involved removal of Sanctions Target-related information from funds transfer information in a process called transaction stripping, have resulted

in very large criminal and civil fines against European banks. The various Deferred Prosecution Agreements (DPAs) have differing characterizations of the U.S. nexus that provides the jurisdictional basis for invoking U.S. economic sanctions laws.

One of the first "transaction stripping" cases that targeted non-U.S. actors involved the UK firm Lloyds TSB, which entered into a DPA in January 2009, agreeing to forfeit US$350 million. The DPA alleges that Lloyds UK branches (with no involvement from its U.S. branches, but with unwitting involvement from other unrelated U.S. financial institutions) allegedly stripped customer names, bank names and addresses, and other identifying information from wire transfers to U.S. financial institutions over a period of ten years. Similarly, Credit Suisse entered into a DPA in December 2009, agreeing to forfeit US$536 million. The DPA alleges that the Swiss and UK branches stripped customer names, bank names and addresses, and other identifying information from wire transfers to U.S. financial institutions.

With respect to IEEPA-based restrictions, the Credit Suisse DPA alleges violations of 31 C.F.R. §§ 560.203 and 560.204 of the then-named Iranian Transactions Regulations (ITRs), which "prohibit (a) the exportation from the United States of a service to Iran without authorization, and (b) any transaction within the United States that evaded and avoided, or had the purpose of evading and avoiding such regulations."[22] The Lloyds TSB DPA similarly alleges that Lloyds TSB violated the ITRs and the then-effective Sudanese Sanctions Regulations' prohibitions on the export of services from the United States to Iran and Sudan, respectively.[23]

Barclays' DPA, entered into in August 2010, characterizes the IEEPA-based charges differently. The underlying activity is similar to Credit Suisse and Lloyds TSB, with a similarly large settlement. Barclays agreed to forfeit a total of US$298 million because it allegedly stripped identifying information from sanctioned country customers and routed the payments through U.S. banks. The Barclays DPA states that Barclays "engaged in conduct and practices outside the United States that caused its New York Branch and other financial institutions located in the United States to process payments in violation of U.S. sanctions."[24]

This characterization of the IEEPA jurisdictional link is supported by an amendment of IEEPA. In October 2007, IEEPA was amended to extend civil and criminal penalties not only to those that engage in prohibited

activity directly but also to those that "cause" violations, stating now that it shall "be unlawful for a person to violate, attempt to violate, conspire to violate, or *cause a violation* of any . . . prohibition."[25] Many other "transaction stripping" cases, including enforcement settlements with BNP Paribas and HSBC, take similar approaches.

While the various DPAs and other settlements contain somewhat differing characterizations of the U.S. nexus justifying application of IEEPA, these non-U.S. financial institution cases all reflect a common theme: non-U.S. persons that use the U.S. financial system must accept the jurisdiction of U.S. law, even where all of their actions appear to them to take place wholly outside the United States, and the U.S. actor is unaware of the ultimate beneficiary of the services it provides. There is some consistency between this position and that taken in Foreign Corrupt Practices Act (FCPA) cases. The DOJ takes the position that anti-bribery jurisdiction exists even where the only U.S. nexus is the transfer of funds for illegal purposes through a U.S. bank account.

The jurisdictional theories in the transaction stripping cases have not been tested in court. U.S. and non-U.S. companies (including those operating outside the financial sphere) should nonetheless be mindful that the U.S. government will pursue those outside the United States that conduct business with Sanctions Targets, if in doing so they benefit in some way from funds or other assets moving through, or services originating in, the United States, particularly where such movement or services were unwittingly provided.

(d) Jurisdiction through Ownership or Control

Prior to IEEPA, the TWEA was the most frequently invoked authority for economic sanctions programs. Currently, the only TWEA program in effect is the Cuban Asset Control Regulations (CACRs). The CACRs prohibit almost all commercial transactions between the United States and Cuba. The CACRs extend their jurisdiction beyond the narrower "U.S. person" concept to the broader category including any "person subject to the jurisdiction of the United States," which is defined to include U.S. persons plus "[a]ny corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by" U.S. persons.[26] Under the CACRs, therefore, entities outside of the United States

that are owned or controlled by U.S. persons are equally prohibited from doing business in Cuba or with Cuban state-owned enterprises and from exporting products, technology, or services to Cuba, even non-U.S.-origin items from foreign locations. Unlike the IEEPA programs for Venezuela and Syria, therefore, the CACRs apply to non-U.S. subsidiaries of U.S. companies.

This broad extraterritorial jurisdiction on the basis of ownership or control alone has led to tensions with the United States' trading partners, including the European Union. The EU, Mexico, and Canada all have enacted blocking statutes intending to prohibit companies from complying with U.S. laws considered to be wholly extraterritorial; most notably, these laws target the CACRs and related statutes targeting Cuba. Therefore, in addition to the IEEPA-based compliance risks just identified, U.S. and non-U.S. companies must find ways to navigate these conflicting statutes.

Separately from Cuba, one other current sanctions program also directly regulates the activities of foreign subsidiaries of U.S. companies. With the enactment of the Iran Threat Reduction and Syria Human Rights Act in 2012,[27] the Iran sanctions also apply directly to non-U.S. subsidiaries of U.S. firms. As discussed later, this prompted the EU to amend its blocking regulation to counter U.S. laws and regulations targeting Iran that apply to EU subsidiaries of U.S. firms.

(e) Denial of Access to U.S. Market and Other Benefits: Secondary Sanctions

The enforcement posture underlying the transaction stripping cases (i.e., that non-U.S. persons should not be able to use the U.S.-based financial infrastructure to advance activities inconsistent with U.S. foreign policy) is taken one step further through U.S. secondary sanctions measures, also called retaliatory sanctions. Secondary sanctions contrast with primary sanctions because they reach persons that are not subject to U.S. jurisdiction in relation to activity with a Sanctions Target. Although the United States cannot prohibit activity in such circumstances, it can exert economic coercion through secondary sanctions. The most notable of these measures is the Iran Sanctions Act of 1996 (ISA), which was amended and significantly expanded through passage of CISADA in 2010 and the Iran

Threat Reduction and Syria Human Rights Act in 2012. There are many others, including ones imposed through executive order.

These measures typically apply to any person, but primarily target non-U.S. persons (as U.S. persons are already prohibited from investing or trading with the Sanctions Target under primary economic sanctions programs). Under these measures, sanctions may be imposed if an investigation concludes that certain "sanctionable" activity has occurred. As a general matter, such "sanctionable activity" is typically tied to sectors that are the most critical sources of revenue for the Sanctions Target or support for malign activity. For Iran, secondary sanctions apply to a range of sectors, including large investments in the Iranian energy sector, along with activities that support the production of refined petroleum products in Iran and the importation of refined petroleum products into Iran. The Trump administration expanded the secondary sanctions on Iran to the iron, steel, aluminum and copper, construction, mining, manufacturing, and textile sectors in Iran. Non-U.S. entities (including foreign financial institutions) that facilitate Iran's nuclear program, its support for terrorism, or the activities of Iran's Islamic Revolutionary Guard Corps may also be sanctioned under ISA.

Russia is another notable target of secondary sanctions. As with Iran, those Sanctions Target industries that are key to the health of the Russian economy (energy), or are a perceived source of problematic activity (defense). Specifically, CAATSA, which came into force in August 2017, focuses on the energy sector, through Title II (the Countering Russian Influence in Europe and Eurasia Act of 2017, or CRIEEA). Among other elements, these statutory measures impose secondary sanctions on persons involved in certain activity related to Russia's energy export pipelines; significant investment in deepwater, Arctic offshore, or shale oil projects; and foreign financial institutions that facilitate certain transactions for Russia's energy sector. The Protecting Europe's Energy Security Act of 2019 requires sanctions on foreign persons who provide subsea pipe-laying vessels for the construction of Nord Steam 2 and Turkstream.

Under most secondary sanctions measures, if the President determines that a person engaged in specified activities should be sanctioned, the President must select from a menu of sanctions, absent a presidential waiver. ISA, for example, requires the President to select at least three of nine enumerated sanctions:

- Denial of export-import bank loans, credits, or guarantees;
- Denial of licenses to export military or militarily useful technology;
- Prohibition on U.S. financial institutions making loans or providing credit of more than US$10 million in any 12-month period (with minor exceptions);
- Prohibition on obtaining U.S. government procurement contracts;
- Restrictions on imports into the United States;
- If the violator is a financial institution, prohibition on being designated as a primary dealer in U.S. government debit and/or prohibition on acting as an agent for U.S. government funds;
- Prohibition on foreign exchange transactions in the United States;
- Prohibition on transfer of credits or payments by financial institutions in the United States; and
- Prohibition on any dealings in property in the United States.

The principal distinction between secondary sanctions (such as ISA) and primary sanctions (such as IEEPA and TWEA) is that secondary sanctions use different tools to influence behavior than the penalties applied in primary programs. Since ISA and other secondary sanctions measures seek to sanction enumerated activities where there is no U.S. nexus between the activities in question and the United States, there is no jurisdictional basis for civil or criminal fines. Rather, secondary sanctions measures present actors with a choice: if you engage in certain enumerated activities, then benefits originating in U.S. commerce that would otherwise be available to you will no longer be available.

The most draconian secondary sanctions consequence for engaging in specific activities contrary to U.S. interests (and the one used more frequently in recent years) is the blocking order. As discussed further later in the chapter, the blocking order is a very powerful tool because it completely shuts down the Sanctions Target's ability to move funds through the U.S. financial system or otherwise deal with U.S. persons. The increasing use of blocking orders as a threat under secondary sanctions has been effective. Many non-U.S. firms have ceased activities with Sanctions Targets to avoid that risk.

The frequent use of blocking orders in the secondary sanctions context is most starkly illustrated in a number of executive orders authorizing the sanctioning of persons that provide "material support" for Sanctions Targets. This authority was used frequently in the case of Iran by the Trump

administration, as exemplified in the January 23, 2020, sanctioning of various petrochemical companies in Asia and the Middle East that were determined to be providing material support to the National Iranian Oil Company (NIOC). In March 2020, OFAC then added two Rosneft affiliates, Rosneft Trading and TNK Trading International, to the SDN list for Venezuela oil trading activity. The threat of a blocking order pursuant to secondary sanctions is also the point at which secondary sanctions essentially converge with primary sanctions. From a primary sanctions perspective, U.S. persons face civil and criminal liability for any dealings with persons subject to blocking orders, regardless of whether that order is imposed as a result of a secondary sanctions measure, or because the United States is focusing on a newly recognized problematic or malign activity (e.g., SDN listing for interference with a U.S. election).

(f) Conclusion

The United States has been criticized for the extraterritorial application of its economic sanctions laws, many of which are unilateral programs with no parallel, or significantly narrower, United Nations' counterparts. As explained earlier, however, non-U.S. persons will incur civil or criminal liability only where there is a U.S. nexus. That nexus is admittedly more attenuated in the transactions stripping cases, but it nonetheless exists. U.S. and non-U.S. parties seeking to mitigate risk under U.S. economic sanctions laws must therefore be alert to the existence of a U.S. nexus to activities that may have a direct or indirect connection to Sanctions Targets. Even without a U.S. nexus, however, non-U.S. persons must be alert to the potential risk of secondary sanctions.

1.3 Core Restrictions and Obligations

This section summarizes the core tools OFAC uses in furtherance of the goals of a given sanctions program. The tools generally fall within one of three categories: blocking of property, vesting of property, and prohibiting certain defined types of transactions.

(a) Blocking of Property

The blocking of property is a commonly used and very broad measure. Subject to certain exemptions, blocking orders prohibit all transfers and dealings in a target's property or interests in property within the United States or otherwise within the possession or control of a U.S. person[28] (regardless of where the U.S. person is located). Therefore, U.S. persons have a duty to retain, or "freeze," blocked property interests within their possession or control, and they may not engage in any unauthorized disposition of a "frozen" asset.[29] Thus, U.S. persons may not perform blocked contracts, and OFAC regulations normally require that they deposit funds and liquid assets, including securities, into a blocked interest-bearing account.[30] Commonly, blocking prohibitions catch U.S. dollar-denominated wire transfers that pass through U.S. financial institutions, which then place the wired funds into a blocked account and timely notify OFAC.

Various OFAC regulations define "property" and "interests in property" extremely broadly,[31] and they do not distinguish between real, personal, mixed, or intangible property. Examples include money, securities, debts, security rights, bills of lading, goods, accounts payable, judgments, contracts of any nature, as well as any other present, future, or contingent interests in them. Absent authorization from OFAC, U.S. persons cannot credit or debit blocked bank accounts; sell or pledge blocked shares of stock or pay related dividends; issue, confirm, or perform under letters of credit for goods carried on a vessel that is an SDN or is owned by an SDN; or trade commodity contracts benefiting an SDN.

OFAC regulations also include "services of any nature whatsoever" within the definition of "property" and "property interests."[32] This step, which goes significantly outside of a normal understanding of "property," allows OFAC blocking sanctions to effectively cut off all trade, whether in merchandise or services, with a Sanctions Target.

Blocking measures apply to all property and interests in property of any person on the SDN list; to the property and interests in property of the governments of Cuba, Iran, North Korea, Venezuela, and Syria (including agencies, instrumentalities, or entities controlled by them, such as central banks); and to the property and interests in property of any person directly or indirectly owned 50 percent or more, alone or in the aggregate, by one or more blocked person.

The question of ownership by an SDN can create compliance challenges, as entities owned 50 percent or more by an SDN are not necessarily themselves on the list. For this reason, a thoughtful, risk-based due diligence process is important. To compound the challenge, OFAC urges caution regarding dealings with entities that are less than 50 percent owned by a blocked person or persons; the blocked person(s) may have an interest in the specific dealings at issue, and these entities may be added to the SDN list by OFAC in the near future for acting on behalf of the blocked person(s).

(b) Vesting of Property

In essence, vesting is the transfer by the U.S. government of title to blocked property from a Sanctions Target to another person or agency. For example, section 5(b) of TWEA permits assets to be vested and used by presidential directive. In peacetime, this power is rarely used. However, vesting authority was used in the early 2000s to transfer blocked Cuban funds to pay compensation to the families of the "Brothers to the Rescue" pilots shot down by Cuba in 1996.

In addition, section 106 of the 2001 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act[33] amended IEEPA to grant vesting authority to the President with respect to the assets of governments or persons found to have engaged in armed hostilities with, or attacks on, the United States. This authority was used to transfer blocked assets of the government of Iraq to the Development Fund for Iraq to benefit the Iraqi people in compliance with United Nations Security Council Resolution 1483.

(c) Prohibitions on Transactions with Sanctions Targets

A variety of other building blocks of economic sanctions programs may be chosen by the President to prohibit engaging in, facilitating, or exporting services by U.S. persons or within the United States in support of certain defined types of transactions, but shy of blocking property involved in those transactions. These measures may focus on all transactions in a targeted country, with a targeted government (including entities owned or controlled by a targeted government), or involving targeted persons or targeted

activities. The definition of the specific transaction type can range from being precise (such as the ban on transactions in debt of more than a certain days maturity with certain listed Russian entities) to broad (such as the prohibition on virtually all exports and re-exports of services to Syria).

(d) Reporting Requirements

The Reporting, Procedures, and Penalties Regulations (RPPRs) set forth the reporting and recordkeeping requirements for economic sanctions programs administered by OFAC. Most notably, these include requirements to report blocked property and rejected transactions to OFAC. As discussed earlier, if a person is added to the SDN list, OFAC's regulations block all "property" in which the party has an interest, including present, future, and contingent interests. The RPPRs require any U.S. person or person subject to U.S. jurisdiction that holds blocked property to submit relevant reports to OFAC within ten business days of the property becoming blocked.[34]

The RPPRs also require parties to report "rejected" transactions in circumstances where the relevant sanctions program prohibits the transaction, but it is not subject to a blocking order. For rejected transactions, prior to June 21, 2019, only U.S. financial institutions were required to submit reports to OFAC for rejected funds transfers.

Effective June 21, 2019, OFAC amended the RPPRs to require any U.S. person or person subject to U.S. jurisdiction, including parties that are not financial institutions, that rejects a transaction to submit a report to OFAC within ten business days of the rejected transaction. "Transaction" is defined to include "transactions related to wire transfers, trade finance, securities, checks, foreign exchange, and goods or services."[35]

One question presented is what actions trigger reporting requirements for "blocked" or "rejected" transactions. Clearly, these reporting requirements are triggered if there is an actual or attempted exchange of value (i.e., sending money or attempting to send money). The question is whether the reporting is triggered prior to that point. FAQ 53 is somewhat instructive, as it distinguishes between a mere inquiry (not reportable), and an actual instruction (reportable). It explains:

> In the case of a wire transfer, the bank will be holding blocked property upon the receipt of concrete instructions from its customer to send the funds. In this case, the funds must be blocked and reported to OFAC within ten days. If, on the other hand, a customer simply asks "Can I send money to Cuba?" there is no blockable interest in the inquiry and the bank can

answer the question or direct the customer to OFAC. The same logic applies to cases where the transaction would be required to be rejected under OFAC regulations. There is not technically a "reject" item until the bank receives instructions from its customer to debit its account and send the funds.

The reporting requirements, and the parallel deadlines, are affirmative requirements. Failure to comply can lead to penalties, and therefore it is an important part of any compliance program to have procedures to comply with these rules. OFAC's receipt of such reports gives it the ability to track the effectiveness of a given program, and also provides an important enforcement tool. It scrutinizes blocking and rejection reports to detect illegal activity.

1.4 Country-Based Economic Sanctions Programs

Most U.S. economic sanctions adopted through the late 1990s targeted specific countries and their governments. Often called comprehensive, country-based, or territorial economic sanctions, these programs usually function by blocking the government of the targeted country and imposing prohibitions on certain defined types of transactions with or within the territory of the targeted country.

More specifically, the country-based programs generally prohibit regulated persons from engaging in or facilitating trade in goods, services, technology, or financial transactions within a targeted country's territory, and prohibit all transactions with, and all property of, its government (including its agencies, instrumentalities, and controlled entities). Most of the country-based programs also incorporate some level of restriction on imports into the United States of goods, software, or technology of targeted country origin. Additionally, these country-based sanctions programs often have certain list-based components for designating and blocking the assets of SDNs associated with the targeted country and its government.

As a general matter, the more recently adopted country-based programs tend to have a narrower range of targeted activities than their predecessors do. The oldest of the current country-based programs is the sanctions program against Cuba. The program was developed against the backdrop of the Cuban revolution, taking of American property, missile crisis, and concern about communism on the United States' doorstep. These concerns are reflected in the program's broad blocking of and prohibition on dealings

with all Cuban individuals and entities—even when dealing with nongovernmental persons or when they are located in third countries outside of Cuba—unless such persons' assets have been unblocked by an OFAC license.

By contrast with the Cuba sanctions, the later broad-based U.S. economic sanctions programs (currently including Iran; North Korea; Syria; and the Crimea, Donetsk, and Luhansk regions of Ukraine) and sectoral sanctions programs (discussed later and currently including Venezuela, Russia, and China) generally do not restrict U.S. persons from engaging in or facilitating transactions with nationals of those countries that occur entirely outside the targeted country. However, these programs generally would prohibit a U.S. person from engaging in or facilitating a transaction outside the targeted country either with an individual acting as an agent for a targeted government or in a context that places that U.S. person on notice that the transaction—for example, a transfer of goods or technology—is intended to lead to a prohibited export or other targeted transaction or activity.

While third countries' economic sanctions programs may mirror certain aspects of U.S. country-based economic sanctions (particularly where they are based on UN Security Council resolutions), the United States has often adopted country-based programs unilaterally. The unilateral nature of these economic sanctions programs creates business and compliance challenges for U.S. businesses. These programs place U.S. firms at a competitive disadvantage in global markets where non-U.S. firms are not required to comply with similar restrictions.

Appendix A includes a detailed chart of the distinguishing features of each of the comprehensive country programs, including key prohibitions, general licenses, and secondary sanctions.

1.5 List-Based Economic Sanctions Programs

As noted earlier, the United States generally followed a country-based model when implementing its earliest economic sanctions programs. These programs typically targeted the countries and governments of wartime enemies and imposed blocking prohibitions that restricted all dealing with those enemies, their nationals, and the territories they controlled. However, an integral part of such programs was the identification of and imposition of

economic sanctions on SDNs of the targeted country. In general, SDNs were persons that were owned, controlled, or acting for or on behalf of those enemy governments and were often located in third countries. Insofar as they were treated with the same blocking restrictions as all the nationals of the targeted country but were often specifically identified and designated for sanctions, they were termed “specially designated” nationals. Over time, however, U.S. economic sanctions began to target persons who were not tied to specific countries or regimes, such as international terrorist organizations or narcotics traffickers, and more recently organizations that have engaged in human rights violations, malicious cyber-enabled activities, corruption, and interference with U.S. elections. Therefore, the name of this list was broadened to be the “List of Specially Designated Nationals and Blocked Persons,” although its shorthand reference remains the “SDN list.”

Diverging from the mix of territorial restrictions and restricted party designations in country-based programs, economic sanctions programs that primarily rely on the designation of targeted persons and entities are called list-based programs. U.S. list-based programs typically target specific individuals, entities, or government agencies involved in activities threatening the national security, foreign policy, or economy of the United States. Among others, these targeted threats stem from terrorism, narcotics trafficking, weapons proliferation, human rights abuses, suppression of civil rights, genocide, corruption, and transnational organized crime. The United States also uses list-based economic sanctions to implement mandatory UN Security Council resolutions (e.g., resolutions related to al-Qa’ida, Iran, Somalia, and Syria), and certain cooperative programs adopted with the European Union (such as programs addressing terrorism or targeting the governments of Belarus and Zimbabwe).

The U.S. government’s current preference (and that of both the European Union and the UN Security Council) for list-based programs reflects two key traits of these programs. First, list-based programs target specific “bad actors” rather than placing the burden of economic sanctions on a country’s population at large. Second, list-based programs can be implemented with relative ease through automated screening, which has become one of the most important instruments for compliance with economic sanctions. However, this current preference for list-based

economic sanctions is not without exceptions, as evidenced by the broader features of both the Russia and the Venezuela programs.

1.6 Sectoral Sanctions

In addition to blocking sanctions prohibiting transactions with specific countries, entities, and individuals, OFAC imposes sanctions targeting specific sectors of a country's economy. The most notable example is Russia. With the 2022 invasion of Ukraine, the United States has significantly expanded its strategy of sanctioning key sectors of that economy while avoiding a comprehensive embargo.

(a) Russia

Following Russia's annexation of Crimea in 2014, OFAC adopted sectoral sanctions, focused on Russia's energy, defense, and finance sectors, that prohibit U.S. persons from engaging in certain transactions with entities designated on a new Sectoral Sanctions Identification (SSI) list. OFAC Directives 1, 2, and 3 under Executive Order 13662 implement sectoral sanctions restricting the issuance of debt and equity for designated financial institutions, defense companies, and oil and gas companies beyond short periods of time (tenor varies from 14 to 60 days). Debt and equity are broadly defined. Debt includes "bonds, loans, extensions of credit, loan guarantees, letters of credit, drafts, bankers acceptances, discount notes or bills, or commercial paper"; equity includes "stocks, share issuances, depositary receipts, or any other evidence of title or ownership."[36] Because the concept of "debt" includes extensions of credit, the sale of products and services to entities designated under Directives 1, 2, and 3 can violate the directive if the terms of payment exceed the number of days specified in the relevant directive; as well, if the customer pays late, a license is needed to accept such payment. Key designations include Gazprombank, VTB Bank, and Sberbank under Directive 1, and Gazprom Neft, Novatek, and Rosneft under Directive 2. Directive 4 prohibits U.S. persons from providing goods, services, and technology in support of exploration or production of oil in deepwater, Artic offshore, or shale projects in Russia or with designated companies outside Russia. Gazprom, GazpromNeft, Lukoil, and Rosneft have been designated under Directive 4.

In 2022, in response to Russia's invasion of Ukraine and occupation of the Donetsk and Luhansk regions of Ukraine, the United States imposed additional sanctions, largely in coordination with its allies. OFAC Directives 1A, 2, 3, and 4 (under E.O. 14024) implement sectoral sanctions restrictions on financial sector and capital market access. Directive 1A prohibits participation in the primary and secondary markets for bonds issued by the Russian Central Bank, National Wealth Fund, or the Ministry of Finance. Directive 2 prohibits the opening or maintaining of correspondent or payable-through accounts and processing of transactions involving foreign financial institutions at designated financial institutions. Directive 3 prohibits dealings in new debt and equity of certain Russian financial institutions and Russian-owned state enterprises. Directive 4 prohibits U.S. persons from engaging in transactions involving the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, and the Ministry of Finance of the Russian Federation, including any transfer of assets to such entities or any foreign exchange transaction for or on behalf of such entities, except for certain energy-related transactions licensed by OFAC.

In addition, the United States imposed restrictions on new investment in any economic sector, as well as restrictions on the provisions of additional types of services. To date, these include the provision of certain accounting, trust and corporate formation, and management consulting services by U.S. persons in Russia. The United States also banned the import into the United States of the following products from Russia: gold, crude oil, petroleum, petroleum fuels, oils and related distilled products, liquefied natural gas, coal and coal products, fish and seafood, alcohol, and nonindustrial diamonds, and imposed export licensing requirements of all items on the Commerce Control List and a long list of industrial, commercial, and luxury items.[37]

(b) Venezuela

In May 2018, the United States imposed sectoral sanctions restricting transactions in debt and equity involving the Venezuelan government.[38] Like those imposed on Russia, these restrictions were designed to restrict access to capital, but also restricted what terms of payment could be provided to the listed entities in the context of trade in goods and services.

Sectoral sanctions on Venezuela expanded in November 2018, with Executive Order 13850, authorizing blocking orders on persons determined to operate in Venezuela's gold sector. In January 2019, OFAC broadened the sectoral sanctions further to target persons operating in Venezuela's oil sector and added PdVSA (Petroleos de Venezuela, S.A.), Venezuela's state oil company, to the SDN list.[39] Ultimately, in August 2019, the government of Venezuela was itself blocked pursuant to President Trump's Executive Order 13884.

(c) China

Sectoral measures restricting access to U.S. capital were most recently imposed on China. On November 12, 2020, President Trump issued Executive Order 13959, prohibiting U.S. individuals and entities from investing in Chinese companies that the U.S. government identified as having ties with the Chinese military. In July 2021, President Biden issued Executive Order 14032, replacing E.O. 13959, which prohibits U.S. individuals and entities from engaging in transactions in publicly traded securities, or securities derivative of or designed to provide investment exposure to entities determined to be operating or having operated in the defense and related material, and surveillance technology sectors of the Chinese economy.

These sectoral sanctions show another area of overlap between primary and secondary sanctions. Both tools seek to influence the behavior of governmental Sanctions Targets by undermining the functioning and health of key sectors of the economies of their countries.

1.7 Exemptions and Licenses

The drafters of sanctions measures (whether statutes, executive orders, regulations, or specific OFAC actions) recognize that there may be circumstances where a given restriction may have collateral consequences that conflict with the measure's underlying purpose or other important policies, or create short-term challenges for U.S. persons. Exemptions and licenses are tools used in order to avoid such unintended or unwanted consequences.

The terms “exemption” and “license” are often used interchangeably to denote relief from the application of an economic sanctions prohibition. They are different tools however. An “exemption” is either a statutory provision that removes particular categories of transactions from the President’s congressionally authorized power to impose economic sanctions, or refers to a limitation in an executive order that removes stated classes of transactions from the scope of the imposed economic sanctions. The term “license” is a regulatory provision or independent OFAC action establishing an exception to an economic sanctions prohibition.

(a) The Berman Amendments

The most notable statutory exemptions are the so-called Berman Amendments, which circumscribe the President’s authorities under IEEPA and TWEA to restrict the flow of information and personal travel. In 1988 and 1994, Congress enacted amendments to IEEPA and TWEA proposed by Representative Howard Berman resulting in exemptions for the import and export from/to any country of certain information and informational materials. IEEPA was also amended to exempt certain transactions related to travel to or from any county. The IEEPA travel exemption of the Berman Amendments is limited to international travel and related in-country maintenance transactions (including related in-country domestic travel). However, it does not cover activities that are not purely incidental to such exempted travel (such as prohibited contracting or trade transactions), even if they occur during otherwise exempted travel.

The exemption for trade in information and informational materials broadly covers both tangible and electronic media, but there are some important carve outs. First, the Berman Amendments do not exempt exports of information and informational materials that are controlled under U.S. export control laws. Second, items covered by espionage laws are also not exempted by the Berman Amendments.[40] Third, and most importantly, the OFAC regulations implementing the exemption narrow it to exclude transactions in informational materials that are not “fully created and in existence at the date of the transaction.”[41] This qualifier makes clear that the exemption is not intended to cover services provided in the course of creating informational materials (e.g., the commissioning of a report or piece of art). OFAC has issued guidance on where that line is drawn: for

example, holding conferences (services), providing internet access (informational materials, but to a point), and publishing (not exempt, but covered by a general license). An OFAC advisory also offers another interpretation that has the effect of circumscribing this exemption in another important way. In its advisory regarding sanctions risks in dealing in high-value artwork, OFAC states that, notwithstanding the fact that art is expressly included in the Berman Amendment, it "does not interpret this exemption to allow blocked persons or their facilitators to evade sanctions by exchanging financial assets such as cash, gold, or cryptocurrency for high-value artwork or vice versa."[42] This interpretation introduces an intentional limitation to the use of the exemption. One cannot use the exemption opportunistically to evade sanctions through a cross-border transaction in preexisting informational materials if the purpose of that transaction is to exchange value with seeming indifference to the aesthetic or cultural value of the underlying informational materials.

(b) OFAC Licensing

There are two kinds of licenses: general and specific. OFAC often employs a combination of each to calibrate the breadth of a particular sanctions program.

General licenses. A general license is a published OFAC authorization covering any transaction that meets its stated conditions. General licenses are standing authorizations (albeit sometimes with an expiration date) that apply without any further government action. They typically relate to particularly important objectives, relationships, and humanitarian or civic values of the United States. They are also frequently used as temporary measures at the outset of a blocking order, providing U.S. persons with a limited period of time in which to wind down their activities with a blocked entity. Licenses may dictate the manner in which the licensed transactions can be performed, and they may require that certain notifications or reports be submitted to OFAC before, during, or after the licensed transactions.

OFAC normally publishes general licenses in the regulations of a particular economic sanctions program, although it sometimes publishes them as "freestanding" licenses in the Federal Register. In either situation, OFAC may first publish a general license on its website in order to make it immediately available in response to an urgent situation. The Venezuela

program is an example of a program where general licenses have been frequently used. In that context, OFAC has carved out many areas of allowable activity from its broader blocking measures, particularly the order applying to the government of Venezuela.

Some general licenses are required by statute. Most notably, Congress has adopted statutes that mandate certain licensing programs, such as section 906 of the Trade Sanctions Reform and Export Enhancement Act of 2000 (TSRA).[43] TSRA generally eliminated the authority to impose certain unilateral economic sanctions on exports of agricultural commodities, medicine, or medical devices to most countries, but directed the creation of a licensing program for exports of these items to certain targeted countries. OFAC has issued general licenses to ensure its programs are consistent with TSRA.

Finally, OFAC's regulations for most programs include general licenses permitting the provision of certain legal services for the benefit of Sanctions Targets. Among other limitations, such legal advice cannot facilitate targeted transactions in violation of U.S. economic sanctions, and there are strict limitations on how payment can be received for such legal advice. Consistent with such general licenses, OFAC has also issued guidance stating that U.S. persons can provide economic sanctions compliance advice concerning activity with Sanctions Targets.

Specific licenses. When general licenses or exemptions do not apply to a proposed activity, a person may seek a specific OFAC license. OFAC has discretion to issue or deny a specific license in response to a written application, which should contain the elements required by 31 C.F.R. § 501.801(b) of the Reporting, Procedures, and Penalties Regulations.[44] Licenses must be submitted through OFAC's web portal, using a prescribed form, available at https://ofac.treasury.gov/ofac-license-application-page.

While there is no required content for most specific license applications, successful requests generally (1) provide a comprehensive explanation of the facts, parties, and proposed transactions (explaining any technical terms that are unique to the type of transaction); (2) explain why OFAC has jurisdiction to issue the license; and (3) indicate why authorization of the requested transaction(s) would be consistent with U.S. economic sanctions policy, with the objectives of the relevant economic sanctions program or, if relevant, with a compelling national interest on which the U.S. government should act. It is also useful to include the precise language desired for the

text of the authorization, particularly where loose or nontechnical language may undermine the applicant's objectives.

OFAC generally will not issue a specific license involving novel circumstances without first receiving foreign policy guidance from the U.S. Department of State. Therefore, if a license application advocates that it be granted for foreign policy reasons, the party requesting the license should include information that would assist in the review by the State Department and may wish to contact the State Department separately.

Any person with an interest in the prohibited transaction may apply for a specific license. Unless otherwise specified in the license, anyone participating in a licensed transaction may rely on the terms of the specific license. Persons relying upon a specific license obtained by another person must ensure their own compliance with all license conditions, including any recordkeeping, reporting, or expiration provisions. Therefore, since OFAC generally will not provide copies of licenses to third parties, it is critical to obtain a copy of the relevant license directly from the named licensee and to review its text; determine its scope; and understand the conditions, expiration, and other requirements of the license. OFAC often issues specific licenses for a transaction "as described in the application"; in such cases, obtaining the application is also critical to a person's ability to reasonably rely on the OFAC license.

While some specific license requests take significantly longer, OFAC aims to process license requests within two to three months. There is no deadline for OFAC to take action on a license request. OFAC's current practice is to include an expiration date in any specific license, which is typically one to two years from the date of issuance but may be much shorter. OFAC may be responsive to a request for a period required to accomplish the licensed transactions.

Finally, for some situations, OFAC regulations or more informal communications include guidance on specific licensing policies for frequently encountered situations in which OFAC is prepared to grant specific licenses to resolve problems created by an economic sanctions program, such as a humanitarian crisis.

1.8 Risk of Providing Indirect Support to Sanctioned Targets

While most companies operating internationally have a heightened awareness that they cannot engage in direct activity with Sanctions Targets, and have controls to prevent such activities (such as screening), mitigating the risk of providing indirect support to Sanctioned Targets can be more challenging. This is both because the breadth of the law in this area is unclear, and because the nexus between any given commercial activity and a Sanctions Target can be hard to discern. An area of particular compliance focus is the prohibition on "facilitation."

(a) Facilitation/Indirect Services

Many economic sanctions programs administered by OFAC prohibit the exportation or re-exportation of services and facilitation. (The "exportation of services" is made directly from the United States, and the "re-exportation" of services occurs from a third country if those services originated in the United States.) In general, the restrictions on the exportation or re-exportation of services prohibit U.S. persons from providing services that generate a benefit that is received in a targeted country or by a targeted government. The restrictions on facilitation prohibit U.S. persons from facilitating any transaction by non-U.S. persons if U.S. economic sanctions would prohibit a U.S. person from directly participating in the same transaction.

Programs that include blocking prohibitions are also understood to implicitly encompass a prohibition on the export/re-export of services and facilitation related to Sanctions Targets, because those transactions would themselves be dealings in property (the export, re-export, or facilitation service) in which a Sanctions Target has an interest.

Since the act of facilitating a transaction essentially involves a service, the prohibitions in practice are essentially interchangeable. The concept of facilitation has a slightly different connotation, however, as it was intended to circumscribe acts that are ancillary, but critical, to moving a transaction forward. The prohibition first originated in the context of the Iranian sanctions to address the support that a U.S. parent company might provide its foreign subsidiaries (which at the time were not subject to the broad restrictions of that embargo).[45] The concept more broadly means to enable, or to support, a given transaction.

The Iran Transactions and Sanctions Regulations (ITSRs) contain the most detailed facilitation provision. Section 560.208 of the ITSRs provides that "no United States person, wherever located, may approve, finance, facilitate, or guarantee any transaction by a foreign person where the transaction by that foreign person would be prohibited . . . if performed by a United States person or within the United States." The ITSRs contain examples of conduct that fall within the scope of this prohibition, including (1) the referral of specific business opportunities with Iran to a foreign person; and (2) the institution by a U.S. person of changes in a foreign affiliate's operating policies to facilitate transactions that would be prohibited if performed by a U.S. person, even if such changes are not made in anticipation of any particular transaction involving Iran.

To the extent that "but for" a U.S. person's activity with a foreign entity that foreign entity would not be able to in turn conduct business with a Sanctions Target, there is some risk of a facilitation violation. A notable example in this context is that OFAC has made clear that for a U.S. parent to host an "automated and globally integrated computer, accounting, email, or other business support systems necessary to store, collect, transmit, generate, or otherwise process documents or information related to transactions" to a foreign person requires authorization under the Iran sanctions. (*See* Iran General License H.[46])

In sum, risk arises when there is a clear nexus between services offered by a U.S. person and a third-country entity's business with Sanctions Targets. If a U.S. person enables activity with a sanctioned target, then there is a facilitation risk.

Appendix B includes a more detailed discussion of considerations for multinational companies with respect to facilitation risk.

(b) The Limits on Indirect Risk

While broad, the breadth of the facilitation prohibition is not unlimited. Outside of the defined circumstances that secondary sanctions measures target, OFAC's regulations do not, as a general policy matter, prohibit U.S. persons from doing business with third-country entities that in turn do business with a Sanctions Target, as long as the U.S. person is not involved in that business, and as long as any connection is sufficiently attenuated.

One regulatory provision that has served as a broader guiding principle for when a link to a Sanctions Target is sufficiently attenuated is the so-called inventory rule in the ITSRs.

When a U.S. person engages in an international transaction for the sale of goods, technology, or services, he or she risks facilitating the resale and re-exportation of those goods, technology, or services in a subsequent transaction by the purchaser with a Sanctions Target or in an otherwise targeted transaction. Section 560.204 of the ITSRs provides that the "exportation, re-exportation, sale or supply of goods, technology or services to a third country is only prohibited when: (1) they are intended specifically to be directly or indirectly supplied, transshipped or re-exported to Iran or the Government of Iran or (2) they are intended specifically for use in the production of, commingling with or incorporation into goods, technology or services to be directly or indirectly supplied, transshipped or re-exported *exclusively or predominantly* to Iran or the Government of Iran" (emphasis added). The inventory rule allows U.S. persons to export or re-export to a third-country manufacturer or distributor if two conditions exist. First, the predominant business of the third-country manufacturer or distributor in the specific item to be exported or re-exported, or in goods produced from that item, must not be with Sanctions Targets. Second, the U.S. exporter or re-exporter must not have knowledge or notice that the specific item it is exporting to that third country is directly or indirectly destined for, or for the benefit of, a Sanctions Target. Under this rule, the original exportation is lawful even though the U.S. exporter or re-exporter may know that a minority of the items shipped could potentially come to rest in the sanctioned country.

The inventory rule arose from a perception that, to remain globally competitive, U.S. exporters must be allowed to do business with distributors and other importers in third countries, even if a third country has a different economic sanctions or foreign trade policy toward a U.S. targeted country. While OFAC has not expressly acknowledged that the principles underlying this rule can be applied in other sanctions programs, it is generally understood that it does, provided the reexport activity is not circumscribed by independent re-export restrictions in the EAR.[47] The general principle underlying this rule is that if a U.S. person's activity is not intended to support a Sanctions Target, but results in minor incidental benefit to a Sanctions Target, it is not prohibited.

1.9 Compliance Programs

OFAC regulations do not mandate compliance programs.[48] That said, a compliance program is critical to avoiding liability and to mitigating penalties that arise in an enforcement action.

In May 2019, OFAC issued *A Framework for OFAC Compliance Commitments*, a new guidance document outlining the key features of a sanctions compliance program. The Framework adopts key elements that are generally common to compliance programs, identifying five key elements: (1) a firm compliance commitment from management; (2) a risk assessment that serves as the basis for the company's compliance program; (3) internal controls, such as policies and procedures; (4) testing and auditing to evaluate the program's effectiveness on an ongoing basis; and (5) annual training for relevant employees, with more frequent training to be provided if required by the company's risk profile. The guidance builds upon OFAC's risk matrices, adopted by OFAC in 2006 and later affirmed in OFAC's Economic Sanctions Enforcement Guidelines, which provide guidance on how a financial institution can assess whether its business model presents low, moderate, or high sanctions risk.[49]

The Framework provides a particular emphasis on the importance of risk assessments; that is, a company's ability to effectively identify and address risks that result from its particular management structure, business partners, and business activities. Therefore, before a company designs and implements an economic sanctions compliance program, it should conduct a risk assessment. The Framework explains that, while there is no one-size-fits-all approach to conducting a risk assessment, OFAC has high expectations of how most companies should approach risk assessments.

The Framework is generally consistent with other government enforcement agency guidance in other compliance areas, such as anti-corruption. It includes some sanctions-specific perspectives however. The Framework identifies common root causes of noncompliance, including different standards and awareness between U.S. and non-U.S. business partners. The Framework also focuses on facilitation risks, noting that areas presenting a high risk of prohibited facilitation often result from the company's corporate and management structure as well as its provision of consolidated support functions, including human resources, information technology, and financial administration. Another notable observation is the

Framework's suggestion that compliance policies focus on influencing the behavior of counter-parties and encouraging compliant behavior by its agents, customers, and vendors.

1.10 Voluntary Self-Disclosures, Enforcement, and Penalties

When a compliance program fails to prevent a violation of U.S. economic sanctions, a company or an individual must decide whether to disclose the violation to OFAC. While circumstances may exist where a person may choose not to self-disclose, OFAC considers voluntary self-disclosures as a strong mitigating factor. Penalties are often significantly lower in enforcement actions where voluntary self-disclosures occur.

(a) Voluntary Self-Disclosures

OFAC's determination of whether a self-disclosure is "voluntary" depends largely on two factors. A self-disclosure is likely to be deemed voluntary if the disclosed information would not have otherwise been available to OFAC and if no other person had an obligation to report the information to OFAC. Pursuant to OFAC's Economic Sanctions Enforcement Guidelines, the potential civil penalty amount from the voluntary portion of a self-disclosure will be reduced by 50 percent.[50]

OFAC will not view a self-disclosure as "voluntary" if a mandatory report is required of, and is ultimately made by, another participant in a transaction (such as an intermediary bank in a funds transfer) or even if OFAC learns of the matter from another source, including another agency. Nevertheless, even in such cases, strong cooperation with OFAC may lead to very substantial (25%–40%) mitigation of the base amount of a penalty, pursuant to OFAC's Economic Sanctions Enforcement Guidelines.[51]

While OFAC does not prescribe the format for voluntary self-disclosures, a voluntary self-disclosure should provide OFAC the facts and context of a potential violation, including the parties and transactions involved, and the results of the transaction. When a determination is made to file a voluntary self-disclosure and an internal investigation will be required, it is generally advisable to notify OFAC of the potential violation as soon as it is discovered through an abbreviated initial filing that identifies the potential violation and states that further information will be

submitted in the future. This avoids the possibility that OFAC or a third party participant in the transaction will become aware of the issue and report it first, which could potentially destroy the "voluntary" nature of the self-disclosure and resulting mitigation.

If an abbreviated initial filing is submitted, OFAC requires that a final report containing full details required for the case's adjudication be submitted within "a reasonable time."[52] This time period depends on the circumstances; however, many practitioners apply a "rule of thumb" of 60 to 90 days after the initial filing absent special circumstances (which should be discussed on a continuing basis with the OFAC case agent). If the disclosing party is engaged in business where it is required to certify to potential customers that it has had no allegations or findings of legal violations, it may be helpful to request that no pre-penalty notice be issued and that settlement negotiations commence immediately. If a settlement is reached under this approach, OFAC's settlement agreement and website publicity will indicate no allegation or finding of violations and will speak in neutral terms of "apparent violations" (meaning "actual or possible") rather than "alleged violations" (meaning "alleged by OFAC").[53]

(b) Enforcement

An enforcement case for violations of U.S. economic sanctions may be triggered by a self-disclosure by a potential violator, by a report from a third party (private, state, federal or foreign), or by the U.S. government's own investigation. Federal criminal prosecutions for violations of U.S. economic sanctions are handled by the DOJ. However, OFAC's Economic Sanctions Enforcement Guidelines establish the procedures and concepts applicable to enforcement matters handled by OFAC. These guidelines provide a number of "general factors" used by OFAC to determine the gravity of a violation, including whether it is an "egregious case" deserving the maximum civil penalty available. The general factors also suggest certain mitigating or aggravating circumstances that OFAC will consider.

Where no self-disclosure has been received, an OFAC enforcement action typically starts with an administrative subpoena (also called a 602 request, from its regulatory citation, 31 C.F.R. § 501.602). A 602 request requires the recipient to provide a report with information and documents about a specific transaction or series of transactions. The subpoena specifies

the scope of information that the report should contain, the documents that must be submitted and the time period for response. Although it is very rarely exercised, OFAC also has the authority to require the recipient of the 602 request, also known as the respondent, to be present at a hearing. Failure to comply with a 602 request is itself a violation of OFAC's regulations and could result in a penalty.

If the respondent fails to answer or to cooperate in the investigation by OFAC's Sanctions Compliance & Evaluation Division (for financial institution respondents) or Enforcement Division (for other respondents), OFAC may send a pre-penalty notice to the respondent. The pre-penalty notice states the alleged violations (which may include failure to respond to a 602 request), the relevant general factors, the maximum penalty to which the respondent could be subjected, the civil penalty proposed for the respondent (based on the information then currently known to OFAC), and the deadline for a required response. The respondent may then respond to the pre-penalty notice's elements and furnish relevant documents to support its assertions before that deadline. For potential violations of IEEPA-based economic sanctions programs, the response will be due in 30 days. For violations of the TWEA-based program against Cuba, the response will be due in 60 days. (Either period may be extended for good cause.) The respondent can also contact OFAC to request that negotiations toward settlement of the allegations in the pre-penalty notice commence and that no final penalty notice be issued while those negotiations are continuing.

If OFAC does not receive a timely response to a pre-penalty notice from the respondent, OFAC will likely issue a final penalty notice requiring payment of the penalty amount proposed in the pre-penalty notice. For cases involving a violation of an IEEPA-based economic sanctions program, this final agency action triggers the right to appeal into the appropriate federal district court to challenge OFAC's determination. A request to OFAC for reconsideration is also possible. For violations of the TWEA-based program against Cuba, a respondent has a right to appeal to an administrative law judge, but the determination of that administrative law judge can be overturned by a non-OFAC Treasury Department official. The decision of that Treasury Department official constitutes a final agency action, which may be appealed to a federal district court.

(c) Penalties and Non-penalty Outcomes

Violations of U.S. economic sanctions are resolved through a combination of civil and criminal enforcement tools. On the civil side, OFAC's enforcement authority consists of the right to levy civil monetary penalties under the President's statutory authority to impose economic sanctions. This authority is found in IEEPA, TWEA, and special purpose economic sanctions statutes, such as the Foreign Narcotics Kingpin Designation Act (Kingpin Act).[54] Maximum civil penalties vary widely. For the Cuba program under TWEA, the maximum penalty per violation is $97, 529.[55] For IEEPA programs, the maximum penalty per violation is the greater of $330,947 or twice the value of the violative transaction.[56] Under the Kingpin Act, the maximum penalty is $1,644,396.[57] Each maximum penalty is annually updated to reflect inflation adjustments.

Additionally, the DOJ can initiate its own investigations and criminal prosecutions for violations of U.S. economic sanctions. Furthermore, OFAC and the other federal agencies with enforcement responsibility for violations of OFAC economic sanctions (such as the Department of Homeland Security's U.S. Customs and Border Protection, the Federal Bureau of Investigation, and the Department of Commerce's Office of Export Enforcement) can refer serious cases to the DOJ. As part of the adoption of CISADA, the criminal penalties for most U.S. economic sanctions violations were made uniform and now result in fines of up to $1 million and/or 20 years of imprisonment. (Maximum Kingpin Act fines are up to $10 million and/or 30 years of imprisonment.) Moreover, criminal prosecutions may result in the forfeiture of property involved in a violation.

Frequently, however, enforcement cases are resolved through the respondent's negotiation of a settlement with OFAC. These settlements can result in the payment of a settlement amount without a finding or admission of a violation. Other possible outcomes established in OFAC's enforcement guidelines include taking no action, cautionary letters warning the respondent to be more vigilant, a formal finding of a violation, or other administrative actions (such as a cease and desist order issued by OFAC or a denial, suspension, modification, or revocation of an OFAC license). OFAC will often publish a notice providing the public with the facts related to the violation, including mitigating and aggravating factors and any penalties paid.[58]

1.11 Conflicts with Non-U.S. Laws

As noted earlier, compliance with U.S. economic sanctions outside the United States may violate local non-U.S. laws in certain cases. These non-U.S. laws may prohibit discrimination based on nationality or prohibit the application of extraterritorial laws if they contravene domestic public policy. They also may specifically identify and prohibit compliance with particular U.S. economic sanctions laws and regulations.

These conflicts of law issues can be particularly problematic. The fact that compliance with U.S. economic sanctions may violate an applicable non-U.S. law does not, however, excuse noncompliance under U.S. law. The preamble to OFAC's Economic Sanctions Enforcement Guidelines states:

> OFAC does not agree that the permissibility of conduct under the applicable laws of another jurisdiction should be a factor in assessing an apparent violation of U.S. laws. In cases where the applicable laws of another jurisdiction require conduct prohibited by OFAC economic sanctions (or vice versa), OFAC will consider the conflict under [a general factor], which provides for the consideration of relevant factors on a case-by-case basis. OFAC notes that Subject Persons can seek a license from OFAC to engage in otherwise prohibited transactions and that the absence of such a license request will be considered in assessing an apparent violation where conflict of laws is raised by the Subject Person.[59]

While potentially applicable to any U.S. economic sanctions program, conflicts of law issues are particularly common in connection with the CACR and the ITSRs because of their explicit requirement for extraterritorial compliance by non-U.S. subsidiaries of U.S. firms.

In response to the United States' extraterritorial assertion of jurisdiction with respect to Cuba, the European Union, Canada, and Mexico adopted measures that prohibit compliance with U.S. economic sanctions against Cuba. Through the European Union's Council Regulation (EC) No. 2271/96 (EU Blocking Statute), Canada's Foreign Extraterritorial Measures Act (FEMA), Mexico's Law of Protection of Commerce and Investments from Foreign Policies that Contravene International Law (Antidote Law), and other related laws and implementing orders, these governments made it unlawful for persons in their territories to comply with certain aspects of the U.S. economic sanctions against Cuba. FEMA, the Antidote Law, and, to a lesser extent, the EU Blocking Statute require domestic government notification under certain circumstances (such as requests for cooperation with U.S. government investigations or requests by a U.S. parent company

that the non-U.S. subsidiary comply with U.S. economic sanctions against Cuba).

In 2018, the European Commission expanded the EU Blocking Statute to counteract the extraterritorial effects of the United States' reimposition of sanctions on Iran. After the United States announced in May 2018 that it would withdraw from the Iran nuclear deal (Joint Comprehensive Plan of Action) and reimpose sanctions on Iran, including secondary sanctions on non-U.S. persons who conduct business with or in Iran, the European Commission adopted an expanded Blocking Statute (Commission Delegated Regulation (EU) No. 2018/1100) forbidding EU persons from complying with U.S. sanctions on Iran, allowing EU economic operators to recover damages arising from U.S. extraterritorial sanctions, and nullifying the effect in the European Union of any foreign court rulings purporting to enforce U.S. sanctions on Iran.[60] Each EU member state is responsible for the implementation and enforcement of the amended EU Blocking Statute, including the application of penalties. Some member states have adopted more stringent measures than other states. These blocking laws are addressed in more detail in Chapter 9 of the Handbook.

The extraterritorial effect of the Trump administration's May 2019 announcement that it would cease waiving Title III of the 1996 Helms-Burton Act has also sparked an international response, particularly from the European Union and Canada. Under this action, U.S. citizens are now permitted to file lawsuits against companies that benefited from properties seized by the Cuban government. The EU Blocking Statute, as originally adopted, prohibited compliance and enforcement of the Helms-Burton Act, and the change in U.S. policy brings these provisions to life. The EU also threatened to seek further relief from the Trump administration's policy at the World Trade Organization. Similarly, under FEMA, the Canadian attorney general prohibited persons from complying with the Helms-Burton Act and authorized the imposition of significant fines for violations (up to approximately US$1.15 million per violation for corporations; approximately US$115,000 and five years in prison per violation for individuals). Canadian persons are also permitted to file counterclaims against Helms-Burton claimants in Canadian court.

While there is no fully effective resolution of these conflicts of law issues for multinational companies, more workable solutions are generally

customized and unique to the specific circumstances under which the conflicts arise.

---

1. David J. Ribner, Aysha Chowdhry, Mary Pat Dwyer, and Kristin Marshall provided substantial assistance in the preparation of this chapter. Mathew Tuchband also provided valuable input on later drafts. This chapter is based on a previous chapter drafted by J. Daniel Chapman and William B. Hoffman.

2. 50 U.S.C. §§ 1701–1706.

3. 15 C.F.R. 730–774; 50 U.S.C. §§ 4801–4852.

4. 50 U.S.C. §§ 4301 *et seq*.

5. 22 U.S.C. § 287c.

6. *See* § 101(b) of Pub. L. 95-223.

7. TWEA contains an identical exemption for trade in information. However, given TWEA's wartime applicability and the inherent need to restrict civilian travel during wartime, it provides no exemption transactions related to travel. Accordingly, restrictions on travel to Cuba continue.

8. *See* 50 U.S.C. § 1702(b)(1), (2).

9. 50 U.S.C. §§ 1601–1651.

10. These reports describe the executive orders and regulations issued to impose or modify economic sanctions programs, the litigation involving economic sanctions, the civil penalties collected, and the expense to the federal government of administering each economic sanctions program (other than the TWEA-based economic sanctions on Cuba). The initial reports and termination reports are published in the *Weekly Compilation of Presidential Documents*. From 1979 through the mid-1990s, that publication also contained the semiannual reports. However, following the delegation in the mid-1990s by the President to the Secretary of the Treasury for the preparation and filing of the semiannual reports, neither the administration nor Congress has made these semiannual reports available to the public.

11. 22 U.S.C. §§ 6021–6091.

12. *See, e.g.*, 31 C.F.R. § 585.101.

13. Pub. L. 111-195.

14. Pub. L. 108-175; 22 U.S.C. § 2151.

15. *See* U.S. Dep't of the Treasury, Office of Foreign Assets Control—Sanctions Programs and Information, https://ofac.treasury.gov/ (last visited April 16, 2023).

16. 50 U.S.C. § 1702(a)(1)(A).

17. *See, e.g.*, 31 C.F.R. §§ 595.315, 560.314.

18. The use of the term "person" in this chapter refers to organizations, entities, and natural persons unless indicated otherwise. The term "United States person" is abbreviated in most economic sanctions literature and will be referenced in this chapter as simply "U.S. person." Furthermore, for ease of reference, the use of the term "U.S. person" in this chapter refers to all parties that must comply with U.S. economic sanctions (such as persons subject to the jurisdiction of the United States, except as noted in discussions of the unique extraterritorial issues implicated in the U.S. economic sanctions program for Cuba).

19. Such facilitation can be prohibited explicitly (*see, e.g.*, 31 C.F.R. § 560.208) or considered a prohibited dealing in property (which includes services) in which a sanctions target has an interest (*see, e.g.*, 31 C.F.R. §§ 541.201, 541.308, 541.405).

20. IEEPA contains statutory authority for such in rem jurisdiction. 50 U.S.C. § 1702(a)(1)(A) applies ". . . with respect to any property subject to the jurisdiction of the United States." Some sanctions programs, most notably the Iran program, include restrictions that reach non-U.S. persons transactions with U.S.-origin goods outside of the United States. Most sanctions policy with respect to such goods outside the United States, however, is reflected in the export control laws of the

Department of Commerce's EAR, which regulates the export and re-export of all U.S.-origin goods, but focuses primarily on dual-use goods.

21. United States v. McKeeve, 131 F.3d 1 (1st Cir. 1997).

22. Credit Suisse Deferred Prosecution Agreement (Dec. 16, 2009), exhibit A, para. 14.

23. Lloyds TSB Deferred Prosecution Agreement (Jan. 9, 2009), exhibit A, para. 11.

24. Barclays Bank Plc. Deferred Prosecution Agreement (Aug. 16, 2010), exhibit 1, para. 20.

25. 50 U.S.C. § 1705(a) (emphasis added).

26. *See* 31 C.F.R. § 515.329(d).

27. Pub. L. 112-158.

28. Although sanctions could be applied to the broader "persons subject to U.S. jurisdiction" as discussed earlier, this discussion will focus on the much more common application to "U.S. persons."

29. *See, e.g.*, 31 C.F.R. § 594.201.

30. *Id*. § 594.203.

31. *Id*. § 515.311.

32. *Id*. § 594.309.

33. Pub. L. 107-56.

34. 31 C.F.R. § 501.603.

35. *Id*. § 501.604(a)(3).

36. *See* https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#ukraine, FAQ 371 (last visited Dec. 5, 2022).

37. *See* E.O. 14071, E.O. 14068, and E.O. 14066, and Appendix A for more details.

38. E.O. 13835.

39. *See* https://www.state.gov/venezuela-related-sanctions/.

40. 18 U.S.C. ch. 37.

41. *See, e.g.*, the ITSRs, 31 C.F.R. § 560.210(c).

42. *Advisory and Guidance on Potential Sanctions Risks Arising from Dealings in High-Value Artwork*, Oct. 30, 2020.

43. Title IX of Pub. L. 106-387.

44. 31 C.F.R. pt. 501.

45. A U.S. parent's mere receipt of information (such as receiving written reports on pending or completed transactions that are targeted by U.S. economic sanctions) does not cause a facilitation violation. However, a violation would occur if a U.S. person used that information to approve or support targeted transactions or activities. *See* 31 C.F.R. § 538.407(a).

46. General License H was revoked when the United States withdrew from the JCPOA. However, the fact that OFAC believed it was necessary to authorize such automated business support systems based in the United States in that context indicates that OFAC would likely consider the provision of such U.S.-based automated activity to constitute prohibited indirect services or facilitation in the context of comprehensive sanctions programs generally.

47. The EAR imposes a re-export license requirement on most shipments of EAR99 items (which are items not listed on the Commerce Control List) to embargoed countries other than Iran (Cuba, North Korea, Syria, and the Crimea, Donetsk, and Luhansk regions of Ukraine). As such, re-exports by non-U.S. companies of virtually all U.S. origin items subject to the EAR (except food, medicine, and medical devices) are separately prohibited for Cuba, North Korea, Syria, and the Crimea, Donetsk, and Luhansk regions of Ukraine.

48. Most financial institutions are required to have economic sanctions screening programs under separate money laundering regulations however.

49. 31 C.F.R. pt. 501, app. A.

50. *See* Base Penalty Matrix at 31 C.F.R. pt. 501, app. A(V)(B)(2)(a).

51. 31 C.F.R. pt. 501, app. A(V)(B)(2)(b)(i).

52. *Id*. pt. 501, app. A(I)(I).

53. *See id*. pt. 501, app. A(I)(A) (definition of "apparent violation").

54. 21 U.S.C. §§ 1901–1908. The UNPA provides only for criminal penalties.

55. 31 C.F.R. pt. 501, app. A(V)(B)(2)(a); *see also* 50 U.S.C. app. 16(b) *as modified in accordance with* Pub. L. 101-410 (1990), 28 U.S.C. § 2461 note; reflected in 31 C.F.R. § 501.701.

56. 31 C.F.R. pt. 501, app. A(V)(B)(2)(a); *see also* 50 U.S.C. § 1705 *as modified in accordance with* Pub. L. 101-410 (1990), 28 U.S.C. § 2461 note; typically reflected in section 701 of each set of IEEPA-based sanctions regulations; *see, e.g.*, Iran penalties at 31 C.F.R. § 560.701.

57. 31 C.F.R. pt. 501, app. A(V)(B(2)(a); *see also* 21 U.S.C. § 1906(b) *as modified in accordance with* Pub. L. 101-410 (1990), 28 U.S.C. § 2461 note; reflected in 31 C.F.R. § 598.701.

58. For example, in a December 2020 enforcement action against a California-based technology company, OFAC detailed the "conduct leading to the apparent violations," aggravating and mitigating factors, and details of the penalty calculation. OFAC, BitGo, Inc. Settlement, Dec. 30, 2020, https://ofac.treasury.gov/media/50266/download?inline. OFAC's enforcement actions can be found at https://ofac.treasury.gov/civil-penalties-and-enforcement-information.

59. 74 Fed. Reg. 57593 at 57599 (Nov. *9, 2009)*.

60. *See also* Commission Implementing Regulation (EU) 2018/1101; Guidance Note, Questions and Answers: Adoption of Update of the Blocking Statute (2018/C 277 I/03), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.CI.2018.277.01.0004.01.ENG&toc=OJ:C:2018:277I:TOC (last visited Dec. 5, 2022).

Appendix A

Chart of Country/Territory Programs

U.S. Economic Sanctions Currently in Place (as of July 22, 2022)

China

China has recently been targeted by a variety of U.S. economic sanctions measures in response to the country's interference in Hong Kong, see, for example, E.O. 13936, Hong Kong Autonomy Act (HKAA) (P.L. 116-149), and human rights abuses against Muslim ethnic minorities in the Xinjiang province in northwest China, see, for example, E.O. 13818, Uyghur Human Rights Policy Act of 2020 (P.L. 116-145). These measures include SDN designations and restrictions on U.S. travel. A newly enacted U.S. law (HKAA) also authorizes OFAC to impose secondary sanctions on foreign financial institutions that conducted a significant transaction with certain individuals designated by the State Department. The U.S. also restricts dealing in the securities of certain Chinese companies identified as operating in the defense and related material sector or the surveillance technology sector of the PRC economy.

Other U.S. federal agencies have also taken actions targeting certain exports and re-exports, suspending the Fulbright exchange program with regard to China and Hong Kong, and suspending preferential treatment for Hong Kong under U.S. trade laws.

Primary sanctions apply to:

- U.S. entities
- U.S. citizens
- U.S. permanent residents
- Persons in the United States
- Foreign branches of U.S. entities

Principal Prohibitions	Select Exemptions and Observations
Primary • Any transaction involving publicly traded securities, derivatives of such securities, or any securities designed to provide investment exposure to such securities of companies determined to be operating in the defense and related material sector and	

surveillance technology sector of the PRC economy (E.O. 14032, 31 C.F.R. 586)

- The following persons may be designated as SDNs:
  - Persons determined to be involved, directly or indirectly, in the coercing, arresting, detaining, or imprisoning of individuals under the authority of, or to be or have been responsible for or involved in developing, adopting, or implementing, the China National Security Law (E.O. 13936)
  - Persons who with respect to Hong Kong are determined to be responsible for, complicit in, or to have engaged in (1) actions or policies that undermine democratic processes or institutions; (2) actions or policies that threaten the peace, security, stability, or autonomy; (3) censorship that restricts the exercise of freedom of expression or assembly or that limits access to free and independent print, online, or broadcast media; or (4) extrajudicial rendition, arbitrary detention, or torture or other gross violations of internationally recognized human rights or serious human rights abuse (E.O. 13936)
  - Persons determined to be leaders or officials of entities, including government entities, that have engaged in or supported the preceding activities, which are owned or controlled by or have acted on behalf of entities designated under this sanctions authority, or who are members of the board of directors or a senior executive officer of entities designed under this sanctions authority (E.O. 13936)
  - Persons who are materially contributing to, have materially contributed to, or attempts to materially contribute to the failure of the government of China to meet its international obligations regarding Hong Kong as identified by the State and Treasury Departments (Hong Kong Autonomy Act (HKAA))
  - Persons responsible for or complicit in, or have directly or indirectly engaged in, serious human rights abuses (E.O. 13818)

Secondary

• Foreign financial institutions that knowingly conduct a significant transaction with a foreign person identified by the State and Treasury Departments pursuant to the HKAA (HKAA)	

Cuba

U.S. measures against Cuba are implemented under the United States' most long-standing comprehensive country-based program, and which is authorized under the Trading with the Enemy Act. In 2014, the Obama administration moved to normalize relations with Cuba, lifting select U.S. sanctions against the country. In 2017, the Trump administration rolled back some of the Obama administration's efforts to normalize relations with Cuba and introduced new sanctions. The Trump administration imposed additional sanctions in 2019 and 2020 in response to the Cuban government's support of Nicolas Maduro's regime in Venezuela and human rights abuses carried out by the Cuban regime. The Trump administration also relisted Cuba as a State Sponsor of Terrorism in January 2021.

Primary sanctions apply to:

- U.S. entities
- U.S. citizens
- U.S. permanent residents
- Persons in the United States
- Foreign branches of U.S. entities
- Foreign entities that are owned/controlled by U.S. persons (subsidiaries of U.S. entities)
- Foreign entities/persons involved in a transaction of property subject to U.S. jurisdiction

15 C.F.R. Part 746
31 C.F.R. Part 515

Principal Prohibitions	Select Exemptions and Observations
Primary • Exports or re-exports of goods, technology, and services (sections 515.201, 746.1(1), and 746.2) • Direct and indirect imports from Cuba (section 515.204) • Transactions involving property in which Cuba or a Cuban national has an interest (sections 515.201 and 515.202) • Transactions with Cuban nationals, even those not physically located in Cuba (section 515.201) • Cuban property in possession/control of a U.S. person is blocked (section 515.205) • Travel to Cuba without a license (section 515.420) • Approval or facilitation of transactions by non-U.S. persons that are prohibited as to U.S. persons (section 515.201)	• General observation: specific licenses and, in some cases, general licenses are available for certain activities. Both the Office of Foreign Assets Control (OFAC) and the Bureau of Industry and Security (BIS) continue to regulate in this area, and both sets of rules need to be consulted in determining whether a particular activity will qualify for a specific or general license. • Some areas of activity that may be subject to a license include infrastructure projects (except tourism-related infrastructure), healthcare, sanitation, and activity that fosters the Cuban private sector. Some other specific areas are: • Transactions related to the dissemination of informational materials (sections 515.206 and 515.545)

• Transactions with entities and sub-entities identified on the State Department's Cuba Restricted List (section 515.209) • Processing remittances through any entity on the Cuba Restricted List (31 C.F.R. 515.421) • Transactions involving "U-turn transactions" (section 515.584(d)) • Transactions with entities identified on the State Department's Cuba Prohibited Accommodations List (section 515.210) • License is required for the export of all items subject to the EAR, with certain exceptions (section 746.2) • Exports from a third country of a foreign-made product with more than 10 percent controlled de minimis U.S. content (15 C.F.R. part 734) **Secondary** • N/A	• Transactions ordinarily incident to a licensed transaction, with certain exceptions (section 515.421) • Certain transactions relating to intellectual property (section 515.527) • Transactions incident to the exportation of items from the United States or the re-exportation of items from a third country, with certain exceptions (section 515.533) • Transactions incident to the establishment of facilities to provide telecommunications services linking the United States and Cuba (section 515.542) • Travel to Cuba within 12 existing travel categories, such as educational, journalistic, and religious activities, without case by case specific licensing (section 515.560) • Travel to Cuba for group people to people education and other academic educational activities (section 515.565) • Provision of authorized travel and carrier services by travel agents and airlines (section 515.572) • Export of certain services incident to internet-based services (section 515.578) • Physical presence and operations in Cuba in support of authorized activities (section 515.573) • Use of U.S. credit and debit cards in Cuba for authorized travel-related transactions (section 515.584)

Iran

Since 1995, the United States has maintained comprehensive economic sanctions against Iran. These sanctions are implemented through the Iranian Transactions and Sanctions Regulations (the ITSRs, or Regulations, 31 C.F.R. part 560). The United States has also imposed secondary sanctions against Iran in response to its nuclear weapons program and malign activities. Under the Joint Comprehensive Plan of Action ("Iran Nuclear Deal"), the United States lifted some of its primary and secondary sanctions against Iran in January 2016. In May 2018, President Trump withdrew the United States from the Iran Nuclear Deal and reimposed nearly all sanctions that had been lifted under the Iran Nuclear Deal. Thereafter, the Trump administration issued additional sectoral sanctions to target various aspects of Iran's economy, including Iran's construction, mining, manufacturing, energy, and financial sectors. The Biden administration is engaging in negotiations with Iran related to restarting the Nuclear Deal, but no agreement has been reached at present.

Primary sanctions apply to:

- U.S. entities
- U.S. citizens
- U.S. permanent residents
- Persons in the United States

- Foreign branches of U.S. entities
- A U.S. parent may be sanctioned for actions of controlled foreign subsidiaries in Iran prohibited as to the parent company
- Foreign persons are subject to controls on U.S. goods and technology and may not procure U.S.-based services for activity in Iran

31 C.F.R. Part 560
15 C.F.R. Part 746 (export controls)

Principal Prohibitions	**Select Exemptions and Observations**
Primary • Direct or indirect exports or re-exports to Iran or the government of Iran of goods, technology (including technical data or other information subject to the Export Administration Regulations (EAR)), or services (including brokerage) from the United States or by a U.S. person wherever located (section 560.204) • Exports or re-exports of goods, technology, or services from the United States to a third country with knowledge or reason to know that the goods are intended for Iran or that the third country entity sells predominantly to Iran (section 560.204) (predominant sales exist where Iran is the largest market for that entity) • Direct or indirect imports of goods or services of Iranian origin (section 560.201) • Dealing abroad. Transactions or dealings by U.S. persons, wherever located, in goods, technology, or services of Iranian origin, or goods, technology, or services directly or indirectly destined for Iran or the government of Iran (section 560.206) • Transshipment of goods through Iranian territory to third countries (section 560.403) • New investments in Iran and property or entities owned by the government of Iran (section 560.207) • Approval, financing, facilitation, or guaranteeing of transactions by U.S. persons for transactions by non-U.S. persons that are prohibited as to U.S. persons (sections 560.208 and 560.417) • Actions designed to evade the sanctions (section 560.203(a))	• Imports or exports of gifts valued at $100 or less (section 560.506) • Imports or exports of information or informational materials (section 560.210(c)) • Personal communication, which does not involve the transfer of anything of value (section 560.210(a)) • Re-exports by non-U.S. persons of low-level goods or technology to Iran, provided that the goods were not exported to a third country for the purpose of re-exporting the goods to Iran, and provided the goods are not subject to U.S. export licensing requirements (sections 560.204 and 560.205) • Re-exports from a third country to Iran by non-U.S. persons of U.S. goods or technology that have been substantially transformed into a foreign-made product outside the United States (section 560.205(b)(1)) • Re-exports from a third country to Iran by non-U.S. persons of foreign-made products containing de minimis (below 10 percent) levels of “controlled” U.S. content (sections 560.205(b)(2) and 560.420) • Certain transactions related to patents, trademarks, and copyrights (section 560.509) • Exportation of certain medicine and medical supplies (section 560.530(a)(3)(i)) • Exportation of certain agricultural commodities (section 560.530(a)(2)(i)) • Certain transactions related to humanitarian efforts (Gen. License 8A; see also section 560.210(b)) • Transactions involving Iranian financial institutions designated pursuant to E.O. 13902 that are authorized, exempt, or otherwise not prohibited under the Iranian

• Exports from a third country of a foreign-made product with more than 10 percent controlled U.S. content (15 C.F.R. part 736) • Significant transactions by U.S. persons related to the iron, steel, aluminum, or copper sectors of Iran (E.O. 13871) • Significant transactions by U.S. persons related to the construction, mining, manufacturing, textiles, or financial sectors of the Iranian economy (E.O. 13902; *see also* https://ofac.treasury.gov/recent-actions/20201008) • Transactions involving the purchase of certain oil, petroleum, or petrochemical products from Iran or transactions with the National Iranian Oil Company or Naftiran Intertrade Company (E.O. 13622, E.O. 13846) • Transactions with Iranian Specially Designated Nationals and Blocked Persons (SDNs), including but not limited to Iranian government entities • **Iran Sanctions Act (as amended, 50 U.S.C. 1701 App.) makes 31 C.F.R. part 560 applicable to all entities controlled by U.S. persons** • Subjects to sanctions U.S. persons who engage in trade with Iran with respect to the procurement of Iranian petrochemical products and the supply to Iran of petrochemical products above certain dollar thresholds **Secondary** U.S. secondary sanctions generally fall into two categories. First, those aimed at hindering Iran's revenue generating capacity, such as: • Significant transactions, by non-U.S. persons, related to the iron, steel, aluminum, copper, construction, mining, manufacturing, textiles, or financial sectors of Iran (E.O, 13871, E.O. 13902; *see also* https://ofac.treasury.gov/recent-actions/20201008) • Any person that, on or after August 7, 2018, knowingly engages in any significant financial transaction for the sale, supply, or transfer to Iran of significant goods or	Transactions and Sanctions Regulations (Gen. License L)

services used in connection with the automotive sector of Iran (E.O. 13846)

- Any person that, on or after November 5, 2018, knowingly engages in any significant financial transaction for the purchase, acquisition, sale, transport, or marketing of petroleum, petroleum products, or petrochemical products from Iran (E.O. 13846)
- Any person that materially assists, sponsors, or provides financial, material, or technological support for, or goods or services in support of, the purchase or acquisition of U.S. bank notes, precious metals, precious stones, or precious jewels by the government of Iran (E.O. 13846, E.O. 13645)
- Any person who knowingly provides significant financial, material, technological, or other support to, or goods or services in support of, any activity or transaction on behalf of designated persons involved in the energy, shipping, or shipbuilding sectors of Iran (E.O. 13846)
- Any person who knowingly engages in the sale, supply, or transfer to or from Iran of raw and semi-finished metals, graphite, coal, and software for integrating industrial processes to be used in connection with the construction sector in Iran or certain strategic materials designated by the State Department (Iran Freedom and Counter Proliferation Act of 2012, P.L. 112-239, sections 1245–1246)
- Any foreign financial institution who knowingly conducts or facilitates any significant financial transaction involving various aspects of the Iranian economy, including but not limited to:
  - significant goods or services used in connection with iron, steel, aluminum, or copper sectors of Iran, or for or on behalf of any person whose property and interests in property are blocked pursuant to E.O. 13871 (E.O. 13871)
  - significant goods or services used in connection with the construction, mining, manufacturing, or textiles sectors of the Iranian economy, or for or on behalf of any person whose property and interests in

property are blocked pursuant to E.O. 13902 (E.O. 13902) – the sale, supply, or transfer to Iran of significant goods or services used in connection with the automotive sector of Iran, on or after August 7, 2018 (E.O. 13846) – the purchase, acquisition, sale, transport, or marketing of petroleum, petroleum products, or petrochemical products from Iran, on or after November 5, 2018 (E.O. 13846) – the purchase or sale of Iranian rials, or any financial institution that maintains significant funds outside of Iran denominated in Iranian rial on or after August 7, 2018 (E.O. 13846) Second, those responding to the regime's malign activities, including: • Any entity or person who facilitates or finances a transaction involving the supply, sale, or transfer, directly or indirectly, to or from Iran, or for the use in or benefit of Iran, of arms or related material, including spare parts (E.O. 13949) • Any foreign financial institution that conducts significant transactions with the Islamic Revolutionary Guard Corps or any of its agents or affiliates sanctioned by the United States (Comprehensive Iran Sanctions, Accountability, and Divestment Act, P.L. 112-239, section 104) • Any foreign financial institution that facilitates the government of Iran's efforts to acquire or develop weapons of mass destruction or delivery systems, or to provide support for organizations designated as foreign terrorist organizations (Comprehensive Iran Sanctions, Accountability, and Divestment Act, P.L. 112-239, section 104)	

North Korea

The United States has imposed comprehensive sanctions against North Korea, restricting most trade in goods and services, financial transactions, and arms sales and transfers. New U.S. investment in North Korea is also prohibited. During his term, President Trump imposed a variety of secondary sanctions to in response to certain North Korea actions.

Primary sanctions apply to:

- U.S. entities

- U.S. citizens
- U.S. permanent residents
- Persons in the United States
- Foreign branches of U.S. entities
- Foreign persons subject only to controls on U.S. goods

31 C.F.R. Part 510
15 C.F.R. Part 746 (export controls)

Principal Prohibitions	Select Exemptions and Observations
Primary • Property blocked as of June 16, 2000, remains blocked (dection 510.201(a)(2)) • Transactions with North Korean vessels are prohibited, as are transactions with persons involved in the North Korean regime's illicit activities (sections 510.207, 510.201(a)(3)) • Imports of North Korean-origin goods (including indirect) without OFAC's prior approval (31 C.F.R. section 500.586(a)) • Exports of goods, services, and technology by a U.S. person to North Korea (section 510.206) • New investment in North Korea by U.S. persons without a license (section 510.209) • Approval, financing, facilitation, or guarantee by a U.S. person of a transaction by a foreign person (section 510.211) • Funds that pass through a foreign bank account owned, controlled, or used by a North Korean person required to be blocked by U.S. financial institutions (section 510.210) **Secondary** • Any person who operates in the construction, energy, financial services, fishing, information technology, manufacturing, medical, mining, textiles, or transportation industries in North Korea (section 510.201(a)(3)(v)(A)) • Any person who owns, controls, or operates any port in North Korea, including any seaport, airport, or land port of entry (section 510.201(a)(3)(v)(B)) • Any person who has engaged in at least one significant importation from or exportation to North Korea of any goods, services, or technology (section 510.201(a)(3)(v)(C)) • Any foreign financial institution that	• Imports of items from North Korea into the United States with OFAC's permission (section 510.205(b)(2)) • Any transaction necessary to comply with U.S. obligations under international agreements (section 510.213(f)) • Activities subject to the reporting requirements under the National Security Act of 1947 or to any authorized intelligence activities of the United States (section 510.213(f))

knowingly conducts or facilitates any significant transaction with a blocked North Korean person or any transaction in connection with trade with North Korea (section 510.210(b)) • Any person involved in certain North-Korea-related activities, including persons who, directly or indirectly, maintain a correspondent account with any North Korean financial institution, except as specifically approved by the United Nations Security Council (section 510.201(a)(3)(vii)(N)), and persons who, directly or indirectly, import, export, or re-export luxury goods to or into North Korea (section 510.201(a)(3)(vii)(D)) • Any foreign financial institution that, on or after April 18, 2020, knowingly provides significant financial services to any person designated for the imposition of sanctions with respect to North Korea (section 510.210(c))	

Specially Designated Nationals and Blocked Persons

OFAC designates sanctions targets for inclusion on its SDN list. Individuals from the following countries and programs are currently listed on the SDN list:

Afghanistan, Balkans, Belarus, Burma, Central African Republic, China, Cuba, Democratic Republic of the Congo, Ethiopia, Hong Kong, Iran, Iraq, Lebanon, Libya, Mali, Nicaragua, North Korea, Russia, Somalia, South Sudan, Sudan, Syria, Ukraine, Venezuela, Yemen, Zimbabwe, terrorists, rough diamond traders, cyberattackers, narcotics traffickers, human rights violators, actors involved in corruption, transnational criminal organizations, weapons of Mass destruction proliferators, foreign interferers in U.S. elections

Primary sanctions apply to:

- U.S. entities
- U.S. citizens
- U.S. permanent residents
- Persons in the United States
- Foreign branches of U.S. entities
- For Cuba and Iran, foreign subsidiaries of U.S. firms

Various executive orders and regulations. List is maintained by OFAC at https://sanctionssearch.ofac.treas.gov/.

Principal Prohibitions	Select Exemptions and Observations
Primary • Transfer of assets and property in which such persons/entities have an interest	• Transactions involving the export or import of informational materials are permitted (see, e.g., section 542.206(b))

• Financial or technical assistance to these persons/entities • Dealings or any business transactions with these persons/entities • Approval or facilitation of transactions by non-U.S. persons that are prohibited as to U.S. persons • Actions designed to evade the sanctions • **Any entity owned 50 percent or more by a blocked entity is also automatically blocked by operation of law** **Secondary** • May apply to significant transactions involving SDNs, particularly those in Iran or Russia	• Transactions involving humanitarian, safety, and sanitation-related goods and services to certain SDNs (see, e.g., OFAC FAQ 830–33)

Syria

The United States has maintained a comprehensive program against Syria since 2011. Prior to that point there had been targeted sanctions stemming from Syria's designation as a state sponsor of terrorism, as well as strict export controls since 2004.

More recently, in June 2020, the Trump administration issued regulations pursuant to the Caesar Syria Civilian Protection Act (P.L. 116-92, sections 7411–7413), named for a photographer who documented the Syrian regime's torture against civilians. The Caesar Act authorized the President to imposed various secondary sanctions.

Primary sanctions apply to:

- U.S. citizens
- U.S. entities
- U.S. permanent residents
- Persons in the United States
- Foreign branches of U.S. entities

31 C.F.R. Part 542
15 C.F.R. Part 746 (export controls)

Principal Prohibitions	**Select Exemptions and Observations**
Primary • All transactions with the government of Syria are prohibited as to U.S. persons • All imports, transactions, and dealing of Syrian petroleum or petroleum products are prohibited (sections 542.208 and 542.209) • The export of services to Syria are prohibited as to U.S. persons (section 542.207) • All investment in Syria is prohibited as to U.S. persons (section 542.206)	• Personal communications and informational materials are exempt (section 542.211) • Transactions necessary and ordinarily incident to publishing (section 542.532) • Authorizes transactions related to the prevention, diagnosis, and treatment of Covid-19 through June 17, 2023 (Gen License 21A)

- Facilitation of transactions by non-U.S. persons that are prohibited as to U.S. persons (section 542.210)
- Prohibition on export to Syria of all items on the Commerce Control List and the export to Syria of products of the United States, other than food and medicine (section 746.9)
- Exports from a third country of a foreign-made product with more than 10 percent controlled U.S. content (15 C.F.R. part 736)

Secondary

- Any foreign person who knowingly provides significant financial, material, or technological support to, or knowingly engages in a significant transaction with the government of Syria (including any entity owned or controlled by the government of Syria); a foreign person that is a military contractor, mercenary, or a paramilitary force knowingly operating in a military capacity for or on behalf of the government of Syria, Russia, or Iran; or a foreign person subject to sanctions with respect to Syria (Caesar Syria Civilian Protection Act, P.L. 116-92, section 7412(a)(2)(A))
- Any foreign person who knowingly sells or provides significant goods, services, technology, information, or other support that significantly facilitates the maintenance or expansion of the government of Syria's domestic production of natural gas, petroleum, or petroleum products (P.L. 116-92, section 7412(a)(2)(B))
- Any foreign person who knowingly sells or provides aircraft or spare aircraft parts that are used for military purposes in Syria for or on behalf of the government of Syria to any foreign person operating in an area directly or indirectly controlled by the government of Syria or foreign forces associated with the government of Syria (P.L. 116-92, section 7412(a)(2)(C))
- Any foreign person who knowingly provides significant goods or services associated with the operation of aircraft that are used for military purposes in Syria for or on behalf of the government of Syria to any foreign person operating in an area

described in section 7412(a)(2)(C) (P.L. 116-92, section 7412(a)(2)(D)) • Any foreign person who knowingly, directly or indirectly, provides significant construction or engineering services to the government of Syria (P.L. 116-92, section 7412(a)(2)(E))	

Ukraine/Russia

In 2014, the United States imposed sanctions on Russia and certain persons in Ukraine in response to Russia's occupation and annexation of Crimea, a region in Ukraine. The program was later expanded in 2017 under the Countering America's Adversaries Through Sanctions Act (CAATSA) (P.L. 115-44), which imposed additional sanctions in response to Russia's involvement in the Syrian civil war, interference with the 2016 U.S. election, and poisoning of a former agent. In 2022, in response to Russia's invasion of Ukraine and occupation of the Donetsk and Luhansk regions of Ukraine, the United States imposed additional sanctions, largely in coordination with its allies. Today, the United States' comprehensive program against Russia includes both primary and secondary sanctions, sectoral sanctions to target specific aspects of the Russian economy, and bans on investment in Russia, the provision of certain services in Russia, and the import from and export to Russia of various products.

As well, there are comprehensive sanctions applicable to the Crimea, Donetsk, and Luhansk regions of Ukraine.

Primary sanctions apply to:

- U.S. entities
- U.S. citizens
- U.S. permanent residents
- Persons in the United States
- Foreign branches of U.S. entities
- Foreign persons are subject to controls on U.S. goods and technology

15 C.F.R. Part 746
31 C.F.R. Part 587
31 C.F.R. Part 589

Principal Prohibitions	Select Exemptions and Observations
Primary • All transactions with designated blocked persons and entities deemed to be contributing to the situation in Ukraine (sections 589.201 and 587.201) • All new investment in the Crimea, Donetsk, and Luhansk regions of Ukraine by a U.S. person (E.O. 13685, E.O. 14065) • The importation into the U.S., directly or indirectly, of any goods, services, or technology from the Crimea, Donetsk, and Luhansk regions of Ukraine (E.O. 13685, E.O. 14065)	• General observations: The Russian sanctions operate on many levels targeting the political leadership of Russia; oligarchs and their families; and financial, defense, and energy sectors of the Russian economy. Commercial activity in Russia is permitted generally. However, major Russian companies, including most large Russian financial institutions, are subject to sanctions, which create significant practical and legal challenges to conducting business in Russia. Diligence is warranted to ensure that there is no inadvertent conflict with

- The export, sale, or supply, directly or indirectly, from the U.S. or by a U.S. person of any goods, services, or technology to the Crimea, Donetsk, and Luhansk regions of Ukraine (E.O. 13685, E.O. 14065)
- Any financing, facilitation, or guarantee by a U.S. person of a transaction by a foreign person, where the transaction would be prohibited if performed by a U.S. person or in the United States (E.O. 13685, E.O. 14065)
- U.S. banks are prohibited from participating in the market for non-ruble denominated bonds issued by any Russian government entity and from lending non-ruble denominated funds to any Russian government entity (E.O. 13883)
- Transactions involving the sale of arms (83 Fed. Reg. 43723)
- Transactions financing the Russian military (83 Fed. Reg. 43723)
- New investments in the Russian Federation by a U.S. person, wherever located (E.O. 14071)
- Export, sale, or supply from the United States or by a U.S. persons, wherever located, of certain services to Russia. At present, the prohibitions apply to the provision of services related to accounting, trust and corporation formation, and management consulting (E.O. 14071). The prohibition does not apply to the provision of such services to entities in Russia owned or controlled by U.S. persons or in connection with a wind down or divestiture of an entity in Russia owned or controlled by a non-Russian person (determination pursuant to section 1(a)(ii) of E.O. 14071).
- Ban on the import into the United States of the following products from Russia: gold, crude oil, petroleum, petroleum fuels, oils and related distilled products, liquefied natural gas, coal and coal products, fish and seafood, alcohol, and nonindustrial diamonds (E.O. 14068, E.O. 14066)
- Ban on the export to Russia of luxury goods and U.S. dollar denominated banknotes (E.O. 14068)
- All items (goods, software, technology) specifically described on the Commerce these rules, many of which target specific entities, but some of which relate more broadly to the energy sector.
- The sanctions with respect to the Crimea, Donetsk, and Luhansk regions of Ukraine are comprehensive, with a few narrowly tailored exemptions and general licenses. Crimea,- Donetsk-, and Luhansk-related exemptions:
  - Export of agricultural commodities, medicine, medical supplies, and replacement parts to Crimea, Donetsk, and Luhansk regions of Ukraine (section 589.513, Ukraine Gen. License 18)
  - Transactions related to telecommunications and mail to Crimea, Donetsk, and Luhansk regions of Ukraine (section 589.516, Ukraine Gen. License 19)
- Other Russia sanctions exemptions:
  - Transactions related to energy involving one or more the following entities are authorized (Russia-related Gen. License No. 8C):
    1. State Corporation Bank for Development and Foreign Economic Affairs Vnesheconombank
    2. Public Joint Stock Company Bank Financial Corporation Otkritie
    3. Sovcombank Open Joint Stock Company
    4. Public Joint Stock Company Sberbank of Russia
    5. VTB Bank Public Joint Stock Company
    6. Joint Stock Company Alfa-Bank
    7. Any entity in which one or more of the above persons, own, directly or indirectly, individually or in the aggregate, a 50 percent or greater interest
    8. Central Bank of the Russian Federation
- Authorizing certain administrative transactions prohibited by Directive 4 under E.O. 14024 (Russia-related Gen. License No. 13A)

Control List require a license from BIS to export to Russia. Approximately 500 industrial and commercial items classified as EAR99 also require export licenses (15 C.F.R. 746.5)

- Export licenses are required for exports of certain items used in exploration for, or production of oil or gas in, Russian deepwater, Arctic offshore, or shale formations in Russia (15 C.F.R. 746.5)
- Export license is required for export of any item subject to the EAR to the Crimea, Donetsk, and Luhansk regions of Ukraine, except food, medicine, and software for internet communications (15 C.F.R. 746.6)

Sectoral Sanctions Restrictions on Raising Capital

- E.O. 13662, Directive 1:
  - For new debt or new equity issued on or after July 16, 2014, and before September 12, 2014, all transactions in, provision of financing for, and other dealings in new debt of longer than 90 days maturity or new equity of persons determined to be subject to Directive 1 or any earlier version thereof, their property, or their interests in property.
  - For new debt or new equity issued on or after September 12, 2014, and before November 28, 2017, all transactions in, provision of financing for, and other dealings in new debt of longer than 30 days maturity or new equity of persons determined to be subject to Directive 1 or any earlier version thereof, their property, or their interests in property.
  - For new debt or new equity issued on or after November 28, 2017, all transactions in, provision of financing for, and other dealings in new debt of longer than 14 days maturity or new equity of persons determined to be subject to Directive 1 or any earlier version thereof, their property, or their interests in property (E.O. 13662, CAATSA section 223)
- E.O. 13662, Directive 2:
  - For new debt issued on or after July 16, 2014, and before November 28, 2017, all transactions in, provision of financing for,

and other dealings in new debt of longer than 90 days maturity of persons determined to be subject to Directive 2 or any earlier version thereof, their property, or their interests in property.
  - For new debt issued on or after November 28, 2017, all transactions in, provision of financing for, and other dealings in new debt of longer than 60 days maturity of persons determined to be subject to Directive 2 or any earlier version thereof, their property, or their interests in property (E.O. 13662, CAATSA section 223)
- E.O. 13662, Directive 3:
  - All transactions in new debt of longer than 30 days with certain defense sector entities designated under Sectoral Sanctions Identifications List Directive 3 (E.O. 13662)

Sectoral Sanctions Restrictions on Financial Sector and Capital Market Access

- E.O. 14024, Directive 1A: Prohibitions Related to Certain Sovereign Debt of the Russian Federation
  - A prohibition on participation in the primary and secondary markets for bonds issued by the Russian Central Bank, National Wealth Fund, or the Ministry of Finance
- E.O. 14024, Directive 2: Prohibitions Related to Correspondent or Payable-Through Accounts and Processing of Transactions Involving Certain Financial Institutions
  - Prohibits the opening or maintaining of correspondent or payable-through accounts and processing of transactions involving foreign financial institutions at designated financial institutions (The Directive designated Sberbank and certain of its subsidiaries, which were subsequently blocked after being designated as SDNs)
- E.O. 14024, Directive 3: Prohibitions Related to New Debt and Equity of Certain Russia-related Entities
  - Prohibits transactions and dealings by U.S. persons in new debt of longer than 14 days maturity and new equity of certain Russian state-owned enterprises

    and entities that operate in the financial

services sector of the Russian Federation economy. Thirteen Russian entities, including Alfa Bank, Sberbank, and Gazprom, are subject to these new debt-related restrictions, six of which were already subject to certain debt or other restrictions under U.S. sectoral sanctions. • E.O. 14024, Directive 4: Prohibitions Related to Transactions Involving the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, and the Ministry of Finance of the Russian Federation – Prohibits U.S. persons from engaging in transactions involving the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, and the Ministry of Finance of the Russian Federation, including any transfer of assets to such entities or any foreign exchange transaction for or on behalf of such entities, except for certain energy-related transactions licensed by OFAC **Sectoral Sanctions Related to the Energy Sector** • E.O. 13662, Directive 4: – The provision of goods, services (except financial services), or technology in support of exploration or production for deepwater, Arctic offshore, or shale projects that (1) have the potential to produce oil and that involve any person determined to be subject to Directive 4, their property, or their interests in property; or (2) that are initiated on or after January 29, 2018, that have the potential to produce oil in any location, and in which any person determined to be subject to Directive 4, their property, or their interests in property has a 33 percent or greater ownership interest, or ownership of a majority of the voting interests (E.O. 13622, CAATSA section 223)	

Secondary • Anyone that facilitates a significant transaction or transactions, including	

deceptive or structured transactions, on behalf of any person subject to any U.S. sanctions imposed with respect to the Russia Federation (CAATSA section 228) • Any foreign financial institution that knowingly engages in significant transactions involving any of the Directive 4-type oil projects in Russia, certain defense-related activities, or Gazprom's withholding of gas supplies or knowingly facilitates significant financial transactions on behalf of any Russian person added to OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) (CAATSA section 226) • Any foreign person who knowingly makes a significant investment in a special Russian crude oil project (CAATSA section 225) • Any person who engages in a significant transaction with a person that is part of, or operates for or on behalf of, the defense or intelligence sectors of the Russian government (CAATSA section 231) • Any person who knowingly makes an investment that directly and significantly contributes to the enhancement of the ability of the Russian Federation to construct energy export pipelines, or sells, leases, or provides to the Russian Federation, for the construction of Russian energy export pipelines, certain goods, services, technology, information, or support that have a certain fair market value (CAATSA section 232) • Any person that knowingly engages in significant activities undermining cybersecurity on behalf of the Russian government, or materially assists, sponsors, or provides support for or provides financial services in support of same (CAATSA section 224)	

Venezuela

The United States has increased sanctions targeting the Maduro regime in recent years. Perhaps most notably, on August 5, 2019, President Trump issued Executive Order 13884, which blocked the property and assets of the Venezuelan government, thereby prohibiting U.S. persons from transacting with the Venezuelan government unless approved by OFAC. The principle goal of these sanctions is to undermine Nicolas Maduro's regime and its main source of revenue: oil. OFAC has issued more than 25 general licenses permitting humanitarian and other activities to reduce the

order's negative impact on Venezuela's general population. The sanctions also target non-U.S. persons providing material support for the Maduro regime.

Primary sanctions apply to:

- U.S. entities
- U.S. citizens
- U.S. permanent residents
- Persons in the United States
- Foreign branches of U.S. entities

31 C.F.R. Part 591

Principal Prohibitions	Select Exemptions and Observations
Primary • All property of the government of Venezuela and entities owned 50 percent or more or otherwise controlled by the government of Venezuela is blocked (section 591.201, see also E.O. 13884) – Definition of the "government of Venezuela" includes any political subdivision of the government (including the Central Bank of Venezuela and Petroleos de Venezuela, S.A. (PdVSA)), any person owned or controlled by the government, and any person who has acted on behalf of the government (section 591.201, see also E.O. 13884) • Transactions related to, providing financing for, or otherwise dealing in new debt with a maturity of greater than 90 days and that is issued by, on behalf of, or for the benefit of PdVSA, its property, or its interests in property (section 591.201, see also E.O. 13808(1)(a)(i)) • Transactions related to, providing financing for, or otherwise dealing in new debt with a maturity of longer than 30 days issued by, on behalf of, or for the benefit of any other segment of the government of Venezuela, its property, or its interests in property (section 591.201, see also E.O. 13808(1)(a)(ii)) • Transactions related to, providing financing for, or otherwise dealing in bonds issued by the government of Venezuela prior to August 25, 2017 (section 591.201, see also E.O. 13808(1)(a)(iii)) • Transactions related to, providing financing for, or otherwise dealing in dividend	• Authorizes all transactions otherwise prohibited by subsections 1(a)(i), (a)(ii), and (b) of E.O. 13808 provided that the only government of Venezuela entities involved in the transactions are PDV Holding, Inc., CITGO Holding, Inc., and any of its subsidiaries (Gen. License 2A) • Authorizes all transactions related to the provision of financing for and other dealings in bonds contained in the Annex to General License 3H that would otherwise be prohibited by section 1(a)(iii) of E.O. 13808 or by E.O. 13850, provided that any divestment or transfer of, or facilitation of divestment or transfer of, any holdings in such bonds must be to a non-U.S. person (Gen. License 3H) • Authorizes all transactions related to the provision of financing for and other dealings in bonds issued prior to August 25, 2017, if such bonds were issued by U.S. person entities owned or controlled, directly or indirectly, by the government of Venezuela, other than PDV Holding, Inc., CITGO Holding, Inc., and any of their subsidiaries (Gen. License 3H) • Authorizes all transactions related to the provision of financing for and other dealings in debt issued on or after August 25, 2017, related to the exportation or re-exportation of agricultural commodities, medicine, medical devices, replacement parts and components for medical devices, or software updates for medical devices to Venezuela, or to persons in third countries

payments or other distributions of profits to the government of Venezuela by any entity owned or controlled, directly or indirectly, by the government of Venezuela (section 591.201, see also E.O. 13808(1)(a)(iv))
- Purchasing any securities from the government of Venezuela other than securities issued on or after August 25, 2017, with a maturity of less than or equal to 90 days (for PdVSA) or 30 days (for the rest of the government of Venezuela) (section 591.201, see also E.O. 13808(1)(b))
- Transactions related to, provision of financing for, and other dealings in any digital currency, digital coin, or digital token that was issued by, for, or on behalf of the government of Venezuela (section 591.201, see also E.O. 13827)
- Involvement in the transfer by the government of Venezuela of any equity interest in any entity owned 50 percent or more by the government of Venezuela, as well as related transactions in the United States (section 591.201, see also E.O. 13835)
- Transactions involving persons determined to operate in Venezuela's gold and oil sectors (section 591.201, see also E.O. 13850)

Secondary
- Any person who materially assists, supports, or provides financial, material, or technological support for, or services to or in support of, a blocked Venezuelan person or a person who is owned or controlled by a blocked Venezuelan person (sections 591.201 and 591.304, see also E.O. 13884)

purchasing specifically for resale to Venezuela (Gen. License 4C)
- Authorizes certain transactions related to PdVSA 2020 8.5 percent bond (Gen. License 5I)
- Authorizes certain transactions involving PdVSA and Chevron, Halliburton, Schlumberger, Baker Hughes, or Weatherford through December 1, 2022 (Gen. License 8J)
- Authorizes all transactions that are otherwise prohibited by E.O. 13808 or E.O. 13850, as amended, that are ordinarily incident and necessary to dealings in any debt (including the bonds listed on the Annex to this general license, promissory notes, and other receivables) of, or any equity in, PdVSA or any entity in which PdVSA owns, directly or indirectly, a 50 percent or greater interest, issued prior to August 25, 2017, provided that any divestment or transfer of, or facilitation of divestment or transfer of, any holdings in such PdVSA securities must be to a non-U.S. person (Gen. License 9G)
- Authorizes U.S. persons in Venezuela to purchase refined petroleum products for personal, commercial, or humanitarian use from PdVSA or any entity in which PdVSA owns, directly or indirectly, a 50 percent or greater interest (Gen. License 10A)
- Authorizes certain transactions to protect intellectual property rights (Gen. License 27)
- Authorizes all transactions with Venezuelan National Assembly and Interim President Juan Guaido and staff (in recognition of Juan Guaido as the Interim President of Venezuela) (Gen. License 31A)
- Authorizes all transactions ordinarily incident and necessary to operation of ports and airports in Venezuela (Gen. License 30A)
- Authorizes U.S. financial institutions to conduct certain limited transactions with blocked persons, such as debiting a blocked account for payment of custody fees (Gen. License 21)
- Authorizes transactions involving certain humanitarian goods and services (Gen.

	Licenses 20B, 22–26, 29) • Authorizes all transactions and activities prohibited by E.O. 13844 by U.S. citizens and other U.S. residents, former government of Venezuela employees, and current government of Venezuela employees who provide health or education services (Gen. License 34A) • Authorizes certain administrative transactions with the government of Venezuela otherwise prohibited by E.O. 13884, such as paying taxes, fees, and import duties, where such transactions are necessary and ordinarily incident to such persons' day-to-day operations (Gen. License 35) • Authorizes transactions involving the government of Venezuela related to the prevention, diagnosis, and treatment of Covid-19 through June 17, 2023 (Gen License 39A) • Authorizes all transactions and activities related to the export of liquefied petroleum gas to Venezuela (Gen. License 40A)

Appendix B

Important Considerations for Multinational Companies

The prohibitions on facilitation found in U.S. economic sanctions programs presents unique compliance challenges for multinational companies. In particular, the risk of noncompliance with these prohibitions is elevated because, in many cases, persons who must comply with U.S. economic sanctions may unknowingly or unintentionally facilitate targeted activities undertaken by other persons who have no obligations under U.S. economic sanctions (such as non-U.S. agents, co-workers, customers, or vendors). There is enforcement risk if OFAC determines, after the fact, that a person required to comply with U.S. economic sanctions "should have known" of these targeted activities by others.

The concept of facilitation potentially covers some corporate support functions performed by U.S. persons if they facilitate activities by non-U.S. affiliates in or with U.S. economic sanctions targets. Examples of these prohibited support activities include workflow approvals, guidance, feedback, and, if intended for use in support of targeted transactions, even certain recordkeeping or data storage functions. Among many other potential risk areas, the following chart lists circumstances where U.S. persons working for multinational companies should exercise caution to avoid facilitating specific transactions and activities conducted by non-U.S. persons working for the same company involving sanctions targets.

Financial Matters	**Information Technology**
• Mandatory approval procedures that require U.S. persons to approve expenditures by • non-U.S. persons Processing of bank transfers and payments by U.S. persons on • behalf of non-U.S. persons Reallocations of "overhead" costs, such as management services or other support services, of U.S. persons to non-U.S. affiliates that engage in • targeted activities Revenue allocations of customer contracts between U.S. and non-U.S. affiliates where subsequent performance could potentially involve activities with economic sanctions targets performed by non-U.S. affiliates (such as a	Global electronic networks that are accessible by both U.S. and non-U.S. persons, including: • Processing and enterprise software programs • Inventory management systems • Servers maintained by U.S. person employees or owned by entities that are • U.S. persons Network connections routed through the United States • Help desks staffed by U.S. persons • Email and other electronic correspondence that allow non-U.S. persons to freely communicate with U.S. persons without procedures that prohibit discussion of

master customer contract regulating future • purchase orders) Financial arrangements and payments between U.S. parent companies • and non-U.S. subsidiaries Commingling of assets and shared bank accounts by U.S. and non-U.S. affiliates • Inadequate capitalization of non-U.S. subsidiaries creating exposure for future • capital calls against U.S. affiliates Accounting and auditing services performed by U.S. affiliates for non-U.S. affiliates	activities prohibited by U.S. economic • sanctions with U.S. persons International movement of cell phones, software, and laptops with U.S. content

Management Practices • Approval by a U.S. company of its non-U.S. affiliate's activities with economic sanctions • targets Policies developed or implemented by U.S. persons that predominantly impact • non-U.S. affiliates Provision of general management or administrative services by U.S. persons for the benefit of non-U.S. affiliates whose activities may have shifted • to predominantly targeted transactions Administration of the benefits of global purchases, such as individual claims under a global insurance policy, by U.S. persons on • behalf of non-U.S. affiliates or employees Transfers of certain business activities, and the motives for doing so, from U.S. persons • to non-U.S. persons Business referrals of potentially targeted transactions by U.S. • persons to non-U.S. persons Changes to U.S. persons' business practices that have the effect of accommodating non-U.S. affiliates' transactions with economic sanctions targets	**Human Resources and Personnel Management** • Involvement by U.S. persons in the hiring processes of non-U.S. affiliates • Failure to terminate U.S. companies' employment contracts with employees who • have been transferred to non-U.S. affiliates Consolidated compensation and benefits administration (payroll, life insurance, pension plans) conducted by U.S. persons on behalf of non-U.S. affiliates and their • employees Reassignment of employees, and the motives for doing so, between U.S. and • non-U.S. affiliates Employment of targeted country nationals by U.S. persons • Non-U.S. persons working on, or facilitating, prohibited activities without appropriate restrictions on generic support and advice from U.S. persons (such as professional guidance on increasing revenue • generation) U.S. person involvement in hiring decisions in regions where non-U.S. colleagues may discourage hiring U.S. persons who cannot engage in targeted • transactions Training programs that mix U.S. person and non-U.S. person instructors and trainees
Corporate Structure and Corporate Formalities • Divergence of functional structure from corporate legal structure • Interlocking officers, directors, or employees among U.S. and non-U.S. affiliates • Lack of maintenance of separate corporate formalities leading to a "piercing" of non-U.S. subsidiaries' "corporate veils" and	

causing their actions to be attributed to their U.S. parent companies	

Appendix C

Key Court Decisions Interpreting U.S. Economic Sanctions Laws

Federal Preemption

Crosby v. National Foreign Trade Council, 530 U.S. 363 (2000). The Court found that a Massachusetts law restricting state agencies from buying goods or services from designated persons doing business with Burma (Myanmar) was preempted under the Supremacy Clause of the U.S. Constitution by federal legislation imposing economic sanctions on Burma (Myanmar), implemented in part by executive order. (*Note*: CISADA and the Sudan Accountability and Divestment Act of 2007 purport to remove federal preemption and to permit state and local governments to adopt legislation, and university endowments to adopt policies, prohibiting those governments and endowments from investing in companies or corporate groups that engage in certain activities in Iran and Sudan. Courts have continued to hold state sanctions programs preempted, however. *See, e.g.*, *Odebrecht Const., Inc. v. Sec'y, Fla. Dep't of Transp.*, 715 F.3d 1268, 1281 (11th Cir. 2013).)

United States v. Curtiss-Wright Export Corp., 299 U.S. 304 (1936). The Court held that the delegation by Congress to the President of the authority to prohibit arms sales to foreign countries was not an invalid delegation of legislative power to the executive branch. The authority to conduct foreign affairs vests in the federal government independently of the authority granted in the Constitution and constitutes, "the very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations—a power which does not require as a basis for its exercise an act of Congress . . ." 299 U.S. at 320.

Regan v. Wald, 468 U.S. 222 (1984). The President's grandfathered authority under section 5(b) of TWEA provides the basis for executive action restricting transactions related to travel to Cuba. The Court also concluded, in part because "[m]atters relating 'to the conduct of foreign relations . . . are so exclusively entrusted to the political branches of government,'" that the travel restrictions do not violate the freedom to travel protected by the Due Process Clause of the Fifth Amendment.

Legality of TWEA and IEEPA

Dames & Moore v. Regan, 453 U.S. 654 (1981). The Court upheld the President's broad exercise of authority under IEEPA, including the authority to impose and modify blocking actions, and the authority to nullify judicial attachments and judgments involving blocked property in connection with the implementation of an agreement between the governments of Iran and the United States. Courts have continued to reject arguments that IEEPA is unconstitutional. *See, e.g.*, *United States v. Amirnazmi*, 645 F.3d 564, 596 (3d Cir. 2011); *United States v. Dhafir*, 461 F.3d 211 (2d Cir. 2006).

Sardino v. Federal Reserve Bank of New York, 361 F.2d 106 (2d Cir. 1965). The President's exercise of authority under TWEA to declare a national emergency and to delegate authority to the secretary of the treasury to issue regulations blocking the assets of Cuban nationals does not violate the Constitution.

Blocked Property and Property Interests: Cases Illustrating a Narrow Interpretation of "Property Interest"

Centrifugal Casting Machine Co. v. American Bank & Trust Co., 966 F.2d 1348 (10th Cir. 1992). The court rejected OFAC's interpretation of property interest because it was inconsistent with the law governing the letters of credit at issue.

Consarc Corp. v. Iraqi Ministry, 27 F.3d 695 (D.C. Cir. 1994). The court followed the reasoning of *Centrifugal* in affirming OFAC's interpretation of "property" and "property interest" where "OFAC's determination was fully in accord with the general law governing letters of credit and thus survive[d]" judicial review. *Id.* at 702.

Consarc Corp. v. U.S. Department of the Treasury, Office of Foreign Assets Control, 71 F.3d 909 (D.C. Cir. 1995). This case illustrates the broad authority granted to OFAC to interpret its regulations and notes "the general interpretive principle that exceptions to a broad regulatory scheme are to be read narrowly." *Id.* at 915.

Blocked Property and Property Interests: Cases Illustrating a Broad Interpretation of "Property Interest"

Milena Ship Management v. Newcomb, 995 F.2d 620 (5th Cir. 1993). OFAC acted reasonably in finding a blocked property interest of the government of Yugoslavia in vessels based on its interpretation of Yugoslav law and resulting presumption of state ownership of the vessels. *See also Behring Int'l, Inc. v. Miller*, 504 F. Supp. 552 (D.N.J. 1980); *United States v. Broverman*, 180 F. Supp. 631 (S.D.N.Y. 1959).

Terrorism / Material Support

Holder v. Humanitarian Law Project, 561 U.S. 1 (2010). It is not a violation of the First Amendment to the Constitution for the federal government to prohibit nonviolent "material support" (including legal services, advice, advocacy) to a foreign terrorist organization—even if that support is limited to humanitarian activities—provided that the material support is coordinated with, directed by, or controlled by the foreign terrorist organization.

Blocking versus Takings under the Fifth Amendment

Nielsen v. Secretary of the Treasury, 424 F.2d 833 (D.C. Cir. 1970). The blocking of Cuban assets pursuant to TWEA is not subject to the "takings clause" of the Fifth Amendment to the Constitution, although the court states that the question whether blocking constitutes a taking subject to due process becomes more difficult if the blocking continues indefinitely.

Tran Qui Than v. Regan, 658 F.2d 1296 (9th Cir. 1981). Neither the blocking of the assets of a Vietnamese bank under TWEA nor prohibiting a Vietnamese shareholder of the bank from obtaining the bank's blocked assets constitute a taking without just compensation in violation of the Fifth Amendment to the Constitution.

Chas. T. Main International, Inc. v. Khuzestan Water & Power Authority, 651 F.2d 800 (1st Cir. 1981). Neither the nullification of judicial attachments nor the transfer of Iranian blocked property pursuant to IEEPA

constitutes a taking without just compensation in violation of the Fifth Amendment to the Constitution.

Civil Penalties Subject to Reversal If "Arbitrary and Capricious"

Epsilon Elecs., Inc. v. United States Dep't of Treasury, Office of Foreign Assets Control, 857 F.3d 913, 927 (D.C. Cir. 2017). Reversing civil penalty on five shipments allegedly intended for end-use in Iran on the grounds that "OFAC failed to adequately explain why it discounted" evidence suggesting the company was unaware the shipments were intended for reexport to Iran. The court declined to uphold the penalty, which applied to 34 shipments in total, on the grounds that severance of the five unsupported shipments would not be appropriate.

Reversal is an unusual outcome, however, as courts often affirm the agency's action under the "highly deferential" arbitrary and capricious standard. *Zevallos v. Obama*, 793 F.3d 106, 114 (D.C. Cir. 2015); *Holy Land Found. for Relief & Dev. v. Ashcroft*, 333 F.3d 156, 162 (D.C. Cir. 2003).

Obligation to Provide Clear Guidance

In December 2019, the U.S. District Court for the Northern District of Texas held that a company could not be liable for sanctions violations where OFAC's guidance on the scope of prohibited conduct was not clear. The case concerned a 2017 penalty levied against Exxon Mobil, which signed contracts with a non-sanctioned entity that were signed by its principal, Igor Sechin, who was listed as an SDN. OFAC took the position that, because Sechin signed the contracts, Exxon had engaged in business with an SDN in violation of U.S. sanctions; OFAC maintained that its business was with the entity itself, which was not listed. The court held that OFAC's guidance at the time was insufficiently clear and as a result the company "lacked fair notice that [its] conduct was prohibited."

Although OFAC has since issued guidance making clear that U.S. persons cannot enter into contracts signed by SDNs (see FAQ 400), the decision signals that OFAC has an obligation to clearly articulate the scope of prohibited conduct. Where the agency declines to clarify whether conduct is prohibited, or a company operates in a "gray area," it may have be able to leverage this uncertainty to avoid penalties.

2

U.S. International Traffic in Arms Regulations

Geoffrey M. Goodale and Douglas N. Jacobson[1]

2.1 Overview

What is regulated: Temporary and permanent exports, as well as temporary imports, of defense articles identified on the U.S. Munitions List (USML) set forth under section 121.2 of the International Traffic in Arms Regulations (ITAR) and defense services relating to defense articles.[2] Brokering of defense articles/services is also covered in Section 2.10. It is important to note that many parts and components for defense articles are regulated by the U.S. Department of Commerce's Bureau of Industry and Security (BIS), as described in Chapter 3.

Where to find the regulations: The ITAR are found in parts 120 through 130 of chapter 22 of the Code of Federal Regulations.[3]

Who is the regulator: The ITAR are administered by the U.S. Department of State, Directorate of Defense Trade Controls (DDTC). Section 2.3, later in the chapter, provides additional details.

How to get a license: Requests for ITAR licenses and other types of authorizations are filed electronically via DDTC's Defense Export Control and Compliance System (DECCS), found at https://deccs.pmddtc.state.gov/deccs.

Key website: https://www.pmddtc.state.gov/ddtc_public.

2.2 A Brief History of U.S. Defense Trade Controls

The U.S. government has long sought to prevent foreign adversaries from obtaining access to items or technology that could harm U.S. national security. Beginning in the 1930s, the Congress and the President focused on achieving this objective through the passage of legislation that placed significant restrictions on the export of defense-related items.

Initially, Congress passed the Neutrality Act of 1935, prohibiting the export of "arms, ammunition, and implements of war" from the United States to "belligerent countries" and establishing the National Munitions Control Board, chaired by the Secretary of State and including the Departments of Treasury, War, Navy, and Commerce.[4] The Neutrality Act of 1935 prohibited any company or individual "to export, or attempt to export, from the United States . . . arms, ammunition, or implements of war . . . to any other country or to import, or attempt to import, to the United States from any other country . . . arms, ammunition, or implements of war" without first obtaining a license.[5] On September 19, 1935, the State Department established the Office of Arms and Munitions Control[6] to register manufacturers of military items and to issue export and import licenses as required by the 1935 Neutrality Act. The Neutrality Act of 1939, which superseded the 1935 Neutrality Act, subsequently constituted the authority of the President to control exports of arms, ammunition, and implements of war.[7]

Congress subsequently expanded the U.S. Department of State's role in defense-related exports through the passage the Mutual Security Acts of 1951 and 1954, the Foreign Military Sales Act of 1968, and the Arms Export Control Act of 1976. The Mutual Security Act of 1951 prohibited the shipment of arms, ammunition, implements of war, and certain items used to produce arms, ammunition, and implements of war "to any nation or combination of nations threatening the security of the United States, including the Union of Soviet Socialist Republics and all countries under its domination. . . ."[8] The Mutual Security Act of 1954 empowered the President to "designate those articles which shall be considered as arms, ammunition, and implements of war, including technical data" for purposes

of controlling the export of such items, which authority the President delegated to the Secretary of State.[9] The Mutual Security Act of 1954 also included for the first time a statutory registration requirement for persons engaged in the "business of manufacturing, exporting, or importing" controlled items, and required registered parties to pay a registration fee.[10] In accordance with section 414 of the Mutual Security Act of 1954, the International Traffic in Arms Regulations (ITAR) were first published on August 26, 1955.[11]

The Foreign Military Sales Act of 1968 required, among other things, that the Secretary of State submit a semi-annual report to Congress on all exports "of significant defense articles on the United States munitions list."[12]

Section 38 of the Arms Export Controls Act of 1976 (AECA),[13] which replaced the Foreign Military Sales Act of 1968 and continues to serve as the primary statutory authority for U.S. defense export controls, authorized the President to "designate those items which shall be considered as defense articles and defense services . . . and to promulgate regulations for the import and export of such articles and services," with the items so designated "constitut[ing] the United States Munitions List," which authority the President subsequently delegated to the Secretary of State pursuant to Executive Order 11958 of January 18, 1977.[14] Following the passage of the AECA, in 1979, the Department of State began a process to revise the ITAR, and significant amendments to the ITAR were published on December 6, 1984.[15]

2.3 U.S. Export Control Reform Initiative

On August 13, 2009, then-President Obama announced the launch of a comprehensive review of the U.S. export control system in order to "address the threats [the U.S.] face[s] today and the changing economic and technological landscape."[16] This review determined that the existing U.S. export control system was "overly complicated, contain[ed] too many redundancies, and, in trying to protect too much, diminishes [the] ability to focus [U.S.] efforts on the most critical national security priorities."[17]

This review led to a multi-year process known as the Export Control Reform Initiative (ECRI or ECR) intended to simplify the U.S. export

control system by enacting "a system where higher walls are placed around fewer, more critical items."[18] As proposed, the ECR originally included four elements, known as the "four singularities," that were to be implemented in three phases:[19]

1. Creation of a single primary export control licensing agency for both dual-use and munitions exports;
2. Adoption of a unified export control list;
3. Establishment of a single enforcement coordination agency; and
4. Creation of a single integrated information technology system, which would include a single database of sanctioned and denied parties.

Although not all of the proposed ECR elements were ultimately enacted, the ECR led to significant changes to the U.S. export control and licensing system. Some of the key changes included:

- Transforming the list of controlled items on the USML to a positive list that includes objective criteria and parameters.
- Moving many parts and components that are "specially designed" for defense articles from the USML to the "600 Series" on the Commerce Control List (CCL) administered by the Department of Commerce's Bureau of Industry and Security (BIS). See Chapter 3.
- Moving certain nonautomatic and semiautomatic firearms, related parts and components, software, and technology, as well as certain small-arms ammunition previously included on USML Categories I, II, or III to the "500 Series" or "600 Series" in CCL Category 0.
- Modifying the definition of many terms in the ITAR and harmonizing many terms with BIS's Export Administration Regulations (EAR).
- Establishing an Export Enforcement Coordination Center (E2C2) to deconflict criminal and administrative enforcement operations and coordination of industry enforcement outreach activity.
- Implementing a single information technology system for use by the agencies involved in licensing of items controlled by the ITAR and EAR.
- Creating a single "destination control statement" for exports of items subject to the ITAR and the EAR.

The ECR-related changes to the USML and CCL published in numerous "bookend rules" required an extensive, multi-year effort of proposed and final rules issued by DDTC and BIS. The first of the final rules implementing changes to the USML, which was to USML Category VIII covering military aircraft, was published in the *Federal Register* on April 16, 2013, and became effective on October 15, 2013.[20] Subsequently, after the issuance of numerous other bookend rules relating to various other USML categories, the latest round of ECR-related changes, which pertained to USML Categories I, II, and III, were published in the *Federal Register* on January 23, 2020, and took effect on March 9, 2020.[21] DDTC intends to continue to issue updates to the USML on a periodic basis.

As a result of the changes made by the ECR, U.S. exporters and non-U.S. re-exporters involved in the defense sector must be familiar with *both* the ITAR and EAR and understand the "order of review" process used to determine whether a defense-related item and related technical data or software are subject to the export controls jurisdiction of the ITAR or EAR.[22]

2.4 Administration and Enforcement of the ITAR

The ITAR are administered and enforced by the U.S. Department of State's Directorate of Defense Trade Controls (DDTC), which is located within the State Department's Bureau of Political-Military Affairs, the agency's principal link to the Department of Defense. While DDTC's organizational structure has changed over the years, DDTC is currently led by the Deputy Assistant Secretary for Defense Trade.

Within DDTC, there are three offices that report to the Deputy Assistant Secretary for Defense Trade:

(1) Office of Defense Trade Controls Licensing (ODTCL), which is responsible for reviewing and adjudicating export license applications and other authorizations, such as technical assistance agreements. ODTCL is led by a Director and Deputy Director of Licensing and consists of various licensing divisions based on USML categories;
(2) Office of Defense Trade Controls Policy, which is responsible for general policies of defense trade, including developing and

implementing changes to the ITAR as well as the commodity jurisdiction process that can be used by exporters to obtain guidance on the proper export controls jurisdiction and classification of items to be exported; and

(3) Office of Defense Trade Controls Compliance, which is responsible for compliance and civil enforcement of the ITAR, including overseeing consent agreements and serving as a liaison with law enforcement, overseeing the ITAR's registration process for manufacturers and brokers of defense articles, and working closely with the Committee on Foreign Investment in the United States (CFIUS).[23]

Useful information about DDTC's policies and procedures can be accessed at www.pmddtc.state.gov/ddtc_public.

With respect to enforcement of the ITAR, DDTC also receives assistance from two agencies within the U.S. Department of Homeland Security: (1) U.S. Customs and Border Protection (CBP) and (2) U.S. Immigration and Customs Enforcement (ICE), both of which have the authority to investigate, detain, or seize any export or attempted export of ITAR-controlled defense articles or technical data.[24] DDTC also receives enforcement assistance from the Federal Bureau of Investigation, and in cases involving classified technical data or defense articles, advisory assistance from the U.S. Department of Defense's Defense Security Service (DSS).[25]

2.5 Scope of the ITAR

The ITAR govern temporary and permanent exports, re-exports, and retransfers of defense articles (including software and technical data) enumerated on the USML, as well as temporary imports of such items.[26] Permanent imports of defense articles enumerated on the U.S. Munitions Import List, which is a list separate from the USML, that is maintained by the U.S. Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), are regulated and enforced by ATF.[27]

To understand the breadth of the ITAR, it is necessary to review how certain key terms are defined.

Under the ITAR, a “defense article” is defined to include any item designated on the USML.[28] In addition, the ITAR cover items that “meets the criteria of a defense article . . . on the [USML]” or “provide[] the equivalent performance capabilities of a defense article on the [USML].”[29]

The definition of “defense article” also includes “technical data” specified on the USML.[30] Technical data includes “information which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles.”[31] This includes, but is not limited to, “information in the form of blueprints, drawings, photographs, plans, instructions or documentation.”[32] In addition, technical data includes:

- Classified information relating to defense articles and defense services on the USML;
- Information covered by an invention secrecy order; or
- Software (as defined in Section 120.40(g) of the ITAR), directly related to defense articles (including, but not limited to, system functional design, logic flow, algorithms, application programs, operating systems, and support software for design, implementation, test, operation, diagnosis, and repair).[33]

However, ITAR-controlled technical data does not include information concerning: general scientific, mathematical or engineering principles commonly taught in schools; basic marketing information on function or purposes; general system descriptions of defense articles.[34] In addition, information in the “public domain” is not subject to the ITAR, including information that is published and is generally accessible or available to the public through various means, such as through sale at newsstands or bookstores; through publicly available patents; through unlimited distribution at conferences, seminars, or trade shows; and at libraries open to the public.[35] The ITAR also does not cover technical data approved for public release by a cognizant government agency, provided it is subsequently placed in the public domain.[36]

Exports of “defense services” also are controlled under the ITAR. A “defense service” is defined as “[t]he furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the

design, development, engineering, manufacture, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles."[37] In addition, a "defense service" includes the furnishing to foreign persons of "any technical data controlled under the ITAR, whether in the United States or abroad," and "military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice."[38] The concept of a "defense service" is not limited to providing ITAR-controlled technical data. If the assistance or training is limited to providing publicly available information, under DDTC's current interpretation of the current definition of defense service, its delivery still constitutes a "defense service" if the purpose of that information is to support the use of defense articles or to train military units.

The ITAR regulates the export of defense articles, technical data, and software that are listed on the USML. The term "export" is defined to include:

- An actual shipment or transmission out of the United States, including the sending or taking of a defense article out of the United States in any manner;
- Releasing or otherwise transferring technical data to a foreign person in the United States (known as a "deemed export");
- Transferring registration, control, or ownership of any aircraft, vessel, or satellite subject to the ITAR by a U.S. person to a foreign person;
- Releasing or otherwise transferring a defense article to an embassy or to any of its agencies or subdivisions, such as a diplomatic mission or consulate, in the United States;
- Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad; or
- The release of previously encrypted technical data as described in § 120.56(a)(3) and (4) of the ITAR.[39]

As can be seen from this broad definition, an export can occur in numerous ways. For example, if ITAR-controlled technical data is "released" or transferred to a foreign person, including an employee of the company that

receives the technical data, the information is "deemed" to have been exported to that person's home country. The term "release," which was added to the ITAR during the ECR process, states that technical data is released through:

(1) Visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person; or

(2) Oral or written exchanges with foreign persons of technical data in the United States or abroad.

(3) The use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data; or

(4) The use of access information to cause technical data outside of the United States to be in unencrypted form.[40]

This definition makes clear that "authorization [from DDTC] for a release of technical data to a foreign person is required to provide access information to that foreign person, if that access information can cause or enable access, viewing, or possession of the unencrypted technical data."[41]

It is important to understand the ITAR's distinction between "U.S. persons" and "foreign persons." In the absence of an ITAR exemption, an authorization from DDTC is required for "U.S. persons" to export ITAR-controlled items and technical data to "foreign persons" or for "foreign persons" to re-export or transfer such items to other "foreign persons." The term "U.S. person" includes (1) U.S. citizens; (2) lawful permanent residents (i.e., green card holders); (3) protected individuals, as defined by 8 U.S.C. § 1324b(a)(3); (4) any corporation and other business entity authorized to do business in the United States; and (5) any U.S. federal, state, or local government entity.[42] As such, the ITAR treats permanent resident aliens and persons granted political asylum, under certain circumstances, as U.S. persons. Thus, dual nationals who are also citizens of the United States, and non-U.S. citizens who hold U.S. green cards, are U.S. persons for purposes of the ITAR.

The ITAR's definition of a "foreign person" includes anyone who is not a U.S. person.[43] This includes any person who is not a citizen, a lawful permanent resident, or a "protected person" of the United States, any foreign corporation or other entity that is not incorporated or organized to do business in the United States, and any foreign government.[44] Thus, persons who are in the United States under visas (e.g., H-1B, L-1, and F-1

visas) are considered to be foreign persons. In addition, care must be taken to consider dual nationals as well. It is DDTC's policy that foreign persons who are not U.S. persons can be considered to be citizens of more than one country (i.e., dual nationals). DDTC considers country of birth, even in cases where a person does not hold a passport from his country of birth, and countries of subsequent citizenship, as factors in determining the nationality of the foreign persons for licensing and other purposes.[45] When a U.S. company employs a foreign person, the U.S. company is obligated to ensure compliance with U.S. export control laws and regulations, including the ITAR, with respect to that employee. This means, among other things, that a U.S. company would be required to obtain authorization from DDTC3 before ITAR-controlled items or technical data could be released to that employee.

2.6 Determining What Is Subject to the ITAR

As the preceding discussion indicates, it is critical to understand whether an item is subject to the ITAR or EAR. The first step in evaluating whether an item is subject to the ITAR is to determine whether the item is identified on the USML. The USML includes the following categories:

Category I: Firearms and Related Articles

Category II: Guns and Armament

Category III: Ammunition/Ordnance

Category IV: Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, and Mines

Category V: Explosives and Energetic Materials, Propellants, Incendiary Agents, and Their Constituents

Category VI: Surface Vessels of War and Special Naval Equipment

Category VII: Ground Vehicles

Category VIII: Aircraft and Related Articles

Category IX: Military Training Equipment and Training

Category X: Personal Protective Equipment

Category XI: Military Electronics

Category XII: Fire Control, Laser, Imaging, and Guidance Equipment

Category XIII: Materials and Miscellaneous Articles

Category XIV: Toxicological Agents, including Chemical Agents, Biological Agents, and Associated Equipment

Category XV: Spacecraft and Related Equipment

Category XVI: Nuclear Weapons–Related Items

Category XVII: Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated

Category XVIII: Directed Energy Weapons

Category XIX: Gas Turbine Engines and Associated Equipment

Category XX: Submersible Vessels and Related Articles

Category XXI: Articles, Technical Data, and Defense Services Not Otherwise Enumerated[46]

USML categories are organized by paragraphs and subparagraphs identified alphanumerically. They start by enumerating or otherwise describing end-platforms, followed by major systems and equipment, and parts, components, accessories, and attachments.[47] Most USML categories contain an entry for technical data and defense services directly related to the defense articles of that USML category. It is important to review the notes contained within the text of the USML categories, since these notes contain useful explanatory information.

Items on the USML that are preceded by an asterisk (*) are considered to be "Significant Military Equipment" (SME) and are subject to additional controls "because of their capacity for substantial military utility or capability."[48] Technical data directly related to the manufacture of production of defense articles designated as SME is also considered to be SME.[49]

Category XXI is a "catchall" category that can be used by DDTC to control items that are not found elsewhere on the USML until the relevant category has been amended. However, items can only be designated in

Category XXI by the Director of the Office of Defense Trade Controls Policy.[50]

An important concept in understanding whether an item is controlled by the ITAR or EAR is the "order of review", a concept introduced by ECR.[51] As a result of ECR, an item that has defense or military applications may not be subject to the ITAR. This is particularly true for parts and components for military end-items. The following steps should be used in determining whether an item (and related technical data or software) is subject to the export controls jurisdiction of the ITAR or the EAR:

1. Begin by reviewing the general characteristics of an item. This should guide you to the appropriate USML category where you should attempt to match the particular characteristics and functions of the article to a specific entry within that category. Be sure to review the notes contained with the USML category.
2. If the USML entry includes the term "specially designed," refer to the definition of that term in section 120.41 of the ITAR to determine if the article qualifies for one or more of the releases articulated in section 120.41(b). This is particularly important for parts, components, accessories, and attachments.
3. In cases where an item is described in multiple USML entries, an enumerated entry takes precedence over an entry controlling the item by virtue of a "specially designed" catchall. The exception to this rule is where an SME entry is involved, where an SME entry will take precedence over a non-SME entry.
4. If it is determined that an item is not subject to the ITAR, because it is not within the scope of any USML categories, the item will be subject to the export controls jurisdiction of the EAR in most cases.[52]

When a USML category includes "specially designed" as a criteria, it is important to understand the ITAR's definition of "specially designed."[53] The specially designed criteria was introduced during ECR as a way to determine whether an item is "caught" by the ITAR or not, rather than having to determine whether it was originally designed for military or commercial applications. One can determine whether an item is "specially designed" by answering a series of yes/no questions. The first two questions

in subsection (a) of the specially designed definition are intended to determine whether an item is "caught" by the specially designed definition:

> (a)(1). As a result of development, does the item have properties peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions described in the relevant U.S. Munitions List paragraph"; or
>
> (a)(2). Is it a part, component, accessory, attachment, or software for use in or with a defense article?

If a part, component, accessory, attachment, or software is caught by subsection (a), the next step is to determine whether the item is released for any of the five reasons included in subsection (b) of the "specially designed" definition:

> (b)(1). Is the item subject to the EAR pursuant to a commodity jurisdiction (CJ) (discussed next)?
>
> (b)(2). Is the part a fastener (e.g., screws, bolts, nuts, etc.), washer, spacer, insulator, grommet, bushing, spring, wire, or solder?
>
> (b)(3). Does the item have the same function, performance capabilities, *and* the same or "equivalent" form and fit as a commodity or software that is or was in production and is not enumerated on the USML?
>
> (b)(4). Was the item developed with knowledge that it would be for use in or with both USML and non-USML items?
>
> (b)(5). Was the item developed as a general-purpose commodity with no knowledge it was intended to be used with a particular commodity?

If the answer is yes to any of the five questions in subsection (b), the part is "released" from the ITAR and is subject to the export controls jurisdiction of the EAR.

In most cases, the ITAR's order of review process allows exporters to make jurisdictional and classification self-determinations and there is no need to seek confirmation from DDTC. However, if there is still doubt as to whether an item is covered by the USML, DDTC has established procedures for applicants to request a commodity jurisdiction (CJ) determination.[54] The CJ issued by DDTC will state whether the item is subject to the ITAR or EAR and indicate the relevant USML category. If an item is determined to be subject to the export controls jurisdiction of the EAR, in most cases the CJ will indicate the ECCN classification.

CJ requests must be submitted to DDTC via DECCS using form DS-4076.[55] Applicants do not need to be registered with DDTC to submit a CJ. DECCS will request the applicant to provide detailed information regarding the item for which a CJ, including the characteristics, end use, product origin, funding history, sales information, and so on. It is also useful to submit attachments with the CJ request to assist the reviewers in making their determination, such as product brochures, technical specifications, and other relevant information. Additional information on CJ requests, including an example form and instructions that can be accessed without logging into DECCS can be found on the Commodity Jurisdiction page of DDTC's website.

Once a CJ request has been submitted, DDTC will consult with the Bureau of Industry and Security, the U.S. Department of Defense (DOD), and other relevant U.S. government agencies to determine the classification, and any disputes among the agencies will be resolved in accordance with established procedures.[56] It can take several months for a CJ determination to be issued. The timing will vary depending on the complexity of the product and the quality of the CJ submission.

The final CJ determination is issued in the form of a letter to the applicant that contains the final determination. If the applicant disagrees with the determination, CJ determinations can be appealed by submitting a written request for reconsideration to the Deputy Assistant Secretary of State for Defense Trade Controls (DAS). If the applicant disagrees with the DAS's determination, which must be issued within 30 days from the date the request for reconsideration was filed, the applicant may appeal the decision to the Assistant Secretary for Political-Military Affairs, although such appeals are rare.[57]

While the information contained in a CJ application is confidential, DDTC posts summaries of CJ final determinations on its website. Summaries include the model name, description, final determination date, final determination (USML or EAR), and manufacturer name, unless requested by the applicant not to do so.[58] The posted CJ final determinations are a useful tool for companies seeking to understand the classification of their products to review the classification of other products for which CJs have been requested and issued.

It is important to note that DDTC's jurisdiction over ITAR-controlled items is extremely broad and extends to the ITAR-controlled items

wherever they are located. In addition, under DDTC's "see-through rule," an ITAR-controlled item remains subject to the ITAR even after it is incorporated into a larger non-ITAR controlled system.

While the "see-through rule" has been DDTC's long-standing policy, this important concept was finally added to the text of the ITAR in March 2022 when the following language was added to section 120.11(c):[59]

> Defense articles described on the USML are controlled and remain subject to this subchapter following incorporation or integration into any item not described on the USML, unless specifically provided otherwise in this subchapter.[60]

As a result, a non-U.S. origin end-item incorporating ITAR-controlled components or technical data are subject to the ITAR and require authorization from DDTC before the non-U.S. item can be re-exported or transferred, even if the non-U.S. item was designed for civil end uses. The "see through" rule has resulted in some foreign companies trying to ensure that their products are "ITAR-free," that is, the products do not contain ITAR parts, components, or technical data, and in some cases "ITAR-free" is used as a marketing strategy in order to avoid being subject to the export controls jurisdiction of the ITAR.

2.7 Registration Requirements

To ensure that the U.S. government has current information regarding which entities are involved in the manufacture, export, and brokering of defense articles and services, DDTC maintains certain registration requirements. Specifically, as discussed next, and subject to few exemptions, any person who engages in the United States in the business of either manufacturing or exporting of defense articles or furnishing of defense services must register with DDTC, and any person subject to U.S. jurisdiction in any location that is engaged in brokering activities is required to register with DDTC.[61]

The only entities that are exempt from the registration requirement relating to the manufacture or export of defense articles or the furnishing of defense services are:

- Officers and employees of the U.S. government acting in an official capacity;

- Persons whose pertinent business activity is limited to the production of unclassified technical data only;
- Persons whose manufacturing and export activities are limited exclusively to activities licensed under the Atomic Energy Act of 1954, as amended; and
- Persons who engage only in the production of articles for experimental or scientific purposes, including research and development.[62]

With respect to brokering activities, the only persons that are exempt from registering with DDTC are:

- Employees of the U.S. Government acting in an official capacity;
- Employees of foreign governments or international organizations acting in an official capacity; and
- Persons exclusively in the business of financing, transporting, or freight forwarding, whose business activities do not also include brokering defense articles or defense services.[63]

Aside from these exempt entities, any U.S. person that engages in the manufacture or export of defense articles or the furnishing of defense services and any person subject to U.S. jurisdiction that performs brokering activities must register with DDTC. It is important to note that manufacturers of defense articles are required to register with DDTC, even if they do not export defense articles.[64] Registration with DDTC should not be used in marketing materials since it is simply a requirement that all manufacturers and exporters of defense articles must comply with and does not confer any rights or privileges. While a company may ask a supplier if it is registered with DDTC, which is reasonable from a compliance standpoint, DDTC encourages a company's registration number to be kept confidential.

To register, a company must submit to DDTC a Statement of Registration (Form DS-2032) using DDTC's online DECCS system. The registrant must also include a document evidencing that the company is authorized to do business in the United States (e.g., a state incorporation certificate or state certificate of good standing) and pay an annual registration fee.[65] Pursuant to DDTC's guidelines, the parent U.S. legal entity is required to register using the Form DS-2032, which must, among

other things, list all wholly owned or partially owned subsidiaries that manufacture or export defense articles or furnish defense services and provide information relating to the company's officers and directors.[66] The completed registration statement must be submitted by a senior officer of the applicant, which requires that a senior officer of the applicant be registered with DECCS.

Unless the information submitted to DDTC is incomplete or there are additional questions, DDTC will then notify the applicant of the registration fee to be paid. Once the registration fee has been paid DDTC will send a letter to the applicant via DECCSs providing the registration number (which remains the same from year-to-year) and requesting that the applicant maintain the following records that are required by section 122.5 of the ITAR:

> (1) The name of the "key senior officer" listed on the registration who will oversee the compliance program and be responsible for designating the direct employees who will serve as "empowered officials" at their place of employment, and
>
> (2) A list of qualified, direct employees who will serve as "empowered officials" by name, position, business unit, and their contact information.

Such "empowered officials" must be U.S. persons who are:

> (1) Directly employed by the applicant or a subsidiary in a position having authority for policy or management within the applicant's organization;
>
> (2) Legally empowered in writing by the applicant to sign license applications or other export approval requests on behalf of the applicant;
>
> (3) Understand the provisions and requirements of U.S. export control laws and regulations, including the AECA and the ITAR; and
>
> (4) Have independent authority to enquire into any aspect of a proposed export or temporary import by the applicant, verify the legality of the transaction and accuracy of the information to be submitted, and refuse to sign any license application or other approval request without prejudice or other adverse recourse.[67]

As discussed in the Darling Industries case in the enforcement section later in the chapter, it is important that the "empowered official" be independent, knowledgeable, and empowered.

A registrant must renew its registration with DDTC on an annual basis. DDTC will send the registrant a notice of the fee due for the following year's registration approximately 60 days prior to its expiration date. While

DDTC now processes new registrations and renewals of existing registrations in a matter of weeks, the registration renewal should be submitted to DDTC no earlier than 60 days prior to the expiration date of the current registration and no later than 30 days prior to the expiration date. In the event a registrant allows their registration to expire, the registrant must ensure that they do not engage in any ITAR-controlled exports or imports until the registration is reinstated by DDTC.

Registrants must notify DDTC in DECCS within five days of the effective date of any "material change" to its statement of registration. Such "material changes" include (1) a change in senior officers of the registrant; (2) changes to the registrant's name or address; (3) the establishment, acquisition, or divestment of a subsidiary or foreign affiliate; (4) the dealing in an additional categories of defense articles or services than those included on the DS-2032; or (5) the indictment, debarment, or denial of import-export privileges of a registrant, board member, or senior officer.[68] A registrant also is required to notify DDTC at least 60 days in advance of any intended sale or transfer of ownership or control to a foreign person.[69]

In addition, when a new entity is formed when a registrant merges with another company or acquires, or is acquired by, another company, the entity must submit a "5-day notice" to DDTC within five days of the event. The 5-day notice includes (1) the new firm name and all previous firm names being disclosed; (2) the registration number that will survive and those that are to be discontinued (if any); (3) the license numbers of all approvals on which unshipped balances will be shipped under the surviving registration number; and (4) amendments to agreements approved by DDTC to change the name of a party to those agreements.[70] Detailed information on registration statement changes are included on DDTC's website.

Due to the volume of authorizations requiring amendments or changes, DDTC has waived the requirement for amendments to change currently approved license authorizations and DDTC publishes on its website a list of name and address changes.

It also should be noted that DDTC registrants are required to maintain certain records concerning the manufacture, acquisition, and disposal of defense articles, technical data, brokering activities, and the provision of defense services.[71] Registrants must store such records in a way that is legible and, for electronic information, in a manner that prevents alterations

without a record of all changes and who made them.[72] In addition, registrants must track information regarding political contributions, fees, and commissions, and they must keep such records for five years after the expiration of the registrant's approval.[73] As discussed in the enforcement cases that follow, DDTC has entered into number of Consent Agreements with companies for failing to comply with the political contribution, fees, and commissions recordkeeping requirements set forth in Part 130 of the ITAR.

2.8 Exportation of Defense Articles

Pursuant to section 123.1 of the ITAR, any person who intends to export, re-export, or temporarily import a defense article into the United States must obtain approval from DDTC prior to the export, re-export, or the temporary import, unless the export, re-export, or temporary import qualifies for an exemption specified under the ITAR.[74] The ITAR requires that applications for the export or temporary import of unclassified defense articles must be made in the following manner:

(1) Applications for licenses for permanent export must be made on Form DSP-5;

(2) Applications for licenses for temporary export must be made on Form DSP-73; and

(3) Applications for licenses for temporary import must be made on Form DSP-61.[75]

The ITAR further specifies that applications for the export or temporary import of classified defense articles or classified technical data must be made on a Form DSP-85.[76] With the exception of Form DSP-85 license applications, all of the other referenced license applications just referenced may be submitted via DECCS, DDTC's web-based licensing system.

A DSP-5 application relating to a commercial sale must be accompanied by a copy of a purchase order, a letter of intent, or other appropriate documentation.[77] If the export involves articles or services valued at $500,000 or more being sold commercially to or for the use of the armed forces of a foreign country or international organization, a statement concerning the payment of political contributions, fees, and commissions must accompany the export application.[78]

With respect to applications involving defense articles designated in the USML as SME (*) or classified defense articles or services, the exporter is required to obtain from the foreign consignee and end user a Non-transfer and Use Certificate (Form DSP-83), pursuant to which the foreign consignee, the end user, and the applicant agree not to re-export such equipment outside the authorized country of destination and not to resell or otherwise dispose of the licensed item to any foreign person, except as may be authorized by DDTC.[79] In addition, DDTC may require the applicant to provide a Form DSP-83 for the export of any defense articles to any destination, and when the foreign customer is a nongovernmental foreign end user, DDTC may also require that the foreign government be a signatory to the Form DSP-83.[80]

It is the general policy of the U.S. government to deny licenses and other approvals for exports and temporary imports of defense articles and defense services destined for or originating in certain countries, commonly referred to as “proscribed countries.” This policy applies to all of the countries specified in section 126.1 of the ITAR, which can change from time to time. The countries that are currently subject to a general policy of denial include Belarus, Burma (Myanmar), China, Cuba, Iran, North Korea, Syria, and Venezuela.[81]

The countries that are currently subject to a policy of denial, except for certain limited types of ITAR-related activities currently include Afghanistan, Cambodia, Central African Republic, Cyprus, Democratic Republic of Congo, Eritrea, Ethiopia, Haiti, Iraq, Lebanon, Libya, Russia, Somalia, South Sudan, Sudan, and Zimbabwe.[82]

A current list of proscribed countries and countries currently subject to restrictive licensing policies is available on DDTC’s website and in the latest version of the Code of Federal Regulations and should be checked prior to submission of a license application in DECCS.

Licenses issued by DDTC are valid for a period of four years.[83] The license expires when the total value or quantity authorized has been shipped or when the date of expiration has been reached, whichever occurs first. Specific procedures for the filing of Electronic Export Information for shipments containing ITAR-controlled goods via the Automated Export System (AES), as well as for filing, retaining, and returning licenses, are set forth in section 123.22 of the ITAR.[84] However, section 123.22 should be

read with care, since some of its provisions have never been put into effect. For example, DDTC intended to set up an electronic notification process for export of technical data, as noted in section 123.22(3)(i), that was exported pursuant to license or exemption, but this process has never been implemented, although exporters are required to notify DDTC of the first export of technical data pursuant to DDTC agreements via a notification letter.

Minor amendments to approved licenses can be sought and obtained from DDTC for small changes, such as corrections of typographical errors, a change in the source of commodity, and the addition of a U.S. freight forwarder or U.S. consignor.[85] However, amendments for more significant changes, such as additional quantity; changes in the kind of commodity covered; alterations to the country of ultimate destination, end use, end user, or foreign consignee; and/or extension of duration, will be rejected and a new license must be sought and obtained from DDTC.[86]

DDTC authorization is required prior to the re-export, resale, retransfer, transshipment, or disposal to a different end user, end use, or destination that is not specified in the license.[87] Re-export, retransfer, and disposition requests must be submitted to DDTC in DECCS using the DS-6004 form, which is the only ITAR authorization that a non-U.S. company can obtain. A company does not have to be registered with DDTC to submit the DS-6004 form; however, registration with DECCS is required. The DS-6004 re-export/retransfer form requires the following information to be submitted: the DDTC license number under which the defense article was previously authorized for export from the United States; a description of the defense article, including quantity and value; a description of the new end use; and the new end user.[88] It is highly recommended that the applicant include a transmittal letter with details on the proposed re-export/retransfer.

DSP-5 license applications are also used as the authorization for ITAR-controlled technical data since all technical data exports are considered to be permanent exports. DSP-5s can also be used to obtain prior approval for other types of ITAR controlled information, such as marketing presentations (commonly referred to as a “marketing license”) and the training of foreign persons where it would be impractical to obtain a Technical Assistance Agreement (TAA).

DSP-5s are also used to obtain authorization to permit the transfer of ITAR-controlled technical data to foreign persons that are employed by

U.S. companies (referred to as “deemed exports”).[89] A license approved for foreign person employment is valid only for a period of four years or until expiration of their authorized stay from U.S. Department of Homeland Security (DHS), whichever is shorter.

There also are a number of exemptions set forth under the ITAR that permit unclassified defense articles to be exported without obtaining a license from DDTC. Most of the exemptions are applicable to U.S. companies only. Some pertinent exemptions that are used for such purposes include:

- Components or spare parts for a defense article previously exported with DDTC approval so long as the value does not exceed $500 in a single transaction;[90]
- Exports, re-exports, retransfers of defense articles conducted by or for use by U.S. government agencies under specified circumstances;[91]
- Unclassified components, parts, tools, or test equipment exported to a subsidiary, affiliate, or facility owned or controlled by a U.S. person if the components, parts, tools, or test equipment are to be used for manufacture, assembly, testing, production, or modification subject to certain conditions;[92]
- Defense articles being exported in furtherance of a technical assistance agreement, manufacturing license agreement, or distribution agreement;[93]
- Unclassified models or mock-ups of defense articles so long as the models or mock-ups are non-operable, do not reveal controlled technical data, and do not contain USML components;[94]
- Unclassified defense articles exported to any public exhibition, trade show, air show, or related event if the article has previously been licensed for such an event and the license is still valid;[95]
- Re-exports and retransfers of U.S.-origin components incorporated into a foreign defense article to a government of a NATO country, or the governments of Australia or Japan to NATO, Australia, or Japan;[96]
- Certain items on the USML may be exported to Canada without a license when the article is for end use in Canada by Canadian federal or provincial governmental authorities or by Canadian companies that

are registered with the government of Canada under the Defense Production Act, or the item will be returned to the United States; and[97]

- Temporary exports of certain firearms, ammunition, and body armor for the personal use of a U.S. citizen or permanent resident subject to safeguarding, use, recordkeeping, and other conditions.[98]

Exporters and importers of ITAR-controlled items should carefully review the specific requirements and limitations before seeking to use the exemptions, including the recordkeeping requirements. The Society for International Affairs' ITAR Exemptions Handbook is a good resource for reviewing the requirements associated with the use of ITAR exemptions.[99]

2.9 Exportation of Defense Services and Technical Data

Like the export of ITAR-controlled hardware, the export of defense services and technical data generally require approval from DDTC, unless an ITAR exemption can be used. The ITAR provides for the use of certain types of agreements for the export of defense services and technical data, the most common of which is a Technical Assistance Agreement (TAA).[100] TAAs are typically used in situations in which the exporter anticipates the need for an unrestricted two-way exchange of technical data with a foreign person or entity over a period of time within certain predetermined technical parameters. TAAs are structured as contracts for the exchange of ITAR-controlled technical data with mutual rights and obligations based on specific required clauses that are required by the ITAR (referred to as "verbatim clauses") and contained in DDTC's "Guidelines for Preparing Agreements" found on DDTC's website. Once the draft TAA has been agreed to between the parties, the TAA is submitted to DDTC in DECCS using a DSP-5 as the licensing "vehicle" to transmit the TAA to DDTC for review by DDTC's licensing officers and the reviewing agencies, including the U.S. Department of Defense. Once the TAA has been approved by DDTC, the final TAA is then signed by all parties. The applicant must provide DDTC with an electronic copy of the signature page plus a cover letter identifying all of the current signatories within 30 days from the date on which the TAA was approved by DDTC. Once the TAA has been

approved and signed, the U.S. parties to the TAA may commence the activities authorized by the TAA.

A Manufacturing License Agreement (MLA) is an agreement whereby a U.S. person grants a foreign person an authorization to manufacture defense articles abroad.[101] An MLA covers the export of technical data or defense articles or the performance of a defense service, or the use by the foreign person of technical data or defense articles previously exported by the U.S. person.[102] It also can establish a sales territory in which defense articles manufactured abroad may be sold.

A Warehouse and Distribution Agreement (WDA) is an agreement to establish a warehouse or distribution point abroad for defense articles to be exported from the United States for subsequent distribution to entities in an approved sales territory.[103] Both MLAs and WDAs require the filing of annual reports on sales of the defense articles made abroad to DDTC.[104]

The following information must be included in all proposed agreements.

- A description of the defense articles to be manufactured and all defense articles (including technical data) to be exported;
- A specific description of any assistance or technical data to be provided (including design and manufacturing know-how) and any manufacturing rights to be granted;
- The duration of the agreement, which can be up to ten years; and
- The specific countries where manufacturing, production, processing, or sale is to be licensed.[105]

As noted, agreements also must include certain specified clauses.[106] These clauses are contained in sections 124.8 and 124.9 of the ITAR and must be copied into the agreements verbatim.

While TAAs are normally valid for ten years, the U.S. applicant of a TAA or MLA must provide written notice to DDTC of the impending termination of the agreement at least 30 days prior to the expiration date of such agreement.[107] Additional filing requirements are set forth under section 123.22 of the ITAR.[108]

In some instances, it may be appropriate to submit a DSP-5 to seek authorization to export technical data. For example, it may be beneficial to submit a DSP-5 application when seeking to allow a U.S. person to be able

to disclose ITAR-controlled technical data to foreign persons in connection with a plant visit or an international conference that is not open to the public or when desiring to export technical data for purposes of filing a patent application in a foreign country when the technical data required exceeds that required for a patent application filing in the United States.[109]

There also are a number of exemptions set forth under the ITAR that permit technical data and defense services to be exported without a license from DDTC, which are primarily included in sections 123.16 and 125.4 of the ITAR. Some pertinent exemptions that are frequently used for such purposes include:

- Technical data in furtherance of an approved Manufacturing License Agreement or Technical Assistance Agreement;[110]
- Technical data in furtherance of a contract between the exporter and an agency of the U.S. government, if the contract provides for the export of the data and such data does not disclose the details of design, development, production, or manufacture of any defense article;[111]
- Technical data to be disclosed pursuant to an official written request or directive from the DOD;[112]
- Copies of technical data previously authorized for export to the same recipient, including revisions provided that the revisions are solely editorial and do not add to the content of the technology previously authorized for export;[113]
- Technical data sent by a U.S. corporation to a U.S. employee overseas or to a U.S. government agency subject to certain limitations;[114]
- Technical data in the form of basic operations, maintenance, and training information relating to a defense article lawfully exported or authorized to export to the same recipient;[115]
- Technical data for which the exporter has been granted an exemption in writing pursuant to an arrangement with the DOD, DOE, or NASA;[116]
- Technical data approved for public release by the cognizant U.S. government department or agency;[117] and

- Defense services and related unclassified technical data necessary to respond to a written request from the DOD for a quote or bid proposal are exempt when transmitted to nationals of NATO countries, Australia, Japan, and Sweden.[118]

Finally, a commonly used exemption authorizes the temporary import into the United States and the subsequent export from the United States of ITAR-controlled items for overhaul, service, and/or repair.[119]

There are numerous requirements and limitations associated with each of the preceding exemptions. For example, section 123.26 of the ITAR requires that the exporter maintain a record of each export of technical data made via an exemption, including a description of the unclassified technical data, the name of the recipient end user, the date and time of the export, and the method of transmission.[120]

As noted earlier, companies should carefully review the requirements and limitations set forth under the ITAR when using exemptions and may wish to consult the SIA's ITAR Exemptions Handbook.

There are additional authorizations required for U.S. Persons Abroad (USPAB) who reside outside of the United States, are employed by a foreign company involved with defense articles and provide defense services to their foreign employer or other foreign parties.

DDTC has issued on its website *Guidance for USPAB Authorizations Requests* and various FAQs describing the process for USPABs to obtain authorizations to provide defense services.

While individuals residing outside of the U.S. do not have to register with DDTC, the USPAB authorization must be submitted in DECCS via a Form DS-6004, along with a submission letter using DDTC's recommended template, resume, detailed job description, an ITAR section 126.13(a) certification, and other information to assist DDTC in evaluating the case.

In many cases, the USPAB authorizations contain numerous provisos that may make it difficult or impractical for the USPAB and the foreign employer to comply with.

2.10 Brokering Under the ITAR

In addition to exports and temporary imports of defense articles and defense services, the ITAR also control the "brokering" of defense articles and

defense services.[121] Under the ITAR, a "broker" is defined as any U.S. person, wherever located, any foreign person located in the United States, or any foreign person located outside the United States where the foreign person is owned or controlled by a U.S. person that engages in the business of "brokering activities."[122] The term "brokering activities" is broadly defined as "any action on behalf of another to facilitate the manufacture, export, permanent import, transfer, reexport, or retransfer of a U.S. or foreign defense article or defense service, regardless of its origin."[123] This includes, among other things, financing, insuring, transporting, or freight forwarding defense articles or service as well as "soliciting, promoting, negotiating, contracting for, arranging, or otherwise assisting in the purchase, sale, transfer, loan, or lease of a defense article or defense service."[124]

Persons who engage in "brokering activities" are required to register with DDTC via DECCS on an annual basis.[125] There are limited exceptions to the registration requirement, including:

- Employees of foreign governments or international organizations acting in an official capacity; and
- Persons exclusively in the business of financing, transporting, or freight forwarding, whose business activities do not also include brokering defense articles or defense services.[126]

Additional details and guidance regarding registration requirements and procedures are set forth in Section 2.7.

Brokers must obtain prior approval from DDTC before engaging in certain brokering activities. Section 129.4 of the ITAR provides that prior approval from DDTC is required before a person can engage in brokering activities involving certain defense articles and services, such as those described in specified subcategories of USML Categories I, II, III, IV, VI, VII, VIII, XII, XIV XX, and XXI.[127] Section 129.5 of the ITAR identifies the limited situations when prior approval to engage in brokering activities is exempt from the approval requirements, such as when the brokering activities are undertaken pursuant to a contract between the broker and a U.S. government agency.[128]

As of this writing, requests for prior approval must be submitted to DDTC in hard copy, although it is contemplated that prior approval request will eventually be able to be submitted via DECCS. The current procedures for obtaining prior brokering approvals are detailed in section 129.6 of the ITAR and are submitted in the form of a letter. The brokering request must include details on the parties to the proposed transaction, information on the defense articles and technical data, and the specific end use(s) and end user(s).[129] The proposed brokering activity may not be engaged in until the approval is issued by DDTC.

If doubt exists as to whether an activity is a brokering activity within the scope of the ITAR or whether the prior approval requirements apply, parties can seek written guidance from DDTC, using the same procedures for submitting advisory opinions.[130]

Brokers also are subject to certain reporting requirements under the ITAR. Specifically, any person who is required to register as a broker with DDTC must file a report to DDTC on an annual basis.[131] For persons already registered as a broker, the brokering report must be submitted to DDTC with the brokering registration renewal submission and must cover all brokering activities undertaken within the past 12 months that were not the subject of a prior brokering report. Brokering reports must cover all brokering activity up to three months prior to the expiration of the brokering registration.[132]

2.11 ITAR Requirements Concerning Fees, Commissions, and Political Contributions

Another section of the ITAR warranting special attention relates to fees, commissions, and political contributions that are paid in connection with the sale of defense articles or defense services and regulated by Part 130 of the ITAR.[133] As discussed later in the chapter, there are important reporting requirements relating to such payments, and significant penalties can be, and have been, imposed by DDTC when companies have filed inaccurate reports or have failed to file reports at all.

By way of background, due to concerns on the use of agents, advisers, and consultants to obtain business in the international defense trade in 1976 the U.S. Congress amended the Arms Export Control Act requiring the

State Department to require the reporting of certain fees, commissions, and political contributions associated with sales of defense articles and services.[134]

The Part 130 reporting requirements apply to "applicants" who have applied for licenses or other approvals from DDTC for the export, re-export, or retransfer of defense articles or defense services valued in an amount of $500,000 or more, which are being sold commercially to or for the use of the armed forces of a foreign country or international organization (i.e., direct commercial sales).[135] The reporting requirements also apply to "suppliers" and "vendors" who are involved in direct commercial sales or foreign military sales. "Suppliers" are defined in Part 130 to mean any person who enters into a contract with the DOD for the sale of defense articles or defense services valued in an amount of $500,000.[136] "Vendors" include (1) any distributor or manufacturer who, directly or indirectly, furnishes to an applicant or supplier defense articles valued at $500,000 or more that are end-items or major components; or (2) any person who, directly or indirectly, furnishes to an applicant or supplier defense articles or defense services valued at $500,000 or more when such defense articles or defense services are to be delivered or incorporated into defense articles or defense services to be delivered to or for the use of the armed forces of a foreign country or international organization under a sale requiring a license from DDTC or a sale pursuant to a contract with the DOD.[137]

Information on the payment of fees, commissions, and political contributions are obtained by DDTC in several ways. First, when submitting a license application or other approval from DDTC in connection with the sale of defense articles or defense services via DECCS, the application form includes a section on "Compliance with 22 CFR 130" that asks several questions. An applicant must state whether the transaction meets the $500,000 threshold. If the transaction meets the $500,000 threshold, the applicant must then state whether the applicant or its vendors have paid, offered, or agreed to pay political contributions, fees, or commissions in the amounts specified in section 130.9(a) of the ITAR, which currently include political contributions in an aggregate amount of $5,000 or more or fees and commissions in aggregate amount of $100,000 or more. If such fees and commissions have been paid, the applicant must include in the application the detailed information required under section

130.10 of the ITAR.[138] This requirement applies regardless of whether such political contributions or fees and commissions are paid directly by the applicant or any of its vendors or by anyone on their behalf or at their direction.[139]

The information that must be provided includes:

> (1) The total contract price of the sale to the foreign purchaser;
>
> (2) The name, nationality, address, and principal place of business of the applicant or the supplier, and, if applicable, the employer and title;
>
> (3) The name, nationality, address, and principal place of business, and if applicable, employer and title of each foreign purchaser, including the ultimate end user involved in the sale;
>
> (4) The amount of each political contribution paid, or offered or agreed to be paid, or the amount of each fee or commission paid, or offered or agreed to be paid;
>
> (5) The date(s) on which each reported amount was paid, or offered or agreed to be paid;
>
> (6) The recipient of each such amount paid, or the intended recipient if not yet paid;
>
> (7) The person who paid, or offered or agreed to pay such amount;
>
> (8) The aggregate amount of political contributions and of fees or commissions, respectively, which shall have been reported.[140]

When providing information regarding each recipient, the following information must be provided: (1) name; (2) nationality; (3) address and principal place of business; (4) its employer and title; and (5) its relationship, if any, to the applicant, supplier, or vendor, and to any foreign purchaser or end user.[141] However, the information regarding the recipients does not need to be provided if the payments do not exceed $2,500 in the case of political contributions or $50,000 in the case of fees or commissions.[142] Any person filing such a report may request that confidential business information contained in the report not be published, divulged, disclosed, or made known in any manner, and no such confidential business information may be made known in any manner unless authorized by law.[143]

It should be noted that applicants and suppliers who file such reports have an obligation to file supplementary reports in certain circumstances.[144] For example, every applicant or supplier who is required under section 130.9 to furnish the information specified in section 130.10 must submit a

supplementary report in connection with each sale in respect of which applicant or supplier has previously been required to furnish information if any political contributions aggregating $2,500 or more or fees or commissions aggregating $50,000 or more not previously reported or paid, or offered or agreed to be paid by applicant or supplier or any vendor.[145]

To determine their reporting requirements, applicants and vendors must determine from each of their applicable vendors a full disclosure by the vendor of all political contributions and fees or commissions paid by the vendor with respect to the sale at issue.[146] Any vendor to whom such a request is made must provide a response within 20 days of the initial request, although if the vendor believes that furnishing the information required would unreasonably risk injury to the vendor's commercial interests, the vendor may provide an abbreviated statement that discloses only the aggregate amount of all political contributions and the aggregate amount of all fees and commissions that have been paid, or offered or agreed to be paid, by the vendor with respect to the sale.[147] If no response is received from the vendor within 25 days of its request to the vendor, the applicant or supplier must file a written submission with DDTC attesting to the applicant's or supplier's attempt to obtain from the vendor the initial statement required under section 130.10(a) of the ITAR, the vendor's failure to comply with the request, and the amount of time that has elapsed between the date of the applicant's or supplier's request and the date of the signed submission to DDTC.[148] Even in such instances, the applicant or supplier still must file with DDTC the report required pursuant to section 130.9 of the ITAR.[149]

In addition, to determine their reporting requirements, applicants, suppliers, and vendors must obtain from each person to whom they have paid, or offered or agreed to pay a fee or commission relating to a covered sale, a statement containing a full disclosure by such a person of all political contributions paid, or offered or agreed to be paid, by itself or on its behalf, or at its discretion, relating to such sale.[150] Moreover, applicants, suppliers, and vendors also may request that each person to whom a fee or commission is paid to provide periodic reports of its political contributions to the extent that such reports may be necessary for the applicants, suppliers, and vendors to comply with their ITAR reporting requirements.[151] Any person who provides such information may request

that confidential business information not be published, divulged, disclosed, or made known in any manner, and no such confidential business information may be made known in any manner unless authorized by law.[152]

There are recordkeeping requirements associated with such reports. Specifically, each applicant, supplier, and vendor must maintain a record of any information that it was required to furnish or obtain under Part 130 of the ITAR for at least five years following the date of the report to which they pertain.[153]

To assist companies with their Part 130 reporting requirements, DDTC has included a "Part 130 Decision Tree Tool" on its website.[154]

Significant penalties can be imposed by DDTC for the filing of materially inaccurate reports or the failure to file such reports at all. For example, in 2020, Airbus SE and its affiliates (Airbus) entered into a Consent Agreement with DDTC pursuant to which Airbus agreed to pay a civil penalty of $10 million for numerous violations of the ITAR, including the Part 130 requirements on reporting and recordkeeping of political contributions, fees, and commissions.[155] This civil penalty was in addition to $237.7 million in criminal penalties that Airbus agreed to pay for violations of the Arms Export Control Act and millions more in additional criminal penalties for violating anti-corruption laws.[156] In view of the potential civil and criminal penalties that can be imposed, exporters must understand and follow the ITAR's Part 130 provisions relating to brokering and reporting of political contributions, fees, and commissions.

2.12 Penalties and Enforcement

Significant penalties can be imposed for violations of the AECA and the ITAR. DDTC's Office of Defense Trade Controls Compliance is responsible for civil enforcement of the ITAR, while the U.S. Department of Justice handles criminal matters.

The maximum civil penalties for engaging in unlicensed exports and for most other violations of the ITAR in 2022 was $1,272,251 per violation. This amount is adjusted each year pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990.[157] Criminal penalties can be as high as $1 million and/or up to 20 years of imprisonment per violation.[158] DDTC

also can debar companies and individuals from participating directly or indirectly in the export of defense articles or the furnishing of defense services.[159] In addition, any attempt to export defense articles in violation of the ITAR can result in the seizure and forfeiture of the defense articles.[160] DDTC also possesses the authority to deny, suspend, or revoke licenses and registrations on the basis of conviction or indictment under the criminal statutes listed in section 120.27 of the ITAR or in other circumstances listed in section 126.7 of the ITAR.[161]

As discussed in Section 2.13, which follows, DDTC strongly encourages voluntary disclosures and most cases involving violations of the ITAR are closed without any civil penalty being imposed by DDTC. However, as indicated by the Airbus SE Consent Agreement in 2000, DDTC will not hesitate in filing a charging letter against a company when there are significant, numerous, and systemic violations of the ITAR. DDTC is also likely to commence a civil penalty action when the violations involve exports to a proscribed country, such as China or Iran, or when DDTC wishes to inform the defense industry of a particular issue, such as in the *Darling Industries, Inc*. case described next.

While the full text of ITAR-related Consent Agreements and related documents can be found on DDTC's website, some of the recent cases involving violations of the ITAR include the following:

- In 2022, California-based Torrey Pines Logic, Inc., and its chief executive officer were charged with five violations of the ITAR, including the unauthorized export and unauthorized attempted export of defense articles, involvement in ITAR-controlled activities while Torrey Pines was ineligible to do so, and failure to maintain required records. The Consent Agreement required Torrey Pines to appoint a Special Compliance Officer, perform an export controls jurisdiction and classification review, improve its policies and procedures, conduct an external audit, and pay a $840,000 fine (of which $420,000 was suspended and may be applied toward the company's remedial compliance costs).
- In 2021, Keysight Technologies, Inc. entered into a Consent Agreement settling allegations that it violated the ITAR in connection with unauthorized exports of technical data and software used for testing radar equipment to various countries, including a proscribed

destination. Under the terms of the 36-month Consent Agreement, Keysight agreed to pay a civil penalty of $6,600,000. DDTC agreed to suspend $2,500,000 of this amount on the condition that the funds will be used for DDTC-approved remedial compliance measures. Keysight was also required to hire an outside Special Compliance Officer for a term of two years and conduct an external audit to assess and improve its compliance program.

- Also in 2021, Honeywell International, Inc. settled allegations that it violated the ITAR in connection with unauthorized exports and retransfers of technical data resulting from the failure to exercise appropriate internal controls. Under the terms of the 36-month Consent Agreement, Honeywell agreed to pay a civil penalty of $13 million. DDTC agreed to suspend $5 million of this amount on the condition that the funds would be used for DDTC remedial compliance measures to strengthen Honeywell's compliance program. In addition, Honeywell was required to engage an external Special Compliance Officer to oversee the Consent Agreement, conduct one external audit of its compliance program, and implement additional compliance measures.
- In 2020, Airbus SE settled allegations that it violated the ITAR in connection with the provision of false statements on authorization requests; the failure to provide accurate and complete reporting on political contributions, commissions, or fees that it paid, or offered or agreed to pay, in connection with sales; the failure to maintain records involving ITAR-controlled transactions; and the unauthorized re-export and retransfer of defense articles. Under the terms of the 36-month Consent Agreement, Airbus SE agreed to pay a civil penalty of $10 million. DDTC agreed to suspend $5 million of this amount on the condition the funds will be used for DDTC-approved remedial compliance measures. In addition, Airbus SE was required to appoint an external Special Compliance Official to oversee the Consent Agreement, conduct two external audits of its compliance program, and implement additional compliance measures.
- In 2019, AeroVironment, Inc. settled allegations that it violated the ITAR in connection with unauthorized exports of defense articles and technical data; failed to properly maintain records involving ITAR-controlled transactions; and violated the provisos, terms, and

conditions of export authorizations. AeroVironment agreed to pay $1 million in civil penalties, of which $500,000 was suspended if the company applied that amount to authorized remedial compliance costs. DDTC also mandated the appointment of a Special Compliance Officer, the conduct of an external audit, and enhanced compliance measures. AeroVironment voluntarily disclosed the alleged violations to DDTC.

- In 2019, L3Harris Technologies, Inc. settled allegations that it violated the ITAR in connection with unauthorized exports of defense articles, including technical data in the form of software; the provision of a false Part 130 statement on a Technical Assistance Agreement; the violation of export license provisos; the violation of terms or conditions of multiple licenses and agreements; and various violations caused by systemic administrative issues. L3Harris Technologies agreed to pay $13 million in civil penalties, of which $6,500,000 was suspended if the company applied that amount to authorized remedial compliance costs. DDTC also mandated the appointment of a Special Compliance Officer; the completion of two external audits; a classification review of all of the company's ITAR-regulated items; and strengthened compliance policies, procedures, and training. Many of the alleged violations were voluntarily disclosed to DDTC.
- In 2019, Darling Industries, Inc. settled allegations that it violated the ITAR in connection with unauthorized exports of defense articles and technical data; the unauthorized provision of defense services; and the failure to appoint a qualified Empowered Official. This was the first time that DDTC charged a company with failing to appoint a qualified Empowered Official. Darling Industries agreed to pay $400,000 in civil penalties, of which $200,000 was suspended if the company applied that amount to authorized remedial compliance costs. DDTC also mandated the appointment of an Internal Special Compliance Officer, the completion of one external audit, a classification review of the company's ITAR-regulated items. Many of the alleged violations were voluntarily disclosed to DDTC.

2.13 Voluntary and Mandated Disclosures

Companies can seek to mitigate potential penalty exposure for violations of the ITAR by filing voluntary disclosures, which are "strongly encouraged" by DDTC, and are a common practice by ITAR-regulated companies.[162] The benefit for submitting a voluntary disclosure is that DDTC "may consider a voluntary disclosure as a mitigating factor in determining the administrative penalties, if any, that should be imposed."[163] In practice, most voluntary disclosures filed with DDTC do *not* result in the imposition of civil penalties and the cases are closed with a warning letter (referred to as a "closing letter"). For example, from 2018 through 2020, DDTC received more than 600 voluntary disclosures per year, but concluded civil penalty cases on only five companies during that same time period.

The procedures for filing a voluntary disclosure with DDTC are set forth in section 127.12 of the ITAR.[164] This provision states that any person wanting to disclose information that constitutes a voluntary disclosure should "initially notify" DDTC "immediately after a violation is discovered and then conduct a thorough review of all defense trade transactions where a violation is suspected."[165]

If an initial disclosure is filed, the full disclosure setting forth all of the pertinent facts must be submitted to DDTC within 60 calendar days from the date of the letter from DDTC acknowledging receipt of the initial disclosure was filed, unless an extension is granted by DDTC.[166] Extensions are commonly granted but must be submitted to DDTC in writing prior to the deadline.

In order to initiate the voluntary process, a company should send a letter to the Office of Defense Trade Controls Compliance that outlines the suspected or alleged violations and commits to providing a final disclosure after completing an investigation into the facts. The initial notification need not be more than two or three pages in length so long as it includes a sufficient summary of the suspected ITAR violations. Alternatively, a company can choose to file a full voluntary disclosure at the outset, if the facts are readily available and can be submitted in a timely manner after the violation occurred.

As of this writing all voluntary disclosures must be sent to DDTC via email or in hard copy form to DDTC via mail or an overnight courier service. However, it is anticipated that, at some point in the near future, DDTC will accept voluntary disclosures that are submitted via DECCS.

Section 127.12(c)(2) of the ITAR states that a full (or final) voluntary disclosure should:

- Describe with precision the circumstances surrounding the suspected violations (e.g., a detailed explanation of why, when, where, and how the violation occurred);
- Provide the identities and addresses of all persons known or suspected to be involved in the activities that resulted in the suspected violation;
- Identify the kinds of defense articles and defense services involved, including their USML classifications;
- Discuss what corrective actions and new compliance initiatives, if any, have been implemented to address the causes of the suspected violations; and
- Provide the name of the person making the disclosure and a point of contact, if different, should further information be needed by DDTC.[167]

The full voluntary disclosure should include substantiating documentation, including licensing, shipping, and any other relevant documents.[168] Both the initial and full voluntary disclosure must include a certification executed by one of the company's empowered officials stating that all of the representations made in connection with the voluntary disclosure are true and correct to the best of the person's knowledge and belief.[169]

It should also be noted that in some cases, the disclosures are not voluntary. Specifically, section 126.1(e) of the ITAR requires any person who knows or has reason to know of such a proposed or actual sale, or transfer, of such articles, services, or data to a proscribed section 126.1 country to "immediately inform" DDTC.[170] Thus, if a company has exported a defense article to China or released technical data to a Chinese national employee, the company is required to notify DDTC immediately and failing to do so is a separate violation of the ITAR.

In addition, there may be situations where a company has to state in its license application that it had unlicensed exports to the same ultimate consignee in the past since failing to explain this would mean that the company would file a license application with a material omission, which again would be a violation of the ITAR. In such cases, companies should

file a voluntary disclosure and cross-reference the voluntary disclosure case number in the license application.

Finally, DDTC may require a company to submit a voluntary disclosure if it has reason to know that the company violated the ITAR and had not previously disclosed the violations. These disclosures are referred to as "directed disclosures" and are not treated as a mitigating factor by DDTC.

2.14 Compliance Program Guidelines

In December 2022, DDTC issued new *Compliance Program Guidelines* (CPG) that contain detailed information on the elements of an effective ITAR compliance program in an effort to assist the defense industry and universities that manufacture, export, broker, or temporarily import defense articles and defense services in helping to mitigate the risk of ITAR violations.

DDTC has identified the following elements as critical for an effective ITAR compliance program:

1. Management Commitment
2. DDTC Registration, Jurisdiction and Classification, Authorizations, and Other ITAR Activities
3. Recordkeeping
4. Reporting and Addressing Violations
5. Training
6. Risk Assessment
7. Audits and Compliance Monitoring
8. Export Compliance Manual and Templates

While companies involved in ITAR regulated activities are not required to adopt the CPG, U.S. companies that register with DDTC are required to state whether they have written policies and procedures for compliance with the ITAR, including the recordkeeping requirements in section 122.5 of the ITAR.

2.15 Conclusion

Understanding and complying with the ITAR is important to all persons, whether in the United States or abroad, that are involved in ITAR-regulated activities. Given that the ITAR and USML are updated on a regular basis, it is important to regularly monitor DDTC's website and review the most updated version of the ITAR prior to engaging in any ITAR regulated activity. As discussed earlier, failure to comply with the ITAR can be costly and can result in the imposition of severe penalties.

---

1. This chapter was co-authored by Geoffrey M. Goodale and Douglas N. Jacobson. Mr. Goodale is a partner in the Washington, DC office of Duane Morris LLP. His practice focuses on export controls, economic sanctions, import compliance, trade litigation, international intellectual property rights protection, foreign direct investment, cybersecurity, and compliance counseling to government contractors. He is a past Co-Chair of the ABA International Law Section's Export Controls and Economic Sanctions Committee and International Trade Committee. Mr. Jacobson is a partner in the Washington, DC office of Jacobson Burton Kelley PLLC. His practice focuses on export controls, economic sanctions, customs matters, and other international trade compliance and enforcement matters. Mr. Jacobson is an adjunct professor of sanctions and export controls at the American University Washington College of Law in Washington, DC and uses this book as the course's textbook.

2. The ITAR controls the export, re-export, and retransfer of "defense articles" included on the USML, including end-items and certain parts, components, accessories, and attachments. 22 C.F.R. § 120.6. The ITAR also controls the export, re-export, retransfer (including release) of "technical data" to "foreign persons" (i.e., information, other than software defined in section 120.10(a)(4) of the ITAR), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. 22 C.F.R. § 120.10. The ITAR also controls the provision of "defense services," which includes having a U.S. person furnish to a foreign person assistance (including training) related to defense articles or ITAR-controlled technical data or provide or any military training to foreign units or forces. 22 C.F.R. § 120.9.

3. The statutory authority for the ITAR is the Arms Export Controls Act of 1976, as amended (AECA). *See* 22 U.S.C. § 2778.

4. Neutrality Act of 1935, 49 Stat. 1081.

5. *Id*.

6. Later renamed the Division of Controls, the Munitions Division, Office of Munitions Controls, Office of Defense Trade Controls, and ultimately the Directorate of Defense Trade Controls. *See* history.state.gov/departmenthistory/timeline.

7. Neutrality Act of 1939, 54 Stat. 11.

8. Mutual Security Act of 1951, 65 Stat. 644, 645.

9. Mutual Security Act of 1954, 68 Stat. 832, 848.

10. *Id*.

11. 20 Fed. Reg. 6250 (Aug. 26, 1955).

12. Foreign Military Sales Act of 1968, 82 Stat. 1320, 1322–25.

13. Arms Export Control Act of 1976 (AECA), 90 Stat. 744 (codified at 22 U.S.C. § 2778).

14. 42 Fed. Reg. 4311 (Jan. 7, 1977).

15. 49 Fed. Reg. 47682 (Dec. 6, 1984). The current version of the ITAR are codified at 22 C.F.R. pts. 120–130.

16. White House press release dated Dec. 9, 2010.

17. https://2016.export.gov/ecr/index.asp.

18. Secretary of Defense Robert M. Gates' speech before the Business Executives for National Security, April 20, 2010, https://fas.org/sgp/news/2010/04/gates-export.html.

19. *Id*.

20. 78 Fed. Reg. 22,740 (Apr. 16, 2013).

21. 85 Fed. Reg. 2,819 (Jan. 23, 2020).

22. *See* 22 C.F.R. § 121.1 for a description of the ITAR's "Order of review."

23. *See* 22 C.F.R. § 120.1(b)(2).

24. 22 C.F.R. § 127.4.

25. *Id*. § 127.5. Pursuant to Executive Order 13869 of April 24, 2019, the U.S. Department of Defense was reorganized, and DSS was renamed as the Defense Counterintelligence and Security Agency (DCSA). *See* 84 Fed. Reg. 18,125 (Apr. 29, 2019).

26. *See* 22 C.F.R. § 120.2.

27. *See* www.atf.gov. The U.S. Munitions Import List (USMIL) is found at 27 C.F.R. § 447.21. Persons in the United States engaged in the business of importing defense articles enumerated on the USMIL must register by submitting an application to ATF. *See generally* 27 C. F.R. pts. 447, 448.

28. 22 C.F.R. § 120.31.

29. *Id*. § 120.3(a).

30. *Id*. § 120.31.

31. *Id*. § 120.33(a).

32. *Id*.

33. *Id*.

34. *Id*. at 120.33(b).

35. *Id*. § 120.34(a).

36. The cognizant agency is the Department of Defense's Office of Prepublication and Security Review, *see* 32 C.F.R. pt. 250 and DoD Instruction 5230.29, *Clearance of DoD Information for Public Release* (updated Feb. 8, 2022), https://irp.fas.org/doddir/dod/i5230_29.pdf. The Office of Security Review's website contains useful information on submitting documents for review for public release. *See* www.esd.whs.mil/DOPSR.

37. 22 C.F.R. § 120.32(a)(1).

38. *Id.* § 120.32(a)(2), (a)(3).

39. *Id*. § 120.50. As part of the ECR, the definition of "export" was revised to "better align with the EAR's revised definition of the term. . . ." *See* 81 Fed. Reg. 62,004 (June 3, 2016).

40. 22 C.F.R. § 120.56.

41. It is important to note that in the June 3, 2016 *Federal Register* notice adding the term "release" to the ITAR that DDTC stated that "theoretical or potential access to technical data is not a release" and that a release will have occurred if a foreign person does actually access technical data, and the person who provided the access is an exporter for the purposes of that release." *See* 81 Fed. Reg. 62004, 62005 (June 3, 2016).

42. 22 C.F.R. § 120.62.

43. *Id*. § 120.6.

44. *Id.*

45. In a FAQ, DDTC has stated that if a foreign person's place of birth is different from the country he/she now resides in and holds citizenship "would bring into question the issue of dual nationality and whether the individual had ties to his country of birth which would indicate a degree of loyalty and allegiance to that country. The license would be considered on the basis that it could be an export to both countries. Normally, this does not present a problem unless the country of birth is proscribed under 22 CFR 126.1 in which case we have to secure additional information to confirm lack of significant ties to the country of birth." *See* Licensing FAQs on DDTC's website, https://deccs.pmddtc.state.gov/deccs?id=ddtc_public_portal_faq_detail&sys_id=478b2d9cdb3d5b4044f9ff621f9619f4.

46. 22 C.F.R. § 121.1.
47. Many of these terms are defined in 22 C.F.R. § 120.45 of the ITAR.
48. 22 C.F.R. § 121.1(a)(2). The term SME is defined in 22 C.F.R. § 120.35.
49. 22 C.F.R. § 121.1(a).
50. See USML Category XXI(a).
51. 22 C.F.R. § 121.1(b).
52. In some cases, an item may be subject to the export controls jurisdiction of the Nuclear Regulatory Commission or the Department of Energy.
53. 22 C.F.R. § 120.41.
54. *Id*. § 120.4.
55. *Id*. § 120.12. *See* https://deccs.pmddtc.state.gov/deccs.
56. 22 C.F.R. § 120.12.
57. *Id.*
58. https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=6ea6afdcdbc36300529d368d7c96194b.
59. On March 23, 2022, DDTC issued extensive amendments to the ITAR in an Interim Final Rule entitled "International Traffic in Arms Regulations: Consolidation and Restructuring of Purposes and Definitions." *See* 87 Fed. Reg. 16396 (Mar. 23, 2022).
60. 22 C.F.R. § 120.11(c).
61. Registration requirements for manufacturers and exporters of defense articles or defense services are set for under 22 C. F.R. § 122.1; registration requirements for brokers are enumerated under 22 C.F.R. § 129.3.
62. *Id*. § 122.1(b).
63. *Id*. § 129.3.
64. *Id*. § 122.1(c).
65. *Id*. §§ 122.2–122.3.
66. DDTC's guidance regarding preparation of registration submissions is available on DDTC's website under the "Conduct Business" menu.
67. 22 C.F.R. § 120.67.
68. *Id*. § 122.4(a).
69. *Id*. § 122.4(b). For purposes of the registration change notification requirements set forth under Part 122 of the ITAR, "ownership" is defined to mean that more than 50 percent of the outstanding voting securities of the firm are owned by one or more foreign persons, and "control" exists when one or more foreign persons have the authority or ability to establish or direct the general policies or day-to-day operations of the firm. *Id*. § 122.2(c). A presumption of control arises when there is 25 percent control of voting stock and no U.S. person controls an equal or larger percentage. *Id.*
70. *Id*. § 122.4(c).
71. *Id*. § 122.5.
72. *Id.*
73. *Id*. pt. 130.
74. *Id*. § 123.1.
75. *Id*. § 123.1(a).
76. *Id.*
77. *Id*. § 123.1(c)(4).
78. *Id*. § 123.1(c)(6).
79. *Id*. § 123.10.
80. *Id.*
81. *Id*. § 126.1(d).
82. *Id*.

83. *Id*. § 123.21.
84. *Id*. § 123.22.
85. *Id*. § 123.25.
86. *Id.*
87. *Id*. § 123.9(a).
88. *Id*. § 123.9(c).
89. *Id*. § 120.50(a)(2).
90. *Id*. § 123.16(b)(2).
91. *Id*. § 126.4(a).
92. *Id*. § 123.16(b)(9).
93. *Id*. § 123.16(b)(1). See discussion of TAAs/MLAs *infra*. Note this exception is of limited utility as DDTC interprets it to permit only one export of defense articles. Thus, most TAAs and MLAs envisioning the export of defense articles will require a series of accompanying DSP-5 licenses.
94. 22 C.F.R. § 123.16(b)(4).
95. *Id*. § 123.16(b)(5).
96. *Id*. § 123.9(e).
97. *Id*. § 126.5.
98. *Id*. §§ 123.17, 126.1.
99. *See* www.siaed.org.
100. 22 C.F.R. §§ 120.57(e), 124.1.
101. *Id*. §§ 120.57(d), 124.1.
102. *Id.*
103. *Id*. §§ 120.57(f), 124.14.
104. *Id*. §§ 124.9(a)(5), 124.14(c)(6).
105. *Id*. § 124.7.
106. *Id.* § 124.8.
107. *Id*. § 124.6.
108. *Id*. § 123.22.
109. *See* 22 C.F.R. § 125.2(a)–(c).
110. *Id*. § 125.4(b)(2).
111. *Id*. § 125.4(b)(3).
112. *Id*. § 125.4(b)(1).
113. *Id*. § 125.4(b)(4).
114. *Id*. § 125.4(b)(9).
115. *Id*. § 125.4(b)(5).
116. *Id*. § 125.4(b)(11).
117. *Id*. § 125.4(b)(13). *Note*: This exemption is used when the company does NOT place the information in the public domain. If the information, once approved for public release, is placed in the public domain, there is no need to use this exemption as the information is no longer technical data subject to the ITAR.
118. *Id*. § 125.4(c).
119. *Id*. § 123.4(a)(1).
120. *Id*. § 123.26.
121. The Commerce Department's Bureau of Industry and Security does not regulate the brokering of items subject to the jurisdiction of the Export Administration Regulations and discussed in Chapter 3.
122. 22 C.F.R. § 129.2(a).
123. *Id*. § 129.2(b).
124. *Id*.

125. *Id*. §§ 129.3, 122.1.
126. *Id*. § 129.3(b).
127. *Id*. § 129.4.
128. *Id*. § 129.5.
129. *Id*. § 129.6.
130. *Id*. § 129.9. The advisory opinion procedures are set forth at *id*. § 120.22.
131. *Id*. § 129.10.
132. A FAQ on DDTC's website states that if the broker's registration expires at the end of November 30, 2021, the initial brokering report would cover the period from January 1 to August 31, 2021. For subsequent years, the brokering report would include the trailing 12 month period, e.g., September 1, 2021 to August 31, 2022. See the brokering FAQs on DDTC's website for more information.
133. 22 C.F.R. §§ 130.1–130.17.
134. Section 39(a) of the Arms Export Control Act (22 U.S.C. § 2779).
135. 22 C.F.R. § 130.1.
136. *Id*. § 130.7.
137. *Id*. § 130.8.
138. *Id*. § 130.10.
139. *Id.*
140. *Id.*
141. *Id.*
142. *Id.*
143. *Id*. § 130.15.
144. *Id*. § 130.11.
145. *Id.* § 130.11(a)(1).
146. *Id*. § 130.12.
147. *Id.*
148. *Id.*
149. *Id.*
150. *Id*. § 130.13.
151. *Id.*
152. *Id*. § 130.15.
153. *Id*. § 130.14.
154. *See* https://deccs.pmddtc.state.gov/deccs?id=ddtc_public_portal_dt_part_130.
155. A copy of the Consent Agreement between Airbus SE and DDTC can be accessed on DDTC's website.
156. *See* U.S. Department of Justice's January 31, 2020, press release, www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case.
157. 22 C.F.R. § 127.10(a)(1)(i) for the current maximum civil penalty amount.
158. 22 U.S.C. § 2778(c).
159. 22 C.F.R. § 127.7.
160. *Id*. § 127.6.
161. *Id*. §§ 120.27, 126.7.
162. *Id*. § 127.12.
163. *Id*. § 127.12(a).
164. *Id*. § 127.12.
165. *Id*. § 127.12(c)(1).
166. *Id.*
167. *Id*. § 127.12(c)(2).

168. *Id.* § 127.12(d).
169. *Id.* § 127.12(e).
170. *Id.* § 126.1(e)(2).

3

U.S. Export Administration Controls[1]

Thad McBride, Mark Sagrans, and Scott Maberry

3.1 Introduction

This chapter provides an overview of the Export Administration Regulations, known as the EAR.

What is regulated: Virtually all items not regulated by the International Traffic in Arms Regulations (ITAR) are regulated by the EAR.[2] Section 3.3 provides more detail.

Where to find the regulations: The EAR are contained in parts 730 through 774 of chapter 15 of the Code of Federal Regulations.[3]

Who is the regulator: The regulations are administered by the U.S. Department of Commerce, Bureau of Industry and Security (BIS).

How to get a license: License applications are filed electronically on BIS's website using the SNAP-R system: http://www.bis.doc.gov/snap/index.htm

Key website: http://www.bis.doc.gov/index.htm

3.2 Structure of the Export Administration Regulations

The structure of the EAR is described briefly herein. It is also the structure of this chapter, which is organized roughly in the order of the steps one

takes to determine the export controls applicable to a particular item.[4]

1. Determine if the item is subject to the EAR. Some items are controlled by the ITAR, some items are subject to the jurisdiction of another specialized agency, and some are not controlled at all. This step is outlined in Section 3.3.
2. Classify the item. The items controlled by the EAR are classified on the Commerce Control List (CCL).[5] Items are described by reference to performance characteristics. This step is outlined in Section 3.5.
3. Determine whether the item is controlled (i.e., requires prior authority) to the relevant destination by review of the relevant Export Control Classification Number (ECCN), the Commerce Country Chart contained in Supplement 1 to Part 738 of the EAR and specific sections of the EAR for controls, such as Short Supply, not listed in the Commerce Country Chart. Unlike the ITAR, even if the item is determined to be subject to the EAR, a license often is not required to export the item. Depending on the sensitivity of the item, a license may not be required for certain destinations. The licensing decision is outlined in Sections 3.8 and 3.9.
4. Determine if there is any other reason that a license may be required in light of the particular parties to the transaction, the end-use of the item to be exported,[6] or other factors. If any of several "general prohibitions" apply, a license is required for export to a particular country, person, or end use, as outlined in Section 3.6.
5. If the item is controlled for the particular destination, end user, and/or end use, determine whether any of several "license exceptions" apply, in which case it may not be necessary to obtain a license for the export. This step is outlined in Section 3.8.
6. Apply for a license if required, as outlined in Section 3.9.
7. Throughout the export classification and licensing process, during the export itself, and even after the export transaction is completed, the exporter must maintain accurate and complete records of the transaction. Recordkeeping is both legally required and important to ensure compliance with the EAR. In the current enforcement landscape, policies and procedures to promote compliance are important to undertake, particularly given the array of penalties that

may be imposed for violations. Those penalties, and the enforcement provisions by which those penalties may be imposed, are outlined in Section 3.10. In addition, several recent enforcement actions are described in the Appendix to this chapter.

8. After allowing the statutory authority underlying the EAR to lapse and many years of efforts to reform the export control system, including transforming the ITAR into a positive list and tweaking the EAR to acknowledge cloud computing and related business challenges under the Obama administration, Congress took action in 2018 through the enactment of the Export Control Reform Act of 2018 (ECRA) to reauthorize and modernize the EAR. (See footnote 3.) Among the key changes made by ECRA are the establishment of a permanent statutory authority for the EAR, increasing the civil and criminal penalties for export controls violations, and instituting an interagency process to identify and establish controls for emerging and foundational critical technologies that are deemed essential to U.S. national security. Section 3.10 has additional information on the updated penalties.
9. During the administration of President Donald Trump, several special measures were introduced to address perceived national security risks, particularly as related to China. Section 3.12 summarizes a few of the most notable measures: restrictions imposed on Chinese telecommunications company Huawei, and restrictions on critical technology, including in the context of review of foreign investment in the United States by the Committee on Foreign Investment in the United States. Each of these actions—and others not specifically discussed in this chapter—can be seen as part of a continuing U.S. government effort to prevent foreign actors, especially those from China, from obtaining access to sensitive U.S. technology. Additionally, as part of its response to the Covid-19 pandemic, the U.S. government has invoked the Defense Production Act (DPA) to restrict exports of certain designated medical equipment.

3.3 What Is Regulated: Scope of the Ear

As noted in Section 3.1, most items specially designed or modified for military application are subject to the ITAR; but some lesser parts and components specially designed or modified for military items are now subject to the EAR. And, while most other common or commercial items are subject to the EAR, a small portion of items are subject to the exclusive jurisdiction of some other export control agency.[7] Although the coverage of the EAR is broad, a license is not needed for exports of most items to most destinations or end users.[8] License requirements are based on the item's technical characteristics, and the destination, end user, and end use to which the item will be exported. To determine whether an item or transaction requires a license, it is useful to consider the following questions, often known as the 4 Ws:

- What are you exporting?
- Where are you exporting?
- Who will receive your item?
- What will your item be used for?

With this information, as summarized further in this chapter, it is possible to analyze whether the EAR controls the transaction and whether a license is required.

The EAR applies to several categories of items, as follows:

- Items, regardless of where manufactured, that are physically located in or transiting through the United States.
- Items, wherever located, that were manufactured in the United States (U.S.-origin items).
- Items manufactured outside the United States (foreign items) that contain more than a de minimis amount of controlled U.S.-origin content by value, and certain technology related to those foreign items.[9]
- Foreign items that are considered to be a "direct product" of certain controlled U.S.-origin technology or software.[10]

In addition to controls on exports of physical goods (referred to as "commodities" under the EAR), the scope of the EAR—and the use of the term "items" in this context—includes technology and software most often related to the development or production of controlled commodities.

Controlled "technology" may include plans, specifications, design information, technical data, and manufacturing knowhow. The EAR imposes controls on exports made in any form, such as by email, facsimile, or in other soft-copy form.[11]

The EAR also specifically controls the "release" of technology or software to a foreign person, including through oral or visual disclosure.[12] Such disclosure of controlled technology may be in the context of an export or international transfer but is considered a "deemed export" if the disclosure takes place within the United States, even if the foreign person recipient of the export is lawfully permitted to be in the United States (e.g., by having a valid visa). This kind of export or transfer of controlled technology is referred to as a "deemed re-export" if the disclosure or transfer is made from one foreign person to another foreign person of different nationality outside the United States.

Note that the term "foreign person" is broadly defined as anyone who is not a U.S. citizen, lawful permanent resident, or protected individual under the Immigration and Naturalization Act. This means, as noted earlier, that even foreign persons authorized to be in the United States or that work for a U.S. company are foreign persons for purposes of the EAR (and the ITAR), unless they are lawful permanent residents or protected individuals.

Some items are specifically excluded from the scope of the EAR, and thus are not covered by any EAR restriction (but may be subject to certain other restrictions such as U.S. economic sanctions and embargoes). Items not subject to the EAR include the following:[13]

- Most books, newspapers, periodicals, music, and films
- Most software or technology that is "published" (but not certain encryption software[14] or "software" or "technology" for the production of a firearm, or firearm frame or receiver)[15]
- Software and technology resulting from "fundamental research" in science and engineering, where the resulting information is "ordinarily published and shared broadly within the scientific community"[16]
- Software and technology that are released by instruction in a catalog course or associated teaching laboratory of an academic institution
- Information included in patents and open patent applications[17]

3.4 Who Is Regulated

Because the EAR generally controls U.S.-origin items wherever located, all items located in the United States, and foreign-origin items containing more than a de minimis amount of controlled U.S. content or that are the direct product of certain export-controlled technology, the actions of both U.S. and foreign persons and companies may be subject to the EAR. Changes in the end use or end user of an item subject to the EAR within the same country may also be covered: these are referred to as transfers (in-country) or in-country transfers. As detailed further in the Appendix to this chapter, many recent export enforcement actions have involved foreign companies or individuals who re-exported EAR-controlled items to an unauthorized end use or end user.

3.5 Classification: The Export Control Classification Number

The CCL is divided into ten broad categories, one of which, Category 5, has two parts. Each category is further subdivided into five item types. Entries on the CCL are identified by an ECCN, which is composed of a single digit, followed by a letter, followed by a three-digit code (e.g., 2B991).

The first digit of the ECCN indicates the CCL category as follows:

0: Nuclear materials, facilities, and equipment (and miscellaneous items)

1: Materials, chemicals, microorganisms, and toxins

2: Materials processing

3: Electronics

4: Computers

5.1: Telecommunications

5.2: Information security

6: Sensors and lasers

7: Navigation and avionics

8: Marine

9: Propulsion systems, space vehicles, and related equipment

The letter in the ECCN indicates the “product group,” as follows:

A: Systems, equipment, and components

B: Test, inspection, and production equipment

C: Material

D: Software

E: Technology

The final three digits of the ECCN indicate the basis for control, as follows:

000–099 indicate control for national security

100–199 for missile technology

200–299 for nuclear-related technology

300–399 for chemical and biological weapons

500–599 for items warranting national security or foreign policy controls (such as commercial satellites)

600–699 (known as the “600 series”) for military items that are on the Wassenaar Arrangement Munitions List or formerly on the U.S. Munitions List

900–999 for anti-terrorism, crime control, and other reasons

As a general rule, the lower the number of the ECCN, the more tightly controlled the item is for export purposes (e.g., an item controlled under ECCN 9A001 is more tightly controlled than an item covered under ECCN 9A991). But items that are controlled under the 500 or 600 series are often the most tightly controlled because they are items that were formerly controlled under the ITAR and are still considered to be defense articles, yet were moved to EAR control because of their relatively limited impact on national security and/or because they are widely available from non-U.S. sources.

If the item is not given an ECCN, it falls in a catchall category known as EAR99, discussed in further detail later.

BIS encourages exporters to self-classify their items and technologies on the CCL in most instances. The agency also provides formal "commodity classifications," which are typically used when the classification of an item is ambiguous or when the compliance profile of a particular export requires a high degree of certainty in the classification. If uncertain about whether an item is controlled under the EAR or the ITAR, best practice—as informed by guidance from the State Department—is to submit a commodity jurisdiction request to the State Department as opposed to submitting a commodity classification request to BIS because the jurisdictional determination is a necessary predicate to ITAR categorization or EAR classification.

To obtain a formal commodity classification, a party must submit an application to BIS containing information about the product, including a description and technical specifications of the product, via BIS's internet-based licensing/classification system, SNAP-R.[18] BIS then will determine whether the item is subject to the EAR and, if so, what ECCN applies. In particular, BIS issues a formal classification through the Commodity Classification Automated Tracking System (CCATS), with a unique number on which the manufacturer and exporters can rely from that point forward.[19]

As noted earlier in Section 3.3, with limited exceptions, the jurisdiction of the EAR extends to all U.S.-origin commercial items wherever located and all commercial items in the United States.[20] EAR99 is the designation for items that fit within the scope of the EAR, and are therefore subject to the EAR, but are not assigned an ECCN with specific technical or functional parameters. The EAR99 designation is thus unique in that it is not described on the CCL; instead, it serves as a catchall classification for

commercial items subject to the EAR that have not been identified to pose particular national security concerns.[21] The EAR99 listing appears in a statement at the end of each CCL category, as follows: "[i]tems subject to the EAR that are not elsewhere specified in this CCL Category or in any other category in the CCL are designated by the number EAR99."[22]

EAR99 items may be exported to most destinations without a license. Important exceptions include situations where a "general prohibition" applies.[23] For example, EAR99 items may not be exported without a license to embargoed destinations, or for certain prohibited end uses, or to certain prohibited end users such as those listed on the Denied Persons List[24] or Entity List.[25] Embargoed destinations are listed in Part 746 of the EAR, although exporters also should consult the U.S. sanctions regulations issued by OFAC, described in Chapter 1. End-use and end-user–based export restrictions are listed in Part 744 of the EAR, and should be consulted prior to exporting items to an unfamiliar party or to a party where there are "red flags" that the receiving party (or "consignee" in EAR terms) may use the product for a prohibited end use or divert the product to an embargoed destination or prohibited end user. Prohibited end uses in Part 744 of the EAR are varied, but the core prohibited end uses include the proliferation of weapons of mass destruction—nuclear weapons; unsafeguarded nuclear and fuel cycle activities; chemical and biological weapons; and rockets, missiles, and unmanned aircraft (UAVs). Part 744 also lists destinations, including China, Russia, and Venezuela, to which certain exports are prohibited. For example, exports of certain lesser-controlled[26] products to Belarus, Burma, Cambodia, China, Russia, or Venezuela for a military end use or to a military end user require an export license even though the export of the same product to a commercial user for a commercial end use would be permitted without a license. In any event, all exports from the United States must be documented in compliance with the recordkeeping provisions of Part 762 of the EAR.

3.6 General Prohibitions

Part 736 of the EAR lists ten general prohibitions that apply to any transaction subject to the EAR. Any violation of one of the general

prohibitions will be subject to possible enforcement and applicable penalties, as described in Part 764 of the EAR.[27]

The general prohibitions are as follows:[28]

1. Export or re-export of a controlled item without a required license or license exception.
2. Re-export or export from abroad of a foreign-made item incorporating more than a de minimis amount of controlled U.S. content without a required license or license exception.
3. Re-export or export from abroad of the foreign-produced direct product of certain U.S.-controlled technology and software without a required license or license exception. This is potentially a significant extension of U.S. jurisdiction over items that have a non-U.S. country of origin and would not otherwise be "subject to the EAR." For further detail on how the direct product rule is being implemented and expanded, see Sections 3.11 (related to Russia) and 3.13 (related to China).
4. Engaging in action prohibited by a denial order. From time to time, under Part 766 of the EAR, the Department of Commerce issues orders denying the export privileges of an entity or individual. Denial orders are published in the Federal Register. Export contrary to the terms of a denial order is prohibited; there are no license exceptions that authorize any such exports.
5. Export or re-export to an end use or end user prohibited by Part 744 of the EAR.
6. Export or re-export to an embargoed destination as set forth in Part 746 without a required license. As of July 2022, Cuba; Iran; North Korea; Syria; and the Crimea, Donetsk, and Luhansk regions of Ukraine are subject to comprehensive embargoes such that virtually all exports to those countries (or regions) require licenses. As described further in Section 3.11, many exports to Russia and Belarus also require a license. Sudan is also subject to somewhat stricter export licensing requirements, while many other countries, such as Venezuela, are subject to more targeted restrictions. As outlined in more detail in Chapter 1, it is important to understand that trade restrictions differ widely by country and evolve regularly based on U.S. policy considerations. Depending on the type of

export and the embargoed destination, either BIS or OFAC will have licensing jurisdiction (though, in certain transactions, both agencies may have jurisdiction).

7. Support of proliferation activities, as well as military-intelligence end uses and end users, such as certain financing, contracting, service, support, transportation, freight forwarding, or employment activities by a U.S. person where the U.S. person knows the activity will assist in the proliferation of weapons of mass destruction, or support for a designated military-intelligence end use or end user, as set forth in sections 744.6 and 744.22 of the EAR, respectively.
8. Certain in-transit shipments: For an item being exported or re-exported via a route that requires the item to be unladen from a vessel or aircraft in any of a list of countries, a separate license must be obtained as if the country of unlading were the ultimate destination.
9. Violation of any order, terms, or conditions of a license. All BIS licenses contain terms and conditions limiting their applicability.
10. Proceeding with a transaction with knowledge that a violation has occurred or is about to occur.

General prohibition 10 merits special mention. First, general prohibition 10 refers to all of the other prohibitions; those prohibitions become, in essence, an element of general prohibition 10. Because a violation under general prohibition 10 turns on a "transaction" related to knowing a violation has occurred or is about to occur, violations include not only an export or re-export itself but also any related activity such as transferring, financing, ordering, transporting, forwarding, or even storing an item subject to the EAR within the United States. Additionally, the "knowledge" requirement under general prohibition 10 can be met by either actual knowledge or constructive knowledge, that is, when a party "should have known" of a violation. General prohibition 10 effectively requires exporters seeking to support past violative exports (for example, to continue to export an item previously exported in violation of the EAR, or to repair such an item) to file a disclosure with BIS so that they may then seek authorization from BIS to provide such support.[29] In other words, a "voluntary" disclosure now effectively becomes "mandatory" in order to avoid a "knowing" violation.

3.7 Reasons for Control

Generally speaking, under the EAR, items are controlled for export in accordance with specified foreign policy aims of the United States. Items on the CCL are assigned one or more reasons for control, which in turn forms the basis for licensing requirements for those items. Most reasons for control are multilateral and based on specific regime guidelines. Usually export licenses are not required for export to other regime members but would be for exports to countries that are not regime members.[30] This would not apply for items with multiple controls (excluding AT) and for some items with NS and CB controls to Russia, so be cautious with this rule of thumb.[31] The reasons for control, and examples (as of July 2022) of items controlled for each reason, are as follows:

1. Proliferation of chemical and biological weapons (CB). Examples of items controlled for this reason include chemicals that may be as precursors for toxic chemical agents (ECCN 1C350) and equipment capable of use in handling biological materials (ECCN 2B352). These controls are shared with other Australia Group regime members.
2. Nuclear nonproliferation (NP). Examples include machine tools and any combination thereof for removing or cutting metals, ceramics, or composites, which can be equipped with electronic devices for "numerical control" (ECCN 2B001) and high explosives other than those on the U.S. Munitions List (ECCN 1C239). These controls are shared with other Nuclear Suppliers Group regime members.
3. National security (NS). Examples include equipment for the manufacturing of semiconductor devices or materials (ECCN 3B001), optical equipment and components (ECCN 6A004), and submersible vehicles and surface vessels (ECCN 8A001). These controls, and many ITAR controls, are shared with Wassenaar Arrangement regime members.
4. Missile technology (MT). Examples include turbojet and turbofan engines (ECCN 9A101) and ceramic materials (ECCN 1C007). These controls are shared with other Missile Technology Control Regime members.
5. Regional stability (RS). Examples include radar systems and equipment (ECCN 6A998) and certain cameras (6A003). These are

broad, foreign policy-based unilateral controls.

6. Firearms convention.[32] Examples include shotguns (ECCN 0A502) and optical sighting devices (ECCN 0A504). These controls are often shared with other Wassenaar Arrangement regime members.
7. Crime Control (CC). Examples include voice print identification and analysis equipment (ECCN 3A980) and restraint devices (ECCN 0A982). These controls are often shared with other Wassenaar Arrangement regime members.
8. Anti-terrorism (AT). Examples include portable electric generators (ECCN 2A994) and "mass market" information security software (ECCN 5D992). These are foreign policy-based unilateral controls.
9. Short Supply (not on Country Chart). Examples include horses for export by sea, petroleum products (not including crude oil) that were produced from the Naval Petroleum Reserves, and western red cedar. These are domestic policy-based unilateral controls.
10. U.N. Sanctions (not on Country Chart). Examples include aircraft and gas turbine engines controlled in ECCN 9A991 and commodities related to military explosive devices (e.g., smoke hand grenades) (ECCN 0A604).
11. Specially designed implements of torture such as those controlled in ECCN 0A983. These controls are often shared with other Wassenaar Arrangement regime members.
12. Encryption items (EI) such as "information security systems" meeting certain technical criteria in ECCN 5A002, and corresponding software (ECCN 5D002) and technology (ECCN 5E002).[33] These controls are often shared with other Wassenaar Arrangement regime members.
13. Communications intercepting devices such as those primarily useful for surreptitious interception of wire, oral, or electronic communications (ECCN 5A980) and software applying to such devices (ECCN 5D980).[34] These controls are often shared with other Wassenaar Arrangement regime members.

The reason for control appears in the heading of the ECCN entries.[35] Following is an example of such an entry:

A. SYSTEMS, EQUIPMENT, AND COMPONENTS

5A002 Systems, equipment, application specic "electronic assemblies". modules and integrated circuits for "information security", as follows (see List of Items Controlled), and other specially designed components therefor.
License Requirements

Reasons for Control: NS, AT, EI

Control(s)	Country Chart
NS applies to entire entry	NS column 1
At applies to entire entry	At column 1

In this example, any systems or equipment meeting the technical specifications of ECCN 5A002 are subject to National Security (NS), Anti-terrorism (AT), and Encryption Items (EI) controls. In order to determine whether the reason for control would require a license or license exception for a given destination, it is necessary to check the Country Chart and applicable related regulations in Part 742 and 740.17 of the EAR as outlined in Section 3.8.

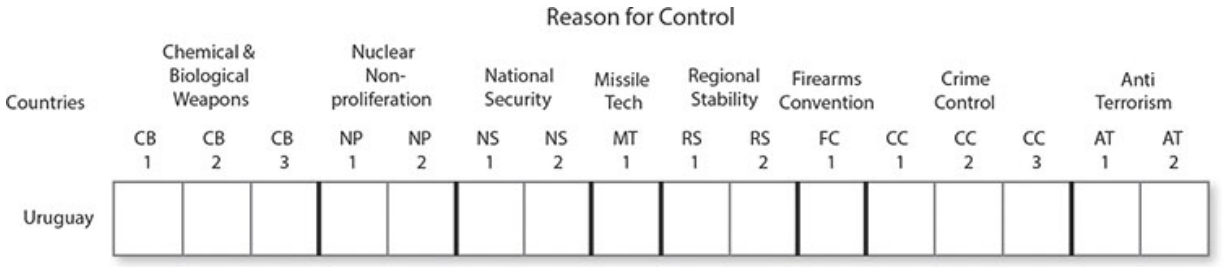
End-user and end-use-based controls, which may apply regardless of the country of destination, are contained in Part 744 to the EAR.[36] While those are not identified as "Reasons for Control," as that label is employed in the EAR, end-use restrictions include but are not limited to certain nuclear end use; restrictions on chemical and biological weapons end uses; missile, rocket, and unmanned air vehicle end uses; maritime nuclear propulsion end uses; and military end users and end uses in Belarus, Burma, Cambodia, China, Russia, and Venezuela.[37]

Separate restrictions on end users include the lists maintained by BIS (the Entity List and the Denied Persons List) and persons designated in certain executive orders and named to OFAC's List of Specially Designated

Nationals (SDN) and Blocked Persons.[38] BIS maintains a collection of "Lists to Check" on its website that can be used to screen parties to any transaction.[39]

Once an item's correct ECCN and reason for control are determined, the Commerce Country Chart[40] is generally used to determine whether a license is required to export that item to a particular destination.[41] Some ECCNs contain self-evident descriptions of the license requirement (e.g., in the rare case where a license is required to all destinations)[42] or refer to another set of controls such as the ITAR.[43] But for most items, the "reason for control" must be found in the ECCN entry, and then the destination (and intermediate destinations for transshipped items) must be checked in the Country Chart.[44]

A sample Country Chart entry (for Uruguay) is reproduced here:



The checked boxes indicate that a license or applicable license exception is required to export to Uruguay any item controlled under the following Reasons for Control: Chemical & Biological Weapons categories 1 and 2, Nuclear Non-proliferation category 1, National Security categories 1 and 2, Missile Technology category 1, Regional Stability categories 1 and 2, Firearms Convention category 1, and Crime Control categories 1 and 3.

As an example, an item classified in ECCN 5A002 (from the preceding example) would be controlled for export to Uruguay because, by the terms of the ECCN, such an item is controlled under NS column 1. As shown in the preceding Country Chart entry, items controlled for National Security column 1 are controlled for export to Uruguay.

It is important to note that if any of the Reasons for Control listed in the ECCN has an X in the box for the destination on the Country Chart, the item is controlled for export or re-export to that destination. In this example, 5A002 is controlled for both NS 1 and AT 1, but Uruguay only

has an X in the box for NS 1. A single applicable reason for control is sufficient to require a license or license exception for the export. The fact that there is no restriction to Uruguay for items controlled for anti-terrorism reasons (i.e., there is no X in the box for AT 1) does not change the fact that the 5A002 item is still controlled for export to the country.

It is also important to note that the "Encryption Item" Reason for Control does not appear in the Country Chart. As an example, the ECCN 5A002 entry lists "EI" as one of the reasons for control. But the Country Chart entry for Uruguay (as with all countries on the chart) does not contain a column for EI controls. For EI controls, it is necessary to review the provisions in the notes to the ECCN and the relevant EAR provisions (particularly 742.15 and 740.17) to determine whether a license is needed. There are additional items that are controlled; for example, items may be controlled for Short Supply even though Short Supply controls are not reflected in the Country Chart. If the description or text of an ECCN identifies a reason for control that does *not* appear as one of the columns in the Country Chart, you must separately research that reason for control in the EAR to determine if an export license is required. Typically, Part 742 is a good place to start, but some controls have their own special section, for example, short supply controls, which are addressed in Part 754 of the EAR.

The fact that an item is controlled for export to a particular destination means that a license or applicable license exception is required to export the given item to that destination. Note that if there are multiple reasons for control, to take advantage of a license exception, that exception must be available for each applicable Reason for Control—and meet all other required conditions—for the given destination and end user, including those set forth in the text of the license exception as well as those generally applicable to license exceptions contained in Part 740.2. *See* Section 3.8 for additional information about license exceptions.[45]

Remember too that, as noted earlier, export controls apply equally to exports physically sent to other countries and to "deemed exports," that is, transfers of controlled technology or source code to a foreign person even while in the United States, and "deemed re-exports," that is, transfers of controlled technology or source code to a foreign person of a country other than the foreign country where the release takes place.[46]

The Commerce Country Chart does *not* cover end-use or end-user restrictions. Although it makes reference to U.S. sanctions and embargoes in some country entries (e.g., Cuba), the Country Chart does not provide full coverage of end-use and end-user restrictions.[47] Because the end-use and end-user restrictions may impose separate licensing requirements administered by BIS or other U.S. government agencies, it is important to implement a screening process for those restrictions in addition to checking the Country Chart.

3.8 License Exceptions

Part 740 of the EAR lists the various license exceptions that are available to exporters. An applicable license exception provides authorization for a transaction that is controlled for export to a given destination, end user, or end use that would otherwise require a license from BIS. License exceptions are highly fact-dependent and may be limited by the dollar value of a shipment or other factors. Some license exceptions are only available after certain steps are completed (such as a specific request to BIS or a technical review by BIS).

By way of example, license exceptions may be available for exports of the following:[48]

- Certain lower-technology items of low dollar value (License Exception LVS)
- Exports of certain items to countries listed in Country Group B of the EAR, found in 15 C.F.R. § 740 Supp. 1 (License Exception GBS)
- Baggage as described in 15 C.F.R. § 740.14 (License Exception BAG)
- Certain aircraft and vessels on "temporary sojourn" in the United States or through foreign countries (License Exception AVS)[49]

As summarized here, several steps will help to determine whether a given transaction is eligible for a license exception.

1. Determine whether any of the general prohibitions (discussed in Section 3.6) apply to the export.[50] If no prohibition applies, a license or license exception is unnecessary (though you may have specific recordkeeping obligations under parts 758 or 762 of the EAR).

2. Determine whether one or more of the restrictions against using a license exception applies.[51] Be sure to carefully check EAR section 740.2, which lists those restrictions, before proceeding, as it is a trap for the unwary. If a restriction in 740.2 renders a license exception unavailable, a license is required to proceed with the export.
3. If no restrictions apply, determine whether any of the license exceptions listed in Part 740 of the EAR are available. Some license exceptions, such as LVS, GBS, TSR, APP, and others, are "list based" and are available *only if* they are listed in the ECCN of the item to be exported. Other license exceptions, such as TMP, RPL, BAG, GOV, TSU, and STA, are "transaction based" and are available without being listed in the ECCN, but each exception is based on the reason(s) for control of the underlying item and thus is restricted from or authorized solely to designated Country Groups.[52] It is therefore necessary to carefully review both the ECCN and the relevant section of Part 740 describing the license exception and the conditions for its use to determine the applicability of a particular license exception to a transaction. Eligibility may depend on the item, the destination country, the end use, and/or end user of the item as well as any special conditions of the license exception.[53]
4. Comply with all terms and conditions listed in the license exception.

3.9 Licensing

License application. When a specific license is required, the exporter must submit a license application to BIS through the agency's electronic application system, known as SNAP-R (an acronym for "Simplified Network Application Process Redesign").[54] To submit an application using SNAP-R, it is first necessary to register with SNAP-R and obtain an authorizing Company Identification Number (CIN) and PIN.

As part of the license application, the exporter must provide information about itself and all other parties to the transaction, for example, the end user, and any freight forwarder and/or other intermediate consignees. The application also must provide the applicable ECCN and a description of items to be exported, including the quantity and value of such items.

License. A BIS license typically will contain a number of standard clauses, a four-year term of validity, and may also include specific terms and conditions. All terms, conditions, and restrictions of a license must be complied with; failure to do so would be considered a violation of General Prohibition 9.[55] A license authorizes exports only within the terms of the license application. It does not constitute an authorization to engage in other transactions with the country of destination or to continue exports or transfers after the license has expired.

764.5(f) authorizations. If a company has inappropriately exported an item without a license and now needs to provide support in a form that would otherwise *not* require a license, as noted earlier, that support would be prohibited by General Prohibition 10.[56] It is possible to obtain an authorization to provide such support, but this process is not conducted through the SNAP-R licensing process.[57] Instead, it is conducted by filing a letter request with the BIS Office of Exporter Services (OES) after the company has filed a voluntary disclosure with the BIS Office of Export Enforcement (OEE). The scope of any such request, and any authorization then granted by OES, is limited to the specific transfers and actions immediately necessary.

In the event that an exporter discovers that it has violated the EAR, it may decide to voluntarily report the violation to the OEE. Part 764 of the EAR details the procedures involved in making a voluntary self-disclosure to the OEE. Reporting a violation of the EAR is not mandatory in most cases but is strongly encouraged by the OEE and can mitigate potential penalties.[58] A person disclosing a violation will be given credit for that violation as being voluntary only if neither OEE nor another U.S. government agency have previously learned of the conduct at issue.

The OEE encourages persons submitting a voluntary self-disclosure to follow a two-step process: (1) submit a brief initial notification with basic information about the parties involved and the conduct at issue, and (2) submit a subsequent, full narrative report detailing the suspected violations at issue, the review conducted, and measures taken to deter future violations. The EAR details the information to be provided in the narrative report and examples of supporting documentation to accompany the report. Submitting parties are required to certify to the accuracy of the information submitted with the disclosure. The OEE generally discourages oral presentations for disclosures but may agree to them upon request. The OEE

also requires that parties retain all records relevant to the disclosure until OEE makes a final determination on how to resolve the matter.

It is important for every exporter to understand the EAR and other relevant export laws, and to have an appropriate compliance program in place to prevent and detect violations. While BIS has created an Export Management System document that provides details of what the agency considers to be essential components of an effective export compliance program, no one sample policy should be considered sufficient for compliance. Rather, a compliance program must be tailored carefully to the exporter's needs. For example, an exporter whose inventory is limited to EAR99 items and whose sales territory consists solely of the United States and Canada will have a very different risk profile from a company that regularly ships highly controlled items to China, Russia, and the Middle East. A company that employs only U.S. citizens may have less of a need for strict technology transfer controls than a company that has many foreign person engineers in its R&D laboratories.

One important component of any compliance program is the ability to identify and respond to "red flags," that is, any circumstances that indicate an export may be destined for an improper destination, end use, or end user.[59] BIS has developed an extensive list of sample red flags on its website, but any abnormal circumstances may give cause for suspicion.[60] BIS expects that any red flags present will be identified and addressed before an export transaction occurs. Exporters also have a duty not to self-blind with respect to information that may constitute a red flag.[61]

Whatever compliance policy the exporter adopts, it is important that relevant personnel be trained on the applicable law and the company's procedures for complying with it. Records of each export transaction generally are required to be maintained for at least five years from the date of the transaction or expiration of a relevant license authority and must be made readily available to the government at its request. Periodic compliance audits may also be appropriate to review how effectively existing compliance processes are working and to identify areas for improvement.

3.10 Penalties and Enforcement

Penalties for violations of the EAR can be severe. Criminal penalties against a company can include fines of up to $1 million.[62] Criminal penalties against an individual can include a fine of up to $1 million or imprisonment for up to 20 years, or both, for each violation.[63]

Civil penalties against a company or an individual can include fines of up to the greater of $300,000[64] or two times the value of the exports for each violation.[65] In addition to the civil and administrative penalties just outlined, the U.S. government may impose administrative penalties in appropriate cases, including the following:

- Denial of export privileges
- Exclusion from U.S. government contracts
- Seizure and forfeiture of goods

The U.S. government continues to aggressively enforce the EAR against companies and individuals both inside and outside the United States. A short list of recent export enforcement actions, including descriptions, is in the Appendix to this chapter.

Several trends emerge from these and other recent enforcement matters. First, the government clearly believes that taking action against individuals who violate the export laws, and in certain cases sending people to jail for such violations, is a particularly effective deterrent against violations. Second, recent enforcement actions show that the U.S. government remains especially focused on export violations involving China—many recent enforcement actions, particularly several high-profile matters, involve unauthorized exports to or by Chinese entities or Chinese nationals. Finally, settlements are increasingly including specific compliance obligations that the settling party has to meet. For example, when settling with individuals, the government is often requiring individuals to attend export compliance training, including certifying to the government as to attendance at such training. With respect to entities, designated officials are also being required to attend training, and entities are being obligated to conduct—and report to the government on the results of—periodic export controls compliance audits. It also appears the government is more willing to impose monitorships for settlements with entities within the EAR enforcement context.

3.11 Special Topic: Export Controls Specific to Russia

In February 2022, Russia invaded Ukraine in a major escalation of the war that began with Russian annexation of the Crimean peninsula in 2014. On the day of the invasion, BIS announced a broad expansion of export controls designed to "severely restrict Russia's access to technologies and other items that it needs to sustain its aggressive military capabilities."[66] The controls target strategic Russian industry sectors, including aerospace, defense, and maritime. The measures were coordinated with those of OFAC (see Chapter 1). The measures also reflect substantial cooperation with regard to export controls on Russia among the United States, the European Union (EU), Australia, Canada, Japan, New Zealand, South Korea, the United Kingdom, and others.[67]

BIS first published new rules related to Russia (and Belarus) on March 3, 2022. The rules imposed a new export license requirement on all items destined for Russia classified under any ECCN in CCL Categories 3 through 9. This was soon extended to all items covered under any ECCN in CCL Categories 0, 1, and 2. *See* 15 C.F.R. 746.8 for many of the export controls on Russia and Belarus. Thus, subject to limited exceptions, all items with a specific ECCN now require a license for export or re-export to Russia and Belarus. Moreover, license applications are subject to a policy of denial except that case-by-case review policy, that is, regular review, applies to items for flight safety, maritime safety, humanitarian needs, international space cooperation, and certain other narrow categories.[68]

BIS has also imposed new Foreign Direct Product restrictions for Russia, and added hundreds of Russian parties to the Entity List.[69] In addition, BIS has extended restrictions to cover any aircraft subject to the EAR and which is registered in, owned, or controlled by, or under charter or lease by the Russian Federation or any Russian national from being eligible for export license exception AVS (Aircraft, Vessels, and Spacecraft). As a result, a license is required to export to Russia any aircraft that includes more than 25 percent controlled U.S.-origin content if it is Russian-owned, chartered, or leased.[70]

Multiple further restrictions on exports to Russia have followed, including the following:[71]

- Additional restrictions against the Russian energy sector[72]

- Issuance of Temporary Denial orders against multiple airlines operating in violation of U.S. export controls[73]
- Addition of specific export control requirements for an extensive list of goods, identified by Schedule B numbers, deemed to be luxury items (see 15 C.F.R. 746.10 and Supplement 5 to Part 746) or that are used in various industrial sectors, including such diverse items as plywood, mechanical shovels, and dry cleaning machines (see 15 C.F.R. 746.5(a)(1)(ii) and Supplement 4 to Part 746)[74]
- Issuance of a Charging Letter against Russian oligarch Roman Abramovich for violations associated with flights of his private jets[75]

Taken together with the Russia and Belarus sanctions administered by OFAC and those put in place by U.S. allies, these restrictions constitute one of the largest multilateral trade near-embargo ever undertaken. U.S. and international companies should take care to remain informed of the details of these programs as they develop, since the impacts are fast moving and far reaching.

3.12 Special Topic: Export Control Reform

In August 2009, President Barack Obama ordered an inter-agency review of U.S. export controls directed at strengthening national security and the competitiveness of key U.S. manufacturing and technology sectors. That review found the current system to be overly complicated, redundant, and, in some cases, ineffective. In response to this finding, the administration launched the Export Control Reform Initiative (ECR Initiative) aimed at simplifying the U.S. export control system. The administration implemented the ECR initiative in three phases. In Phases I and II, which were generally completed, the administration reconciled various export control definitions, regulations, and policies among the various regimes. Phase III, however, which envisioned a single control list, single licensing agency, and single information technology system, has not yet been completed.

Key changes under the ECR initiative included the transfer of certain items from the ITAR to the EAR under specific ECCNs such as those within the 500, 600, and 900 categories, which include items such as launch vehicles, missiles, rockets, torpedoes, bombs, mines, and other military

explosive devices (formerly Category IV), aircraft and associated equipment (formerly Category VIII), military electronics (formerly Category XI), and spacecraft and related articles (formerly Category XV). On a somewhat related note, in early 2020 control over firearms that "do not provide a military or intelligence advantage" were transferred from the ITAR (formerly Categories I, II, and III) to the EAR.[76]

1. The Obama administration also introduced License Exception Strategic Trade Authorization (STA), which was designed to ease trade between the United States and its allies by eliminating the license requirement on the export of eligible items between the U.S. and certain qualifying countries.[77] Items eligible for license exception STA are generally those that are at low-risk for mistreatment or diversion in a manner that could threaten U.S. national security. Exporters utilizing license exception STA must comply with several administrative requirements, such as obtaining consignee statements and maintaining records related to the transactions. BIS has published a useful interactive decision tool that can be used to double-check—and document—if a particular export qualifies for license exception STA.[78]
2. The Obama administration also created a new definition of "specially designed," substantially shared between the EAR and the ITAR, which implements an Order of Review process for jurisdiction and classification. The Order of Review reflects a "catch-and-release" approach, meaning that the item may be "caught" under the first part of the definition as an item specially designed for military use, but "released" under one of the six exclusions identified in the second part of the definition. Under the first part of the definition, an item is considered "specially designed" if:[79]
   (1) As a result of "development" it has properties peculiarly responsible for achieving or exceeding the performance levels, characteristics, or functions in the relevant ECCN or USML paragraph; or
   (2) It is a "part," "component," "accessory," "attachment," or "software" for use in or with a commodity or defense article "enumerated" or otherwise described on the CCL or the USML.

If an item does not meet either of these criteria, it is not specially designed. However, if it does meet both or either of the criteria, it would be considered specially designed, unless it qualifies as one of the following under the second part of the definition:[80]

(i) Has been identified to be in an ECCN paragraph that does not contain "specially designed" as a control parameter or as an EAR99 item in a commodity jurisdiction (CJ) determination or interagency-cleared commodity classification (CCATS) pursuant to § 748.3(e);

(ii) Is, regardless of "form" or "fit," a fastener (e.g., screw, bolt, nut, nut plate, stud, insert, clip, rivet, pin), washer, spacer, insulator, grommet, bushing, spring, wire, solder;

(iii) Has the same function, performance capabilities, and the same or "equivalent" form and fit, as a commodity or software used in or with an item that:

(a) Is or was in "production" (i.e., not in "development"); and

(b) Is either not "enumerated" on the CCL or USML, or is described in an ECCN controlled only for Anti-Terrorism (AT) reasons;

(iv) Was or is being developed with "knowledge" that it would be for use in or with commodities or software (1) described in an ECCN and (2) commodities or software either not "enumerated" on the CCL or the USML (e.g., EAR99 commodities or software) or commodities or software described in an ECCN controlled only for Anti-Terrorism (AT) reasons;

(v) Was or is being developed as a general purpose commodity or software, that is, with no "knowledge" for use in or with a particular commodity (e.g., an F/A-18 or HMMWV) or type of commodity (e.g., an aircraft or machine tool); or

(vi) Was or is being developed with "knowledge" that it would be for use in or with commodities or software described (1) in an ECCN controlled for AT-only reasons and also EAR99 commodities or software; or (2) exclusively for use in or with EAR99 commodities or software.

BIS has published a useful interactive decision tool that can be used to double-check—and document—if an item is "specially designed."[81]

3. The administration also instituted reforms for cloud computing whereby the transmission or storage of technology or software is not considered to be an export, provided that such technology or software is:
   i. Unclassified;
   ii. Secured using "end-to-end encryption";
   iii. Secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications, or other similarly effective cryptographic means; and
   iv. Not stored in designated countries.[82]

3.13 Special Topic: Changes to the Ear Focusing on Huawei And China

In May 2019, the U.S. government designated Huawei Technology Co. and a targeted group of the company's affiliates on the U.S. Entity List. Under that designation, it is prohibited for any person to export EAR-controlled items, technology, or software to Huawei itself—or to any of the designated affiliates—without an export license from BIS. The initial list of Huawei affiliates has subsequently been expanded. Going further, in May 2020 and again in August 2020, the U.S. government expanded the foreign direct product rule (Huawei FDPR) contained in a unique footnote 1 to Supplement 4 of Part 744 of the EAR to impose a license requirement for exports, re-exports, and transfers of certain FDPR items where Huawei and potentially other companies with a footnote 1 in Supplement 4 are parties to the transaction.[83] An item is subject to the Huawei FDPR if it is either a:

(a) Direct product of "technology" or "software" subject to the EAR and specified in certain Category 3, 4, or 5 ECCNs;[84] *or*

(b) Direct product of a plant or major component of a plant that is the direct product of U.S.-origin "technology" or "software" specified in certain Category 3, 4, or 5 ECCNs.[85]

The effect of the Huawei FDPR rule is to impose limits on facilities that use certain U.S.-origin technology and software, or equipment based on such technology or software, to manufacture products intended for (even after incorporation into downstream products) specific Entity List named parties such as Huawei or where such companies are parties. Under these restrictions, such facilities are prohibited from selling products developed with U.S.-origin technology or software to or for Huawei or other designated parties without a U.S. export license.[86]

In another effort to restrict Chinese access to U.S.-origin goods and technology, in June 2020, BIS announced an expansion of EAR section 744.21, which pertains to controls on military end uses and end users in China—as well as those in Russia and Venezuela, and more recently also Belarus, Burma/Myanmar, and Cambodia. What constitutes a military end user and a military end use is broadly defined. Moreover, even an export of a commercial item for a commercial use if made to a military end user in China requires an export license. Likewise, the term military end user includes not only armed services but also national police forces and even any person whose actions are intended to support a military end use. Items subject to this rule are those captured under specific AT-level ECCNs that otherwise would be eligible for export to Belarus, Burma (Myanmar), Cambodia, China, Russia, and Venezuela without a license and are listed in Supplement 2 to Part 744 of the EAR.[87] In December 2020, BIS added a new military end user (MEU) list to a new Supplement 7 to Part 744 of the EAR and added to the MEU List more than 100 'military end users' in China.[88]

In 2020, the U.S. government took a number of steps that eliminated the special status with respect to export controls that the United States has historically accorded to Hong Kong. The U.S. Commerce Department announced that it would begin treating Hong Kong in the same way in which it treats China for export licensing purposes.[89] In July 2020, BIS suspended important license exceptions such as STA that previously were available for Hong Kong. In December 2020, BIS completed the changes necessary to treat Hong Kong as part of China by removing the entry for Hong Kong from the Commerce Country Chart, effectively moving Hong

Kong to country group D and imposing new licensing requirements, such as the military end use and end user rules discussed earlier.[90]

In addition, as referenced in footnote 80, the Department of Defense has listed Chinese companies deemed to qualify as Chinese "military companies operating in the United States." These companies may or may not be added to the Entity List—some, including Huawei, are already named on that List—which would lead to the imposition of export restrictions on these companies. An example of a company added to the Chinese military company list and then added to the Entity List is the Semiconductor Manufacturing International Corporation (SMIC), which was added to the Chinese military list at the beginning of December 2020 and to the Entity List on December 18, 2020.[91] Other companies, however, remain only on the Chinese military company list because they are owned by the Chinese military but may, in fact, not be engaged in military end uses. Their listing should now be considered a "red flag" for being potential producers of military end-use items and additional due diligence and/or end use certifications may be prudent. In addition, as discussed in Chapter 1 on economic sanctions, this listing means that, pursuant to Executive Order 13959 of November 12, 2020, U.S. persons will no longer be able to engage in transactions in their publicly traded securities, or any securities that are derivative of, or are designed to provide investment exposure to such securities beginning in 2021.

The U.S. government continues to introduce new restrictions on China. Of particular note was an interim final rule issued in October 2022, in which BIS announced new controls on advanced semiconductor-related exports to facilities in China and established new criteria for making additions to the Entity List from the Unverified List.[92] In this interim rule, BIS added new control classifications to the CCL for advanced chips and semiconductor manufacturing equipment; three new foreign direct product rules; new U.S. person controls; and catchall controls related to supercomputers and semiconductors. It is possible that the U.S. government will seek alignment with allies to implement new semiconductor rules jointly. Comments on this potential significant rule are expected in January 2023.

3.14 Special Topic: ECRA's "Emerging" and "Foundational" Technologies and Tie-In to CFIUS Review of Foreign Investments

In November 2018,[93] as part of the effort to implement ECRA, the U.S. Department of Commerce published an Advance Notice of Proposed Rulemaking (ANPR) in connection with identifying "emerging and foundational technologies" for purposes of ECRA. Notwithstanding the ANPR, as of July 2022, only a limited number of technologies had been identified under this effort. In January 2020, the U.S. Commerce Department issued an interim final rule establishing that certain Artificial Intelligence (AI) technology was being designated as an emerging and foundational technology. That technology was designated under ECCN 0D521, which covers:

> Any software subject to the EAR that is not listed elsewhere in the CCL, but which is controlled for export because it provides at least a significant military or intelligence advantage to the United States or for foreign policy reasons.

In addition, in June 2020, Commerce announced that (1) certain precursor chemicals, (2) the Middle East respiratory syndrome-related coronavirus (MERS-related coronavirus), and (3) single-use cultivation chambers with rigid walls have been identified as emerging technologies. [94]In October 2021, BIS issued a notice of proposed rulemaking related to brain-computer interface technology, and specifically requested comments as to whether such technology should be considered an emerging technology.[95] In May 2022, BIS similarly requested comments with respect to treatment of certain marine toxins.[96] In the Federal Register notice making this request, BIS stated that it would no longer "characterize a specific technology as 'emerging' or 'foundational' [but will instead] characterize all technologies identified pursuant to Section 1758 as 'Section 1758 technologies' without drawing a distinction between 'emerging' or 'foundational' technologies."

Beyond introducing stringent export licensing requirements on such technologies, these designations mean that any foreign investment in a business that manufactures or has access to such technology is likely to warrant scrutiny from the Committee on Foreign Investment in the United States[97] as is discussed in detail in Chapter 10, Export Controls and Sanctions Compliance in the M&A Context.

3.15 Special Topic: U.S. Encryption Controls

The United States shares the basics of its export controls on encryption hardware, software, and technology with its fellow Wassenaar Arrangement Members. It controls for export only; unlike China, France, and some other countries, the United States maintains no controls on imports of commercial encryption.

(a) Is Your Encryption Subject to Encryption Controls in the First Place?

Following Wassenaar controls, there are many forms of encryption that are not controlled by the EAR, and an analysis of whether a given item is subject to EAR encryption controls begins with an analysis of whether it falls into one of the exemptions. This analysis is as follows:[98]

1. For encryption source code (and for the object code compiled from that source code) is it "publicly available,"[99] and—for source code that provides or performs "non-standard cryptography"[100] as defined in part 772 of the EAR—is also notified to BIS and the Encryption Coordinator at the National Security Agency (NSA)? If so, that code is not subject to the EAR at all. Beware however that many will tell you their software is "open source," but what they mean is that they have taken open source code, which is not subject to the EAR, and used it to program software that is subject to the EAR and subject to encryption controls. It is also important to recognized that this rule only applies to the publicly available (and in most cases) notified source code and the object code compiled from it—not to downstream products.

ONE PRACTICAL TIP: It is often hard to know when something that looks like open source encryption source code is "published." If the cryptography is standard (e.g., AES 256) and anyone can download it from the web (with no controls on its further distribution), it is "published." If it is "non-standard cryptography" however, you need to make sure that it has in fact been notified to BIS and NSA. In

that case, you can notify the source code to BIS and NSA yourself, thereby ensuring that the source code is not subject to the EAR.

2. Is the encryption for "data confidentiality" purposes? Some forms of quite strong encryption are completely exempted from encryption controls because the Wassenaar arrangement governments have concluded that they want to encourage the *function* or *purpose* of the encryption. Thus, the following functions are excluded from the meaning of encryption for "data confidentiality":

   1.a. "Authentication"
   1.b. Digital signature
   1.c. Data integrity
   1.d. Non-repudiation
   1.e. Digital rights management, including the execution of copy-protected "software"
   1.f. Encryption or decryption in support of entertainment, mass commercial broadcasts, or medical records management
   1.g. Key management in support of any previously described function

   Watch out relying on these exemptions: some encryption items may perform one or more of these exempt functions but also perform other functions. If so, they are controlled.

3. Is the key length long enough? The EAR only controls symmetric algorithms with key lengths in excess of 56 bits and other specified asymmetric algorithms. Although uncommon, it is possible to encounter an encryption item under these low thresholds. Such items are not controlled.
4. Does the encryption item fall under a growing list of exempted items? Note 2 to ECCN 5A002 contains a growing list of encryption items that the Wassenaar arrangement has decided do not warrant control. Some of these are quite broad—for example, routers, switches, or relays, where the "information security" functionality is limited to the tasks of "Operations, Administration or Maintenance" (OAM) implementing only published or commercial cryptographic standards. Moreover, the list continues to grow over the years: for

instance, encryption items specially designed for a "connected civil industry application" were added to the exempted items list in 2020.

5. Is the encryption activated (turned on) or usable without cryptographic activation? And finally,
6. Does the encryption fall under one of the controlled categories in 5A002, a.1, a.2, a.3, and a.4?[101] These subheadings cover items that perform the functions of "information security," digital communications and networking, computers and other items for information storage and processing, and items for other purpose but offering an addition encryption functionality that is *not* supporting the main function of the item. This last, which many still call "ancillary cryptography," is hardest to understand, but, in simple terms, if the item is not for information security, digital communication or computers, and other items for information storage and processing, try to identify the primary function of the item. If the encryption is just supporting that primary function, the item is not controlled; but if the encryption is supporting an additional functionality, then it is controlled.

An example of this is a GPS device, which serves the primary function of identifying a location. If the encryption is only used to encrypt location information to send it securely through the internet to a phone, the GPS is not subject to encryption controls. But if the GPS offers an additional function of allowing digital communication with others and the encryption supports that additional function, for example, encrypting voice or text communications, the GPS is subject to encryption controls.

(b) Is Your Encryption "Mass Market"?

After establishing that hardware, software, or technology is subject to the encryption controls in the EAR, the next step is to classify it to determine whether it may qualify for either mass market treatments or one of the variants of license exception ENC, or whether an export license is needed. This analysis is captured by BIS in the second of its two helpful encryption flowcharts (see footnote 98).

This is where U.S. law differs from other Wassenaar arrangement members. Although all share the "mass market" exceptions under which tightly controlled 5A002 hardware and 5D002 software are controlled only

for anti-terrorism purposes, the U.S. has established an easy way to qualify for mass market. In addition, only the United States has license exception ENC with its multiple variants that provide a basis to share encryption items covered under 5A002, 5D002, and 5E002 very broadly without a license.

To qualify for mass market,[102] an item must meet all of the following:

1. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
   a. Over-the-counter transactions
   b. Mail order transactions
   c. Electronic transactions
   d. Telephone call transactions
2. The cryptographic functionality cannot be easily changed by the user;
3. Designed for installation by the user without further substantial support by the supplier; and
4. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in preceding 1 through 3.

In addition, the exporter must file a self-classification report with BIS and NSA by February 1 of the year following the classification or export.[103] Items that are components or executable software of mass market items are also mass market, provided they meet the following:

1. "Information security" is not the primary function or set of functions of the component or "executable software";
2. The component or "executable software" does not change any cryptographic functionality of the existing items, or add new cryptographic functionality to the existing items;
3. The feature set of the component or "executable software" is fixed and is not designed or modified to customer specification; and
4. When necessary, as determined by the appropriate authority in the exporter's country, details of the component or "executable software," and details of relevant end-items are accessible and will be provided to the authority upon request, in order to ascertain compliance with the conditions just described.

In fact, part of the difference between encryption controls in the various Wassenaar arrangement members is due to the different hurdles imposed on gaining mass market treatment in those countries, as well as the flexibility in interpreting these criteria by the governments in question. As noted earlier, the U.S. government applies a relatively flexible approach to qualifying items as mass market.

(c) Does Your Encryption Qualify for License Exception ENC?

If the encryption item is not exempt from encryption controls or mass market, it likely falls under the tight encryption controls in the EAR. However, the U.S. controls are lighter than in many other Wassenaar countries due to the breadth of license exception ENC. There are many flavors of ENC—think of your favorite ice cream store.

1. **License Exception ENC (740.17(a) with no classification determination (CCATs) or self-classification.** There are flavors of ENC that do not require any classification determination by BIS or self-classification. These variants of ENC, contained in 740.17(a), authorize the export of strong encryption hardware, software, and technology to a wide variety of recipients, including non-U.S. employees (except nationals of E:1 and E:2 countries) of U.S. companies, subsidiaries of companies headquartered in the United States, and private sector end users[104] headquartered in a list of favored countries contained in Supplement 3 to Part 740, subject to some conditions and restrictions. One such restriction is that the resulting encryption products from these license exception ENC exports remain subject to the EAR.
2. **License exception ENC (740.17(b) with a classification determination (CCATs) or self-classification.** The remaining flavors of license exception ENC require either a formal classification determination from BIS (traditionally called a CCATs)—for the more tightly controlled encryption items listed in 740.17(b)(2) and (b)(3)—or a self-classification and annual self-classification report for the less tightly controlled items in 740.17(b)(1) (which bucket includes the preceding mass market

items). A detailed look into these three buckets is beyond the scope of this chapter, but in a nutshell:

1. ENC restricted items in 740.17(b)(2) include:
   (A) Network infrastructure commodities and software with key lengths exceeding 80 bits for symmetric algorithms for WAN, MAN, VPN, backhaul, or long-haul throughput equal to or greater than 250 Mbp, transmission over satellite at data rates exceeding 10 Mbps, media (voice/video/data) encryption or encrypted signaling to more than 2,500 endpoints, and terrestrial wireless infrastructure meeting certain criteria.
   (B) "Encryption source code" that is not publicly available.
   (C) Customized items for government end users or end uses or for customer specification or where the user can easily change it.
   (D) Quantum cryptography.
   (F) Network penetration tools. Encryption commodities and software that provide penetration capabilities that are capable of attacking, denying, disrupting, or otherwise impairing the use of cyber infrastructure or networks.
   (G) Public safety/first responder radio (private mobile radio (PMR)).
   (H) Specified cryptographic ultra-wideband and "spread spectrum" items.
   (I) Cryptanalytic commodities and software.
   (J) "Open cryptographic interface" items to any end user located or headquartered in certain designated countries.
   (K) Specific encryption technology.
2. ENC unrestricted items in 740.17(b)(3) include:
   (A) Non-"mass market" "components," toolsets, and toolkits.
   (B) "Non-standard cryptography" (by items not otherwise described in EAR section 740.17(b)(2)).
   (C) Advanced network vulnerability analysis and digital forensics.
   (D) "Cryptographic activation" commodities, components, and software.

3. ENC unrestricted items in 740.17(b)(1) include everything else. License exception ENC items that fall under 740.17(b)(1) and (b)(3) are frequently referred to as ENC unrestricted items because, once you have filed the classification request and waited 30 days (for (b)(3) items) or self-classified (for (b)(1) items), the items can be exported anywhere in the world except the E:1 and E:2 countries, although for certain (b) (3) items there are additional bi-annual export reporting requirements. By contrast, license exception ENC items that fall under 740.17(b)(2) are frequently referred to as ENC restricted items because even after classification, the items only may be exported to certain end users in certain countries, and the precise rules vary depending on the precise 740.17(b)(2) sub-grouping. In addition, license exception ENC restricted items are subject to bi-annual export reporting.

In cases where license exception ENC does not apply, the exporter must obtain a license from BIS for the export. Due to the breadth of ENC, however, licensing is typically limited to a small class of 740.17(b)(2) items going to government end users in countries other than the ENC-favored countries in Supplement 3 to Part 740.

A heads-up: U.S. export control practitioners, used to the breadth of U.S. mass market and license exception ENC, are frequently surprised to encounter far more stringent export control (and import and use) regimes in other countries of the world. For this reason, the country chapters of this Handbook specifically address the encryption controls of their respective countries.

---

1. Thad McBride is a partner at the law firm of Bass Berry & Sims PLC. Mark Sagrans is Corporate Trade and Compliance Counsel, DuPont Legal. Scott Maberry is a partner at the law firm of Shepard Mullin Richter & Hampton LLP. This chapter was prepared in the usual manner, that is, with younger lawyers doing most of the hard work and the listed authors taking most of the credit. Many thanks in particular to Mi-Yong Kim and Sylvia Yi of Bass Berry and Nimrah Najeeb of Crowell & Moring. The authors also thank Kay Georgi who drafted the encryption controls section (in addition to editing the chapter and the entire handbook!). The listed authors take full responsibility for the content of this chapter, including any errors.

2. The EAR were at one time often described as covering so-called dual use items, on the theory that the items subject to the EAR potentially could be used for either civil or military purposes. *See, e.g.*, 15 C.F.R. § 730.3 (2010), "General Information" (stating that, "in general, the term dual use serves to distinguish EAR-controlled items that can be used both in military and other strategic uses

and in civil applications from those that are weapons and military related use or design and subject to the controls of the Department of State or subject to the nuclear related controls of the Department of Energy or the Nuclear Regulatory Commission."). But the term "dual use" tends to create confusion, and BIS has largely abandoned it as part of its 2011 Export Control Reform Initiative. *See* 76 Fed. Reg. 41,971 (July 15, 2011). Therefore, the term is not used extensively in this chapter. The items subject to the EAR are best distinguished from ITAR-controlled items on the grounds that items that are listed positively on the U.S. Munitions List (USML) are covered by the ITAR (*see* Chapter 2, *supra*); whereas items not specifically listed on the USML are generally covered by the EAR. Additionally, as a result of export control reform, the EAR includes many low-level military items that migrated from the USML to the Commerce Control List.

3. For the previous two decades, the statutory authority for the EAR had been the Export Administration Act of 1979. That act lapsed on August 21, 2001, and was never renewed, but Executive Order 13,222 kept the EAR in effect under the President's authority pursuant to the International Emergency Economic Powers Act (IEEPA). *See, e.g.*, Revision and Clarification of Civil Monetary Penalty Provisions of the Export Administration Regulations, 71 Fed. Reg. 44,189 (Aug. 4, 2006). However, in 2018, Congress enacted the Export Control Reform Act of 2018 (ECRA), Pub. L. 115–232, Aug. 13, 2018, 132 Stat. 2208, codified at 50 USCA 4801–4852, which provides a permanent statutory authority for the EAR. *See* Section 3.2, *infra*.

4. The steps described here are somewhat simplified. The EAR section titled "Steps for Using the EAR" describes 29 distinct steps in detail. *See* 15 C.F.R. pt. 732. A helpful graphical summary of the steps for using the EAR is provided at 15 C.F.R. pt. 732 supp. 1 (available online at http://www.bis.doc.gov/policiesandregulations/ear/732.pdf).

5. 15 C.F.R. § 774 supp. 1.

6. Note that under the EAR, the U.S. government controls both exports and re-exports of items. A re-export is an export of an item subject to the EAR from one country outside the United States to another. As a general matter, the U.S. government treats exports and re-exports the same under the EAR, for example, if an item would require a license for export from the United States to country A, a license would also be needed to re-export that same item to country A from country B. Thus, for purposes of this chapter, any reference to "export" should be interpreted to incorporate "re-export" as well.

7. Those agencies include the following:

- U.S. Nuclear Regulatory Commission (NRC). Regulations administered by the NRC control the export and re-export of items related to nuclear reactor vessels. *See* 10 C.F.R. pt. 110; *see also* Atomic Energy Act of 1954, as amended, 42 U.S.C. §§ 2011 *et seq*.
- U.S. Department of Energy (DOE). Regulations administered by the DOE control the export and re-export of technology related to the production of special nuclear materials. *See* 10 C.F.R. pt. 810; *see also* Atomic Energy Act of 1954, as amended (42 U.S.C. §§ 2011 *et seq*.).
- U.S. Patent and Trademark Office (PTO). Regulations administered by the PTO provide for the export of unclassified technology in connection with patent applications and related filings. *See* 37 C.F.R. pt. 5.
- U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC). OFAC administers the U.S. economic sanctions and embargoes contained in 31 C.F.R. ch. V. Exports to embargoed destinations are generally covered by these regulations. *See* Chapter 1, *supra*. In large part, these regulations are *concurrent* with the EAR and violations of OFAC's regulations may simultaneously violate the EAR.

8. http://www.bis.doc.gov/licensing/exportingbasics.htm.

9. *See* 15 C.F.R. § 734.3. The de minimis rule is different depending on the destination of the item. For destinations subject to U.S. embargo, if the controlled U.S.-origin content is valued at 10 percent or less of the total value of the item, the item is not subject to the EAR. For destinations not subject to embargo, if the controlled U.S.-origin content is valued at 25 percent or less of the total

value of the item, the item is not subject to the EAR. For certain special items, such as certain encryption items and military parts and components subject to the EAR, there is no de minimis level.

10. *See id.* § 734.9.

11. While posting information on the internet may also constitute an export, the regulatory treatment of internet exports is complicated by the fact that items on the open internet are considered to be publicly available, and thus not subject to the EAR. *See* Section 3.3 *infra*.

12. *See* 15 C.F.R. § 734.15.

13. *See* 15 C.F.R. § 734.3(b) ("Items Not Subject to the EAR").

14. Open source encryption software that is classified as ECCN 5D002 is "published" as defined by 15 C.F.R. § 734.7 only if it is notified to BIS and the National Security Agency as set forth in 15 C.F.R. § 742.15(b). For more information on the complex encryption classification and licensing regime, *see* Section 3.15, *infra.*

15. The rules for what constitutes "publication" for these purposes are provided in 15 C.F.R. § 734.7.

16. *See* 15 C.F.R. § 734.8. What constitutes "fundamental research" can get complicated quickly depending on, for example, publication restrictions that may be imposed on the results of what would otherwise appear to be fundamental research conducted in a university laboratory setting.

17. *See id.* §§ 734.3(b)(3)(iv), 734.10.

18. http://www.bis.doc.gov/snap/index.htm.

19. Today, many exporters use the term "CCATS" to refer to the BIS classification itself, as opposed to the tracking system. Note that export classifications can change as technologies develop so periodic review of classifications, even those established through a formal CCATs, is a good idea particularly as it can lead to an easing of licensing requirements.

20. 15 C.F.R. § 734.3(a)(1–2).

21. *See id.* §§ 732.3(b)(3), 734.3(c).

22. *See id.* pt. 774, supp. 1.

23. *See* Section 3.6, *infra.*

24. U.S. Department of Commerce, Bureau of Industry and Security, Denied Persons List, http://www.bis.doc.gov/dpl/thedeniallist.asp.

25. 15 C.F.R. pt. 744, supp. 4.

26. In this case, "AT" or anti-terrorism controlled items. For more information on AT controls, see Section 3.7.

27. 15 C.F.R. § 736.1(c).

28. *Id.* § 736.2(b).

29. Applications for such authorizations are not filed through the normal licensing process of SNAP-R, but instead through a hard copy letter submitted to the Office of Exporter Services (see discussion *infra* at Section 3.9).

30. Because regime members share the same guidelines, they usually share the same controls, thus requiring licenses for the same items to the same non-member states. However this is not always the case because determining applicability of specific controls to specific items remains a member's sovereign decision.

31. For example, Russia was admitted to Wassenaar in a fit of post–Cold War exuberance, but many of the licensing agreements that otherwise exist between Wassenaar member states have since been rolled back with respect to Russia due to the decline in the U.S.–Russia relationship. The lesson is that the world of trade controls evolves with foreign policy and national security considerations.

32. The Firearms Convention referred to here is the Inter-American Convention Against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives, and Other related Materials (Nov. 14, 1997), governing nations of the Organization of American States.

33. A license is required for the export to any destination of an item controlled as an implement of torture. *See* 15 C.F.R. § 742.11.

34. A license is required for the export to any destination of an item controlled for surreptitious listening (SL) purposes. *See id.* § 742.13.

35. *See id.* pt. 774, supp. 1.

36. 15 C.F.R. pt. 744.

37. *See id.* §§ 744.2, 744.4, 744.5, 744.21.

38. *See id.* pt. 744, supp. 4 (Entity List); U.S. Department of Commerce, Bureau of Industry and Security, Denied Persons List, http://www.bis.doc.gov/dpl/thedeniallist.asps; 15 C.F.R. § 744.12 (referring to SDN list, 31 C.F.R. ch. V, app. A).

39. *See* BIS, Lists to Check, http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm. The Department of Commerce has also published a consolidated list of most other important lists. That consolidated list is available at http://export.gov/ecr/eg_main_023148.asp.

40. 15 C.F.R. pt. 738, supp. 1.

41. *See id.* § 738.1(b).

42. *See, e.g.*, ECCN 0A983 (Specially designed implements of torture—noting that a license is required for all destinations).

43. *See, e.g.*, 15 C.F.R. § 774 supp. 1, ECCN 7A994.

44. *Id.* § 738.3(a); *see generally* 15 C.F.R. § 738.4.

45. For information on license determinations, *see generally* 15 C.F.R. § 738.4.

46. *See id.* § 734.2(b)(2)(ii).

47. *See id.* pt. 734.

48. The full list of license exceptions, and details related to each, are contained in 15 C.F.R. pt. 740.

49. 15 C.F.R. § 740.15.

50. *Id*. § 736.2(b).

51. *Id.* § 740.2.

52. *See id.* pt. 740, supp. 1.

53. For exports under license exceptions GBS, LVS, APP, TSR, or GOV, it is important to determine the applicability of certain reporting requirements under 15 C.F.R. § 743.1.

54. http://www.bis.doc.gov/snap/index.htm.

55. 15 C.F.R. § 736.2(b)(9); *see also* Section 3.6, *supra.*

56. *Id.* § 736.2(b)(10); *see also* Section 3.6, *supra.*

57. Note that if the support would require a license—for example technical assistance that would require a license—the authorization request is still made via SNAP-R, although the SNAP-R license request should be sure to reference the past export and the pending voluntary disclosure to ensure it is complete.

58. BIS also has published its "Guidance on Charging and Penalty Determinations in Settlement of Administrative Enforcement Cases," 15 C.F.R. pt. 766, supp. 1, which describes BIS's approach to EAR violations. The Guidance specifically includes a list of both mitigating and aggravating factors the agency will consider when making a penalty determination.

59. 15 C.F.R. pt. 732, supp. 3.

60. *See* BIS, Red Flag Indicators, www.bis.doc.gov/complianceandenforcement/redflagindicators.htm.

61. 15 C.F.R. pt. 732, supp. 3.

62. 50 U.S.C. § 1705.

63. *Id.*

64. Civil penalties are adjusted annually for inflation so this number steadily increases. As of January 2022, the adjusted penalty figure was $328,121. *See* 87 Fed. Reg. 157 (Jan. 4, 2022), https://www.federalregister.gov/documents/2022/01/04/2021-28118/civil-monetary-penalty-adjustments-for-inflation.

65. *See* ECRA, 50 U.S.C. § 4819.

66. U.S. Department of Commerce, Bureau of Industry and Security, *Commerce Implements Sweeping Restrictions on Exports to Russia in Response to Further Invasion of Ukraine*," Feb. 24, 2022, https://bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/2914-2022-02-24-bis-russia-rule-press-release-and-tweets-final/file.

67. *Id.*

68. U.S. Department of Commerce, Bureau of Industry and Security, *Implementation of Sanctions against Russia under the Export Administration Regulations (EAR)*, 87 FR 12226 (Mar. 3, 2022), https://www.federalregister.gov/documents/2022/03/03/2022-04300/implementation-of-sanctions-against-russia-under-the-export-administration-regulations-ear.

69. *See, e.g.*, BIS, *Additions of Entities to the Entity List*, 87 FR 20295 (Apr. 1, 2022), https://www.federalregister.gov/documents/2022/04/07/2022-07284/additions-of-entities-to-the-entity-list; BIS, *Additions of Entities to the Entity List*, 87 FR 34154 (June 6, 2022), https://www.federalregister.gov/documents/2022/06/06/2022-12144/additions-of-entities-to-the-entity-list; BIS, *Addition of Entities, Revision and Correction of Entries, and Removal of Entities From the Entity List*, 87 FR 38920 (June 30, 2022), https://www.federalregister.gov/documents/2022/06/30/2022-14069/addition-of-entities-revision-and-correction-of-entries-and-removal-of-entities-from-the-entity-list.

70. *Id.* at 12229.

71. BIS's own list of export control initiatives related to Russia since the invasion appears here: https://bis.doc.gov/index.php/policy-guidance/country-guidance/Russia-belarus (accessed July 14, 2022).

72. U.S. Department of Commerce, Bureau of Industry and Security, *Expansion of Sanctions against the Russian Industry Sector under the Export Administration Regulations (EAR)* (Mar. 8, 2022), https://www.federalregister.gov/documents/2022/03/08/2022-04912/expansion-of-sanctions-against-the-russian-industry-sector-under-the-export-administration.

73. *See* https://www.commerce.gov/news/press-releases/2022/04/bis-takes-enforcement-actions-against-three-russian-airlines-operating (accessed July 14, 2022); *see* specific denial orders (TDO) including the following: https://efoia.bis.doc.gov/index.php/documents/export-violations/export-violations-2022/1365-e2717/file (Aeroflot TDO); https://efoia.bis.doc.gov/index.php/documents/export-violations/export-violations-2022/1364-e2716/file (Azur Air TDO); https://efoia.bis.doc.gov/index.php/documents/export-violations/export-violations-2022/1366-e2718/file (UTAIR TDO); https://efoia.bis.doc.gov/index.php/electronic-foia/index-of-documents/7-electronic-foia/227-export-violations (Aviastar TDO); https://efoia.bis.doc.gov/index.php/documents/export-violations/export-violations-2022/1370-e2722/file (Rossiya TDO); https://efoia.bis.doc.gov/index.php/documents/export-violations/1374-belavia-tdo-final-6-16-2022/file (Belavia TDO); https://efoia.bis.doc.gov/index.php/documents/export-violations/1376-nordwind-tdo-final-6-24-22/file (Nordwind TDO); https://efoia.bis.doc.gov/index.php/documents/export-violations/1377-siberian-tdo-final-6-24-22/file(Siberia (aka S7) Airlines TDO); https://efoia.bis.doc.gov/index.php/documents/export-violations/1375-pobeda-tdo-final-6-24-22/file (Pobeda Airlines TDO) (accessed July 14, 2022).

74. BIS, *Expansion of Sanctions, supra* note 72.

75. BIS, *BIS Issues Charging Letter against Roman Abramovich for Violating U.S. Export Controls Related to Flights of His Private Jets* (June 6, 2022), https://bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3014-2022-06-06-bis-press-release-abramovich-charging-letter/file.

76. *See* Control of Firearms, Guns, Ammunition and Related Articles the President Determines No Longer Warrant Control Under the United States Munitions List (USML), 85 Fed. Reg. at 4136 (Jan. 23, 2020).

77. As of July 2022, the qualifying countries are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Turkey, and the United Kingdom. Certain limited exports are also permitted to additional countries under STA.

78. *See* https://www.bis.doc.gov/index.php/statool.

79. *See* Revisions to the Export Administration Regulations: Initial Implementation of Export Control Reform, 78 Fed. Reg. at 22,728 (Apr. 16, 2013).

80. *Id.*

81. *See* https://www.bis.doc.gov/index.php/specially-designed-tool.

82. 15 C.F.R. § 734.18 (referencing the countries in Country Group D:5). As of July 2022, the list of prohibited countries consisted of Russia and the D:5 countries: Afghanistan, Belarus, Burma, Cambodia, Central African Republic, China, Cuba, Cyprus, Democratic Republic of Congo, Eritrea, Haiti, Iran, Iraq, North Korea, Lebanon, Libya, Russia, Somalia, South Sudan, Sudan, Syria, Venezuela, and Zimbabwe.

83. More specifically, if the item meets the Huawei FDPR requirements, a license is required where there is "knowledge" that:

> (1) The foreign-produced item will be incorporated into, or will be used in the "production" or "development" of any "part," "component," or "equipment" produced, purchased, or ordered by any entity with a footnote 1 designation in the license requirement column of this supplement; or
>
> (2) Any entity with a footnote 1 designation in the license requirement column of this supplement is a party to any transaction involving the foreign-produced item, e.g., as a "purchaser," "intermediate consignee," "ultimate consignee," or "end-user."

84. The foreign-produced item is a direct product of "technology" or "software" subject to the EAR and specified in ECCN 3D001, 3D991, 3E001, 3E002, 3E003, 3E991, 4D001, 4D993, 4D994, 4E001, 4E992, 4E993, 5D001, 5D991, 5E001, or 5E991 of the CCL.

85. The foreign-produced item is produced by any plant or major component of a plant that is located outside the United States, when the plant or major component of a plant, whether made in the U.S. or a foreign country, itself is a direct product of U.S.-origin "technology" or "software" subject to the EAR that is specified in ECCN 3D001, 3D991, 3E001, 3E002, 3E003, 3E991, 4D001, 4D993, 4D994, 4E001, 4E992, 4E993, 5D001, 5D991, 5E001, or 5E991 of the CCL.

86. *See* Export Administration Regulation: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List, 85 Fed. Reg. 34306 (May 19, 2020).

87. *See* Expansion of Export, Reexport, and Transfer (in-Country) Controls for Military End Use or Military End Users in the People's Republic of China, Russia, or Venezuela, 85 Fed. Reg. 34306 (June 3, 2020).

88. *See* Addition of "Military End User" (MEU) List to the Export Administration Regulations and Addition of Entities to the MEU List, 85 Fed. Reg. 83793 (Dec. 23, 2020). In addition, the MEU list is not exhaustive. As described in Chapter 1, OFAC has designated multiple Russian (and Belarusian) military entities as prohibited and restricted parties, and other U.S. government agencies, including within the Defense and State Departments, have published other lists designating Chinese and Russian military end users under section 231(e) of the Countering America's Adversaries Through Sanctions Act (CAATSA) and section 1237 of the National Defense Authorization Act for Fiscal Year 1999 (NDAA FY1999). These lists, which can be referenced at https://www.defense.gov/Newsroom/Releases/Release/Article/2434513/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/, will likely be updated regularly.

89. *See* Suspension of License Exceptions for Hong Kong (June 30, 2020), https://www.bis.doc.gov/index.php/documents/pdfs/2568-suspension-of-license-exceptions-for-exports-and-reexports-to-hong-kong/file.

90. *See* Removal of Hong Kong as a Separate Destination under the Export Administration Regulations, 85 Fed. Reg. 83765 (Dec. 23, 2020).

91. *See* Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities from the Entity List, 85 Fed. Reg. 83416 (Dec. 22, 2020).

92. *See* Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification, 87 Fed. Reg. 62,186 (Oct. 13, 2022), https://www.federalregister.gov/documents/2022/10/13/2022-21658/implementation-of-additional-export-controls-certain-advanced-computing-and-semiconductor.

93. *See* 83 FR 58,201 (Nov. 19, 2018), https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.

94. *See* 85 Fed. Reg. 36,483 (June 17, 2020), https://www.federalregister.gov/documents/2020/06/17/2020-11625/implementation-of-the-february-2020-australia-group-intersessional-decisions-addition-of-certain.

95. *See* 86 Fed. Reg. 59,070 (Oct. 26, 2021), https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2021/2865-86-fr-59070/file.

96. *See* 87 Fed. Reg. 31,195 (May 23, 2022), https://bis.doc.gov/index.php/documents/federal-register-notices-1/2997-marine-toxins-proposed-rule-87-fr-31195-5-23-2022/file.

97. The Committee on Foreign Investment in the United States is U.S. interagency government body that has the authority to review foreign investment in a U.S. business, and may—in rare cases—ultimately recommend to the President that the investment should be blocked. For additional information related to CFIUS, refer to the committee's website: https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius

98. BIS maintains two helpful flowcharts to assist with analysis related to encryption; one of those flowcharts specifically addresses the determination of whether an item is subject to encryption controls. The flowcharts are available at https://www.bis.doc.gov/index.php/documents/encryption/327-flowchart-1/file.

99. *See* 15 C.F.R. §§ 734.7(a) & (b), 742.15(b).

100. Nonstandard cryptography means any implementation of "cryptography" involving the incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body (e.g., IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA, and GSMA) and have not otherwise been published.

101. a.1. Items having "information security" as a primary function;

a.2. Digital communication or networking systems, equipment or components, not specified in paragraph 5A002.a.1;

a.3. Computers, other items having information storage or processing as a primary function, and components therefor, not specified in paragraphs 5A002.a.1 or .a.2; N.B.: For operating systems, see also 5D002.a.1 and .c.1.

a.4. Items, not specified in paragraphs 5A002.a.1 to a.3, where the "cryptography for data confidentiality" having a "described security algorithm" meets all of the following:

a.4.a. It supports a non-primary function of the item; and

a.4.b. It is performed by incorporated equipment or "software" that would, as a standalone item, be specified by ECCNs 5A002, 5A003, 5A004, 5B002 or 5D002.

102. In fact, to qualify as mass market, it is first necessary to ensure that the item does not fall within several more strictly controlled categories of encryption items. *See* 15 C.F.R. § 740.17(b). This summary of mass market eligibility assumes the item is not covered by one of those categories.

103. This self-classification reporting requirement is detailed in 15 C.F.R. § 740.17(e)(3) and Supplement 8 to 15 C.F.R. pt. 742.

104. A "private sector end user" is either an individual who is not acting on behalf of any foreign government, or a commercial firm (including its subsidiary and parent firms, and other subsidiaries of the same parent) that is not wholly owned by, otherwise controlled by, or acting on behalf of, any foreign government.

Appendix

Recent Export Enforcement Matters

BIS has settled multiple export matters in recent years. Many of these matters involve individuals. Four enforcement matters are described briefly here. While ZTE is particularly remarkable, the other three—involving VTA Telecom, Milwaukee Electric Tool, and Cotran Corporation—are less facially interesting. Yet each illustrates an element of the BIS enforcement regime that is worth noting, and thus in that way may be of more immediate relevance to most exporters than ZTE, which is something of an outlier.

VTA Telecom. In October 2021, BIS announced that it had imposed a civil penalty fine against VTA Telecom Corporation (VTA) for the unauthorized export of controlled commodities to Vietnam. VTA was established in 2013 as a California-based subsidiary of a Vietnamese state-owned telecommunications company. According to BIS, VTA procured and exported items from the United States to its parent company in Vietnam with knowledge that certain of those exports were intended to support a Vietnamese defense program. To settle the matter, VTA agreed to the following:

1. A penalty of $1,869,372
2. Expenditure of $25,000 to fund its internal export compliance program (ICP)
3. Hiring and retention of a Director of Trade Compliance to oversee VTA's export activities for at least two years

BIS's aggressive approach to VTA improving its compliance program could be indicative of BIS taking similar measures in future compliance resolutions.

Milwaukee Electric Tool. The company settled with BIS in January 2017 to resolve allegations of 25 separate violations of the EAR. According to BIS, Milwaukee Electric Tool exported thermal imaging cameras without the necessary export licenses to a number of countries. Notably, those countries included important U.S. trading partners such as Colombia, Hong Kong, and Mexico. Milwaukee Electric Tool agreed to pay a civil penalty of $301,000, although the cameras themselves were valued at less than half that amount. While the monetary amount of the settlement was relatively

small, the matter serves as a reminder that even exports of relatively routine items to well-established U.S. allies can require a license.

Cotran Corporation. The company, which is based in Portsmouth, Rhode Island, settled with BIS in November 2019 to resolve allegations of ten unauthorized exports of electric cattle prods. The exports, which required a license, were made to the Czech Republic, Mexico, South Africa, and Venezuela. BIS also charged the company with violating the recordkeeping provisions of the EAR. Cotran agreed to pay a civil penalty of $136,000 to resolve the matter. The total value of the export transactions that led to the violations was approximately $81,000. Like Milwaukee Electric, the penalty paid by Cotran was not particularly large—but the matter does serve as a useful reminder that recordkeeping is not only a good practice, it is required under the EAR.

ZTE Corporation. It is well beyond the scope of this chapter to summarize the U.S. government's enforcement efforts against ZTE Corporation, a Chinese company that is one of the world's largest telecommunications equipment manufacturers. In March 2017, ZTE agreed to a settlement with the U.S. government—including BIS—for alleged export violations involving shipments of U.S.-origin products to Iran and North Korea. At that time, ZTE agreed to a penalty of nearly $900 million to resolve the matter. In addition, as part of that settlement, ZTE agreed to a suspended seven-year denial order that BIS pledged to impose if ZTE deviated from the terms of the settlement agreement. That settlement agreement included, among other conditions, the requirement that ZTE continue to cooperate with the U.S. government regarding improving compliance measures and reporting on discipline of personnel.

In April 2018, the Commerce Department announced that ZTE had not adequately complied with the terms of the settlement agreement, and activated the denial order that had been suspended as part of the March 2017 settlement. This quickly became an existential crisis for ZTE. Ultimately, the company agreed to pay a penalty of approximately $1.3 billion to settle the matter—with the denial order being suspended again but subject to reactivation if ZTE did not comply with the terms of the settlement.

4

Anti-Money Laundering Controls

Cari N. Stinebower and Dainia J. Jabaji

4.1 Overview

Money laundering was first established as a crime in 1986, but has gained great regulatory and public attention post September 11, 2001, as a result of egregious terrorism funding that occurred through U.S. financial institutions. In recent years, money laundering has even been depicted in popular movies and TV shows such as the Netflix series “Ozark” and the popular Martin Scorsese film *The Wolf of Wall Street*. Alongside the growth in public awareness of money laundering, anti-money laundering (AML) laws and regulations have dramatically evolved and developed over time.

As with sanctions and export controls, AML rules and regulations are vital in protecting the domestic and international financial system, and our overall safety. These practice areas, compliance responsibilities, and enforcement investigations often overlap. This chapter provides an overview of AML rules and regulations, notes the key leading international AML organizations, and discusses 2019 and 2020 enforcement actions.

What are money laundering and terrorist financing? Money laundering is the practice of concealing or disguising illegally gained funds, thereby making the funds (and transactions) appear legal. Money laundering is usually accomplished in three steps: placement, layering, and integration.[1] Money laundering attempts to transform ill-gotten gains into “legitimate funds” by placing them into legitimate financial channels, including but not limited to annuity contracts, real estate, trade finance, life insurance

policies, and brokerage accounts. Terrorist financing is the process by which individuals utilize funds to fund illegal activity, that is, terrorist acts. Unlike money laundering, funds underlying terrorist financing may be derived from criminal activities *or* legitimate sources.

What is regulated? Traditional financial institutions and designated nonfinancial businesses and professionals (DNFBPs) are regulated to protect the financial system from exposure to money laundering and terrorist financing. These entities are regulated because they are "gatekeepers" and can help stop illicit financial transactions from entering "clean" commerce. However, over time, companies in nonfinancial industries have also become indirectly subject to AML rules as a trickle-down effect of having to comply with the policies and procedures of regulated financial institutions. Of note, in January 2024, the new Beneficial Ownership Reporting Rule comes into play and requires certain U.S. businesses to report beneficial owners to a newly created data base managed by the Department of the Treasury's financial Crimes Network (FinCEN).

Who are the regulators? In the United States, while there are close to a dozen domestic organizations that have substantial AML responsibilities,[2] the FinCEN maintains primary responsibility for administering the regulations as the United States' Financial Intelligence Unit (FIU). Internationally, some of the leading AML and terrorist financing controls groups include:

- The Financial Actions Task Force (FATF)
- The Egmont Group of Financial Intelligence Units
- The lead industry sector groups, including the Wolfsberg Group

Where to find the regulations. AML regulations are codified in the Bank Secrecy Act of 1970 (BSA)[3] at 31 C.F.R. Chapter X (2012) (formerly 31 C.F.R. 103).

How to get a license. The BSA does not contemplate licenses. Regulated financial institutions and DNFBPs are required to file suspicious activity reports (SARs) and other reports (e.g., currency transaction reports (CTRs) with FinCEN). SARs and other reports may be filed electronically through

FinCEN's e-filing system, which is available at http://bsaefiling.fincen.treas.gov/main.html. In addition, money services businesses and money transmitters also have reporting requirements both with FinCEN and with local state authorities. In some cases, the state authorities also require licensing for such businesses.

Key website. Key websites for AML compliance are http://www.fincen.gov/ and https://www.ffiec.gov/.

(a) The International AML Organizations

Money laundering is often facilitated cross-border, using various currencies, methods, and means. As a result, there are a number of important international organizations to help prevent money laundering. Some of these organizations include FATF, the Egmont Group of Financial Intelligence Units, and leading industry groups such as Wolfsberg Group. Also of note is the United Nations Panel of Experts, created pursuant to UNSCR 1874 (2009). The report highlights money laundering and proliferation financing trends used by the government of the Democratic People's Republic of Korea.

(b) The Financial Actions Task Force

FATF was established at the G-7 Summit in 1989 to examine money laundering techniques and trends, review the response taken at national or international levels, and establish measures to combat money laundering. FATF is not a rulemaking body, but has established principal reputable guidelines that are designed to protect the international financial system from money laundering and terrorist financing threats, and threats posed by proliferators of weapons of mass destructions.

In 1990, FATF issued a report containing a set of 40 recommendations (the "40 Recommendations") that provide a comprehensive plan of action needed to combat money laundering.[4] The 40 Recommendations were then revised in 1996 to reflect evolving money laundering typologies.[5] Further, after the terrorist attacks on September 11, 2001, the FATF issued Nine Special Recommendations to address terrorist financing threats.[6] On February 16, 2012, FATF published a revised 40 Recommendations, incorporating the Nine Special Measures and reorganizing the

recommendations into seven sections: (1) AML/CFT Policies and Coordination, (2) Money Laundering and Confiscation, (3) Terrorist Financing and Financing of Proliferation, (4) Preventative Measures, (5) Transparency and Beneficial Ownership of Legal Persons and Arrangements, (6) Powers and Responsibilities of Competent Authorities and Other Institutional Measures, and (7) International Cooperation. These 40 Recommendations, taken together with FATF's interpretive notes, are considered the international standard for combating money laundering.

FATF now consists of 37 members and two regional organizations.[7] While FATF is an inter-governmental policy-making body with no independent ability to enact laws,[8] it conducts reviews of its members and publishes reports via its Mutual Evaluation Process. During the Mutual Evaluation Process, FATF conducts reviews of its members to assess whether the member has implemented the FATF Recommendations, and provides a detailed description and analysis of each member's AML system.

The most recent FATF evaluation of the United States was in 2016. FATF found the country to have a strong regulatory system but to lack certain key features. In sum, the FATF found:

- The AML/combating the financing of terrorism (CFT) framework in the U.S. is well developed and robust. Domestic coordination and cooperation on AML/CFT issues is sophisticated and has matured since the U.S.'s previous evaluation in 2006. The U.S. also has a number of risk-assessment processes in place.
- The financial sectors bear most of the burden in respect of required measures under the BSA and that financial institutions, in general, have an evolved understanding of money-laundering risks and obligations and have systems and processes to support that understanding.
- Certain significant gaps exist under the regulatory framework and minimal measures are imposed on DNFBPs. The vulnerability of the DNFBP sectors is significant.
- Law enforcement efforts rest on a well-established task force environment that enables the pooling of expertise from a wide range of law enforcement agencies, including prosecutors to support quality investigation and prosecution outcomes.

- Lack of timely access to adequate, accurate, and current beneficial ownership information remains one of the fundamental gaps in the U.S. context.[9]
- At the federal level, the U.S. achieves over 1,200 money laundering convictions a year. However, there is no uniform approach to state-level AML efforts and it is not clear that all states give money laundering due priority.
- The federal authorities aggressively pursue high-value confiscation in large and complex cases in respect of assets located both domestically and abroad.
- The U.S. authorities effectively implement targeted financial sanctions for terrorism and proliferation financing purposes, though not all UN designations have resulted in domestic designations.
- AML/CFT supervision of the banking and securities sectors appears to be robust as a whole and is evolving for money service businesses through greater coordination at the state level. The U.S. has a range of sanctions and dissuasive remedial measures that it can impose on financial institutions, which seem to have the desired impact on achieving supervisory objectives.[10]

In March 2020, FATF published an updated report regarding the United States' 2016 assessment, documenting a number of actions the United States has taken to strengthen its AML/CFT framework, including in the areas of customer due diligence (CDD)—specifically beneficial owner identification and verification, cooperation and coordination between authorities to align AML/CFT requirements with data protection and privacy rules, criminalization of terrorist financing, and more.[11] While FATF noted the United States' progress in these areas, the overall ratings remained the same, with the exception of Recommendation 10, regarding CDD and beneficial owner diligence, for which the United States now ranks as being "largely complaint." Of the 40 Recommendations, FATF has now found the United States to be "largely compliant" with respect to 22; "compliant" with respect to nine; "partially compliant" with respect to five; and "noncompliant" with respect to four.

To further assist private industry sectors in addressing money laundering and terrorist financing threats, FATF has begun to issue industry-by-industry guidance on recommended best practices. FATF has issued risk-

based guidance for legal professionals, trust and company service providers, accountants, casinos, real estate agents, dealers in precious metals and stones, life insurance sector, money services businesses, securities sector, and commercial website and internet payment systems, and virtual currency systems.[12] In addition to the risk-based guidance for legal professionals, these publications should be appropriately considered by attorneys representing clients in these industries.

(c) The Egmont Group

As addressed earlier, a key component to the success of the global AML infrastructure is cooperation between jurisdictions. An important way jurisdictions share information and cooperate during cross-border investigations is through their respective FIUs, including FinCEN. Recognizing the benefits inherent in the development of an FIU network across regions, in 1995, a group of FIUs established an informal group for the stimulation of international cooperation.[13] The Egmont Group is currently composed of 165 FIUs, and meets regularly to address cooperation through the exchange of information, share information regarding cross-border and enterprise-wide suspicious transactions, compile best practices in FIU security and training, and share expertise.[14]

(d) The Wolfsberg Group

In addition to the FATF and the Egmont Group, perhaps the most prominent of the industry sector groups is the Wolfsberg Group, an association of 13 global banks established to develop financial services industry standards and related products for Know Your Customer (KYC), AML, and CFT policies.[15]

The Wolfsberg Group came together in 2000 to draft AML guidelines for the private banking sector. The Wolfsberg Anti-Money Laundering Principles for Private Banking were subsequently published in October 2000, revised in May 2002, and further amended in 2012.[16] The Wolfsberg Group has other helpful publications outside of its Private Banking guidelines. For instance, following September 11, 2001, in January 2002, the Group published a Statement on the Suppression of Financing of Terrorism,[17] and in November 2002, released the Wolfsberg Anti-Money

Laundering Principles for Correspondent Banking.[18] Also, the Group released the Wolfsberg Statement on Monitoring Screening and Searching in 2003, and in 2004, it developed a due diligence model for financial institutions, in cooperation with Banker's Almanac.[19] The due diligence questionnaire was updated in 2014, and again in 2017 with related FAQs published in February 2018.[20] The Wolfsberg Group has published numerous other trusted sets of guidance for financial institutions and helpful FAQs dealing with AML issues in the context of commercial banking, correspondent banking, beneficial ownership, Politically Exposed Persons (PEPs), intermediaries, and more.[21]

(e) UN Panel of Experts—Democratic People's Republic of Korea Report

The United Nations Panel of Experts produces periodic reports detailing patterns of money laundering and sanctions evasion and avoidance by the Democratic People's Republic of Korea.[22] The March 2019 Report includes numerous examples of how the international financial system is used by the North Korean regime to continue its proliferation activities and raise money for the regime.[23]

4.2 U.S. Anti-Money Laundering Laws and Regulations

Domestically, following September 11, 2001, the U.S. government passed the USA PATRIOT Act, a portion of which amended the BSA (originally passed in 1970) to strengthen domestic anti-money laundering laws and regulations. While there are close to one dozen organizations that have substantial BSA responsibilities,[24] Fin-CEN maintains primary responsibility for administering the BSA.[25]

The BSA regulations apply to "financial institutions," which is broadly defined to include insured banks; commercial banks or trust companies; private bankers; agencies or branches of foreign banks in the U.S.; credit unions; thrift institutions; broker-dealers; investment bankers; currency exchange companies; issuers and redeemers of traveler's checks/money orders; operators of credit card systems; insurance companies; dealers in precious metals, stones, or jewels; pawnbrokers; loan or finance companies;

travel agencies; money transmitters; telegraph companies; businesses engaged in vehicle sales, including automobile, airplane, and boat sales; persons involved in real estate closings and settlements; the U.S. Postal Service; certain casinos and gaming establishments; and more. However, the specific requirements amongst the aforementioned entities may vary depending on the entity's business type, and some business types are currently exempt from the requirement to establish an AML program.[26]

Aside from the BSA, other relevant money-laundering rules and regulations include the Money Laundering Control Act of 1986, which criminalizes money laundering and structuring or the attempt to structure a financial transaction to avoid the reporting requirement;[27] and the USA PATRIOT Improvement and Reauthorization Act of 2005, which enhances penalties for terrorist financing, amends the Racketeer-Influenced and Corrupt Organizations Act by adding illegal money transmitters to the definition of racketeering activity, and closes a loophole concerning money laundering through informal money transfer networks.[28]

The Department of Justice (DOJ) prosecutes criminal money-laundering cases. Within the DOJ, the Money Laundering and Asset Recovery Section (MLARS) leads AML enforcement cases.[29] MLARS is comprised of seven units, including the Bank Integrity Unit, International Unit, Money Laundering and Forfeiture Unit, Policy Unit, Program Management and Training Unit, Program Operations Unit, and Special FIU.[30] MLARs is charged with (1) prosecuting and coordinating complex, sensitive, multi-district, and international money laundering and asset forfeiture investigations and cases; (2) providing legal and policy assistance and training to federal, state, and local prosecutors and law enforcement personnel, as well as to foreign governments; (3) assisting the DOJ and interagency policy makers by developing and reviewing legislative, regulatory, and policy initiatives; and (4) managing the DOJ's Asset Forfeiture Program, including distributing forfeited funds and properties to appropriate domestic and foreign law enforcement agencies and to community groups within the United States, as well as adjudicating petitions for remission or mitigation of forfeited assets.[31]

4.3 Complying with U.S. AML Laws and Regulations

The BSA imposes a number of requirements on the entities under its purview to help prevent money laundering. For example, the BSA requires that financial institutions file SARs, CTRs, and other reports with FinCEN.[32] Further, most regulated entities are also required to establish and maintain a customer identification program (CIP),[33] and maintain an appropriate, overarching AML program reasonably designed to ensure that the financial institution meets its reporting, recordkeeping, and other obligations.[34] Regulated entities are also required to respond to inquiries from FinCEN under section 314 of the USA PATRIOT Act and maintain appropriate records.

(a) Risk Assessments

Covered financial institutions are required to have a risk-based compliance program, which means they must first have an understanding of their respective money laundering and terrorist financing risks. Risk assessments at an institutional level and on a customer level are important in creating and implementing risk-based due-diligence procedures that include controls to enable the financial institution to detect and report any known or suspected money laundering. In general, an entity covered by the BSA is expected to conduct a comprehensive evaluation of the level of risk for its (1) products, (2) services, (3) customers, and (4) geographic exposure. Each of the four categories should be carefully assessed, and generally be rated as low, moderate, or high risk for money laundering (though different terminology may be used).

With regard to products and services, the previous Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money Laundering Examination Manual (BSA/AML Exam Manual)[35] (primarily focused on depository institutions) identified as higher risk: electronic services, private banking, monetary instruments, trade finance, foreign correspondent accounts, trust and asset management services, trade finance, services provided to third-party payment processors or senders, foreign exchange, lending activities, special use accounts, and non-deposit account services.[36] There are also higher risks for money laundering in certain operational circumstances, such as wherever the entity and the customer are not face-to-face, where the entity “touches the money” for the customer, and where transactions occur across borders. The previous BSA/AML

Exam Manual also provided examples of higher-risk customers. Higher-risk customers include foreign financial institutions, nonbank financial institutions, nonresident aliens, senior foreign government officials and their immediate family members and close associates (i.e., Politically Exposed Persons, or PEPs), cash-intensive businesses, nongovernmental organizations and charities, deposit brokers, and professional service providers (e.g., lawyers, accountants, doctors, or real estate brokers).[37]

On April 15, 2020, the FFIEC released updates to BSA/AML Exam Manual to clarify that bank examinations must be risk-based.[38] The update made clear that bank examiners should not take a one-size-fits-all approach to its examinations, and the examiners must consider each financial institution's BSA/AML program based on its specific risks for money laundering, terrorist financing, and other illicit activity. The update also clarified what standards are regulatory requirements as opposed to supervisory expectations. Overall, the update to the Manual did not impose new requirements on financial institution—instead, the update provided clarifications and reminders regarding the flexibility of institutions and examiners with respect to AML programs and AML program examination.

There are a number of resources to consider when determining geographic risks. For instance, FinCEN has pointed to the State Department's International Narcotics Control Strategy Report as an indicator of high-risk jurisdictions.[39] Other resources for geographic risk rankings include Transparency International's Corruption Index;[40] the list of countries targeted for sanctions administered by OFAC;[41] jurisdictions determined to be "of primary money laundering concern" by FinCEN pursuant to Section 311 of the USA PATRIOT Act;[42] countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979;[43] and countries identified in section 126.1 of the International Traffic in Arms Regulations (ITAR).[44] Where a geographic risk is identified, entities subject to the BSA are expected to conduct additional due diligence processes to mitigate against that risk.

(b) The Compliance Program

Once a covered entity has conducted its risk assessment and rates its risks, the entity should develop written policies, procedures, and processes to

address how it will protect itself, its customers, and the financial system from exposure to money laundering and terrorist financing. The FFIEC provides that the AML compliance program must (1) be in writing; (2) be approved by senior management; (3) contain sufficient internal controls to ensure ongoing compliance; (4) identify an individual or individuals responsible for managing BSA compliance; (5) offer training to relevant personnel; and (6) be subject to independent auditing and testing to ensure the program remains effective in mitigating potential exposure to money laundering and terrorist financing threats.[45] Because some of the higher risks from an AML perspective are similar to those from a sanctions or anti-bribery/anti-corruption perspective, there are often opportunities to streamline an entity's compliance programs.

For years, financial institutions spoke of "four pillars" of an AML program. These pillars included (1) written policies and procedures, (2) a designated AML compliance officer, (3) independent testing of the institution's AML program, and (4) implementation of an adequate employee training program; however, as of May 2018, covered financial institutions now have a fifth pillar—the development and establishment of risk-based CDD procedure. FinCEN issued its Final Rule for financial institutions for their CDD on May 11, 2016. The Final Rule required full compliance by May 11, 2018, and imposed a new requirement on covered financial institutions to identify and verify the identity of the individuals behind the legal entity customers.

(c) CIP

As noted earlier, financial institutions must have a risk-based CIP. The CIP should allow the bank to form a reasonable belief that it knows the true identity of each customer, and include procedures for document gathering at account opening, and risk-based procedures for verifying the identity of each customer. This process is often referred to as "knowing your customer," or KYC. In KYC, an entity ensures that the customers that it brings in are who they say they are, are conducting legitimate business, and are using legitimate funds. Typically, these assurances are provided during the on-boarding process and by continued transaction monitoring. Before opening an account for a new customer, financial institutions must collect certain identifying information from the client, which should then be

verified through documentary or nondocumentary means. For an individual, this can mean collecting the following:

- The customer's complete name (including former names and aliases)
- A copy of valid government-issued photo identification
- Date of birth
- Current street address
- Proof of current address (i.e., utility bill, bank or credit card statement)

For an entity customer, the following information may be collected:

- Complete name of the entity
- Complete name of contact person
- Address for entity and for contact person
- Certified true copy of certificate of incorporation or registration or other document evidencing establishment
- Details of registered office and place of business
- Due diligence documents as identified for beneficial owners holding more than 25 percent of an interest in the entity

Lesser due diligence is appropriate for U.S. publicly traded entities or other regulated entities; greater due diligence is appropriate for entities comprised of senior government officials, their families or associates—or for instances where red flags are present.

(d) Beneficial Owners

Most BSA-regulated entities must collect beneficial ownership information. In addition, effective January 1, 2024, the vast majority of privately held corporations, limited liability companies and other similar entities created in, or registered to do business in, any of the states and territories of the United States will be subject to ultimate beneficial ownership (UBO) information reporting requirements under FinCEN's highly anticipated "Final UBO Rule," which implements the beneficial ownership information reporting requirements of the Corporate Transparency Act (CTA).[46] Many key entities are exempt from the Final UBO Rule's reporting requirements, including inactive entities, some subsidiaries, banks and credit unions, and Securities and Exchange Commission reporting issuers. The Final UBO Rule does not replace FinCEN's existing customer due diligence (CDD)

rule requiring U.S. financial institutions to collect UBO information from their legal entity customers, although FinCEN will be revising the CDD rule to align it with the CTA.

Under the CTA, a "beneficial owner" of a company is "any individual, who, directly or indirectly, either exercises substantial control over such reporting company or owns or controls at least 25 percent of the ownership interests of such reporting company."[47] Thus, initial reports made to FinCEN must include, in addition to other information, the following information for each beneficial owner of the entities subject to the Final UBO Rule:

- Full legal name
- Date of birth
- Current residential address
- Unique identifying number from an acceptable identification document (or, if information has already been provided to FinCEN, by a FinCEN identifier).

In the coming year, FinCEN will engage in additional rulemakings related to the Final UBO Rule, develop compliance and guidance documents to assist entities in complying with this rule, and will continue to develop the necessary infrastructure to administer these requirements in accordance with the strict security and confidentiality requirements of the CTA, including the information technology system that will be used to store beneficial ownership information: the Beneficial Ownership Secure System (BOSS).

As an initial step in publishing additional rules relating to accessing beneficial ownership information, on December 15, 2022, FinCEN published the Notice of Proposed Rule Making[48] for the standards that financial institutions and government entities to access the beneficial ownership information to be housed within the BOSS. The NPRM also proposes regulations to specify when and how reporting companies can use FinCEN identifiers to report the BOI of entities. Comments are due February 14, 2023.

(e) Other Requirements for Financial Institutions under the BSA

Also within the BSA's expectations for risk based compliance program's policies and procedures are other internal controls to ensure compliance, such as policies and procedures for filing SARs and CTRs. For example, in the SAR context, in order to ensure that suspicious activity is identified promptly, relevant employees must know what to look for and must know to whom to report. An established reporting chain is essential to ensure that potentially suspicious activity is escalated to the appropriate AML compliance officer/s and, where appropriate, SARs are filed.

Further, in addition to the role the AML compliance officer will play in developing and evolving the entity's compliance program, an entity must ensure that the program is independently reviewed and audited to ensure effectiveness. Independent review does not require an outside party to conduct the review; only that someone other than the compliance officer or someone in his chain of command conduct the review. Of course, records for the review, including recommendations and steps taken to implement the recommendations should be maintained. To ensure compliance, companies should be sure to implement and maintain overall recordkeeping and training policies and procedures as well.

(f) Violations

The BSA and its related regulations provide for civil penalties, criminal penalties, and forfeiture of assets depending on the degree of intent involved, the specific entity type, and the AML program violation involved (including, e.g., recordkeeping violations or SAR violations).

Most civil penalties are assessed by FinCEN, whereas penalties for failures regarding Foreign Bank and Financial Account Reports (FBARs) are assessed by the IRS.

While an AML compliance program may look and operate in a manner consistent with sanctions and export controls compliance programs, the concept of a voluntary self-disclosure differs. The BSA regulations do not contain enforcement guidelines providing for mitigating credit where a covered financial institution detects and self-reports an AML program deficiency. Rather, an entity must first decide whether the entity is required to disclose potential AML program deficiencies resulting in potential violations of AML laws and regulations to the entity's other regulators. For example, an entity regulated by the Federal Reserve may notify that

regulator during a routine exam that the entity has identified a potential problem and is in the process of amending procedures. Entities regulated by the SEC and FINRA must consider whether they are required to report a potential BSA violation under the relevant rule and, if not, whether a disclosure will provide cooperating credit.[49]

(g) Compliance Program Pitfalls

There are a few common compliance program pitfalls that occur when either (1) policies and procedures are too stringent to implement and personnel create work-arounds or other informal processes to address practical issues; or (2) the compliance program is not appropriately tailored to the institution's risk.

When a regulator or enforcement officer reviews the entity's policies and procedures, one of the first items typically to be examined will be compliance with those written policies and procedures; many entities have found themselves to be out of compliance with their own policies and procedures. To help mitigate against this pitfall, the AML program should be periodically tested to ensure that the policies and procedures strike the appropriate balance between protecting against money-laundering risks and conducting a productive business. Where relevant, testing should include ensuring that automated screening software is neither creating so many false positive matches that compliance officers suffer from screening fatigue (and miss the few true hits), nor tuned so high that it misses close matches to sanctioned parties.

Further, each institution carries a unique risk based on its customer base, its geographic areas of operations, its products and services offered, and more. Compliance programs must be tailored to meet each individual institution's specific risks, or the program will likely have gaps where potential money laundering could go unnoticed.

Other common pitfalls include failing to obtain management support for the program; understaffing the compliance function so that higher risk transactions pass through undetected; failing to adequately train (or provide periodic updated training to) all relevant personnel; and failing to maintain adequate records so that compliance personnel are not able to retrace a decision-making process when at a later date asked by an examiner (or the DOJ).

(h) FinCEN Inquiries

On occasion, FinCEN may receive a request from a law enforcement agency requesting that FinCEN solicit information from a financial institution related to a terrorist activity or money-laundering investigation. Such requests in the United States are made pursuant to section 314(a) of the USA PATRIOT Act. When law enforcement requests such information from FinCEN, it should provide FinCEN with:

- A statement that each individual, entity, or organization about which the law enforcement agency is seeking information is engaged in, or is reasonably suspected based on credible evidence of engaging in, terrorist activity or money laundering
- Specific identifying information such as date of birth, address, and social security number so that the entity can differentiate between common or similar names
- A contact person at the law enforcement agency who can respond to any questions relating to the request[50]

FinCEN may thereafter request of financial institutions whether they have maintained accounts for or have engaged in transactions with any specified individual, entity, or organization. Such requests for information generally require that the entity search its records to determine whether it maintains or has maintained accounts for, or has engaged in transactions with, any specified individual, entity, or organization.

In responding to a 314(a) request, an entity should be prepared to provide, where available:

- The name of such individual, entity, or organization
- The relevant account number(s)
- Any social security number, tax payer identification number, passport number, date of birth, address, or other similar identifying information provided by the individual, entity, or organization when each such account was opened or each such transaction was conducted
- When the account(s) was (were) established
- The date(s) and type(s) of transaction(s)[51]

(i) Recordkeeping

As noted earlier, and consistent with export controls and OFAC economic sanctions regulations discussed in prior chapters, records covered by the AML program also should be retained for at least five years from the cessation of the relevant underlying contract, business relationship, or transaction.

(j) Sample Industry-Specific Red Flags

In general, an AML program will train personnel to identify risks typical to money laundering and terrorist financing—and specific to the particular industry sector. The FFIEC and other sources provide a number of money-laundering and terrorist financing red flags that financial institutions should look out for. For example, the following are considered potentially suspicious red flags: customers who use unusual or suspicious identification documents that cannot be readily verified; customers with multiple aliases or spelling variations; contact information is not valid (i.e., business or home telephone number is disconnected); the customer's background differs from what is typical for others similarly situated in the industry; and a customer engages in transactions atypical for the industry.[52]

(i) Red Flags for Broker-Dealers

Like other covered industries, broker-dealers are expected to maintain tailored AML programs after risk assessments. In March 2012, the SEC published its AML Source Tool for Broker Dealers, which cites, in relevant part, the National Association of Security Dealers (NASD) Notice 02-21 to Members: Anti-Money Laundering Guidance. Within the Guidance is a list of some customer-focused risks particular to the industry sector. These red flags include but are not limited to instances where the customer:

- Is unusually concerned with the company's compliance policies and procedures (including AML reporting requirements);
- Wishes to engage in transactions that appear to lack legitimate business purpose;
- Provides false information (i.e., false source of income, false identifying information);
- Refuses to disclose source of funds or party on whose behalf he is acting;

- Has a higher-risk profile (i.e., is subject of press reports relating to possible illegal activity);
- Appears to lack general knowledge of his purported industry sector;
- Makes frequent deposits of cash or cash equivalents or appears to structure deposits, keeping each under $10,000;
- Account appears to have unusual or unexplained activity;
- For no apparent business reason, maintains multiple accounts with a large number of inter-account or third-party transfers;
- For no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" stocks, and bearer bonds, which, although legitimate, have been used in connection with fraudulent schemes and money-laundering activity.[53]

(ii) Red Flags for Casinos and Card Clubs

FinCEN has identified risks specific to this industry, some of which are identified as follows:

- Two or more customers each purchase chips with currency in amounts under $10,000, engage in little gaming, and then cash out the chips for a casino check.
- A customer pays off a large credit debt (i.e., over $20,000) over a short period of time through a series of currency transactions, none of which exceeds $10,000.
- A customer receives a payout in excess of $10,000 and asks for currency of less than $10,000 and asks for the remainder in chips. The customer then redeems the chips in an amount less than the currency transaction report requires.
- A customer bets both sides of a game or event.
- A customer requests casino checks below the $3,000 threshold to be made out to a third party.[54]

(iii) Red Flags for Money Services Businesses (MSBs)

As with other industry sector's FinCEN publishes guidance specific to MSBs.[55] Identified "red flags" for MSB include but are not limited to the following:

- **Customer.** Customer uses false identification; two/more customers use similar identification; customer alters transaction upon learning that he/she must show identification; customer uses multiple variations of his name; two or more customers working together to break one transaction into two or more transactions in order to evade the BSA reporting or recordkeeping requirement; customer uses two or more locations or cashiers in the same day in order to break one transaction into smaller transactions and evade the BSA reporting or recordkeeping requirement; customer offers bribes or tips.[56]
- **Services.** Currency exchanges just under $1,000; cash sales of money orders or traveler's checks of just under $3,000.[57]

(iv) Red Flags for Insurers

Insurers offering covered products are subject to the BSA Regulations and must maintain an AML program. Covered products include (1) permanent life insurance policies (other than group life); (2) annuity contracts (other than group annuity contracts); or (3) any other insurance product with features of cash value or investment. FinCEN has identified the following customer-based insurance-specific red flags:

- Purchase of an insurance product inconsistent with customer's needs
- Unusual payment methods
- Early termination of a product
- Payment by or to, or transfer of benefit to, an apparently unrelated third party
- Insured who shows little concern for investment performance but is focused on early termination features
- Reluctance to provide identifying information or provides fictitious identifiers
- Purposeful obscuring of source of funds
- Insured who borrows the maximum amount available soon after purchasing the product
- Insured purchases insurance products using a single, large premium payment, particularly when payment is made through unusual methods such as currency or currency equivalents
- Policies are purchased that allow for the transfer of beneficial ownership interests without the knowledge and consent of the

insurance issuer
- An insured is known to purchase several insurance products and uses the proceeds from an early policy surrender to purchase other financial assets[58]

(v) Red Flags for Lawyers

While lawyers are not covered under the BSA regulations, FATF has identified lawyers as a DNFBPs under the purview of AML laws and regulations. There also have been attempts to include lawyers within the BSA. For example, in 2002, Fin-CEN published the Advanced Notice of Proposed Rule Making that would mandate AML programs for persons involved in certain real estate transactions.[59] Because of the response, the final rule has yet to be published. The American Bar Association (ABA) has resisted formal inclusion of lawyers under the BSA or the BSA regulations and has, instead, promoted a risk-based approach to protecting the sector from money laundering and terrorist financing threats. As a result, on April 23, 2010, the ABA Task Force on Gatekeeper Regulation and the Profession, together with other ABA committees and organizations, drafted the Voluntary Good Practices Guidance for Lawyers to Detect and Combat Money Laundering and Terrorist Financing.[60] Activities covered by the guidance (i.e., the high-risk services) include those five categories identified in the FATF's RBA Guidance for Legal Professionals (October 23, 2008). To keep in (voluntary) line with the FATF Guidance, the ABA's Good Practices identify the covered activities, including (1) buying and selling of real estate; (2) managing a client's money; (3) management of a bank, savings, or security account; (4) organization of contributions for the creation, operation, or management of companies; and (5) creation, operation, or management of legal persons or arrangements, and buying and selling of business entities.[61] In order to be more useful than the broad FATF guidance, the ABA Good Practices modifies the FATF "red flags" (following) by adding practice pointers. The FATF risk factors include the following:

- Geographic risk: transactions involving sanctioned countries; countries ranked as higher risk for corruption
- Client risk: PEPs (i.e., individuals who are or have been entrusted with prominent functions in a foreign country); clients conducting

their relationship or requesting services in unusual or unconventional circumstances; where the structure or nature of the client entity or relationship makes it difficult to identify the true beneficial owner or controlling interests; clients that are cash intensive businesses; charities and other not-for-profits that are not subject to monitoring or supervision; clients using financial intermediaries, financial institutions, or legal professionals not subject to AML laws and regulations; clients convicted of proceeds-generating crimes; clients with no address or multiple addresses without a legitimate reason; clients who change their settlement or execution instructions without appropriate explanation.

- Service risk: transactions where the lawyers touch the client's money; services designed to improperly conceal beneficial ownership from relevant legal authorities; services requested by a client for which the client knows the lawyer does not have the expertise; transfers of real estate between parties in an accelerated fashion (and lacking legitimate business reasons for the expedited treatment); payments for services from unassociated or unknown third parties; transactions where it is apparent to the lawyer that there is inadequate consideration (and there appears no legitimate business reason for the lower consideration); administration of estates where the decedent was known to be a person convicted of proceeds generating crimes.[62]

Of course, as the ABA Voluntary Good Practices emphasizes, the risk factors will vary depending on size of the firm, types of clients, sophistication in addressing money-laundering threats, nature of the client relationship, among others.[63] The expectation unless and until lawyers fall under the BSA Regulations is that we will take tailored and risk-based steps to mitigate exposure to identified money-laundering and terrorist financing threats.

(vi) Risks for Charities

Charities—particularly those operating in disaster zones—can be higher risk for exposure to money laundering and terrorist financing. Soon after September 11, 2001, recognizing this exposure, the Department of the Treasury, working with representatives from the charities sector, drafted the Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-

Based Charities.[64] These Best Practices were not well received by some in the charities sector. In response, the Treasury Guidelines Working Group of Charitable Sector Organizations and Advisors drafted the Principles of International Charity (March 2005).[65] While neither document identifies "red flags" specific to the charitable sector, the Treasury document reminds U.S.-based charities that, as U.S. Persons, they are subject to the economic sanctions regulations, discussed in prior chapters, administered by OFAC. OFAC has also issued guidance and Frequently Asked Questions regarding humanitarian assistance to Iran and Syria, private relief efforts in Somalia, and more.

(k) Regulation of Virtual Currency

In 2011, FinCEN issued a final rule amending regulations relating to MSBs to provide that money transmission covers the acceptance and transmission of value that substitutes for currency (e.g., virtual currency). In 2013, FinCEN issued guidance to persons administering, exchanging, or using virtual currencies. Since then, FinCEN has issued a number of administrative rulings regarding its regulation of the virtual currency space,[66] including an Advisory on Illicit Activity Involving Convertible Virtual Currency on May 9, 2019, highlighting prominent typologies and red flags associated with convertible virtual currency transmission.[67] Many newly formed Fintech companies are engaging in, or are considering engaging in, virtual currency transmission or conversion (e.g., virtual currency administrators, companies offering or engaging in "initial coin offerings," etc.). Importantly, this activity may bring them under the purview of the BSA as money transmitters.

4.4 Representative Enforcement Actions

BSA-regulated financial institutions are subject to substantial civil penalties for willful violations of BSA obligations (the greater of $25,000 or the amount involved in the relevant transaction, if any, up to $100,000).[68] They also are subject to criminal penalties for willful violations (including fines of up to $250,000).[69]

In 2018, FinCEN imposed two enforcement actions and updated one enforcement action from 2017, which is down from the five FinCEN enforcement actions in 2017. Of the seven enforcement actions in the past two years, three were against depository institutions, two were against MSBs, one was against a casino, and one was against a securities and futures firm.

FinCEN Actions in 2019 and 2020

- In January 2019, FinCEN assessed a $35,350 civil monetary penalty against an individual, Eric Powers, for failing to register as an MSB, failing to establish and implement an effective written AML program, failing to detect and adequately report suspicious transactions, and failing to report currency transactions.[70] Within a two-year timespan, Mr. Powers conducted over 1,700 transactions as a money transmitter peer-to-peer exchanger of bitcoin, purchasing and selling bitcoin to and from others.[71] FinCEN clarified that Mr. Powers was not simply a "user" of virtual currency, but was a peer-to-peer exchanger, and thus was subject to the purview of the BSA.[72]
- In January 2020, FinCEN assessed a $25,000 civil monetary penalty against Michael LaFontaine, former Chief Operational Risk officer of U.S. Bank National Association (U.S. Bank) for failing to ensure the bank's compliance division was appropriately staffed to meet regulatory expectations, among other things.[73] Mr. LaFontaine was put on notice a number of times by bank employees that the existing AML monitoring program was inadequate because caps were set to limit the number of alerts, and that the staff was "stretched dangerously thin." U.S. Bank had been previously warned that placing caps on monitoring programs based on the size of its staff and available resources could result in a potential enforcement action. Nonetheless, Mr. LaFontaine did not heed warnings, and was penalized in response.
- In October 2020, FinCEN assessed a $60 million civil monetary penalty against Larry Dean Harmon, the founder and operator of bitcoin "mixers" Helix and Coin Ninja LLC (Coin Ninja), for failing to register as an MSB, failing to implement and maintain an effective AML program, and failing to report suspicious activities.[74] Mr.

> Harmon operated Helix from 2014 to 2017 and Coin Ninja from 2017 to 2020 without registering either "mixer" or "tumbler" as an MSB.[75] Through Helix, Mr. Harmon engaged in more than $311 million worth of transactions in virtual currencies and allowed customers to anonymously pay for services in the "darknet," including for items such as drugs, guns, and child pornography. Coin Ninja operated in the same manner as Helix. Mr. Harmon not only disregarded his obligations under the BSA, but FinCEN's investigation further revealed that he made efforts to circumvent the BSA's requirements.

---

1. *See* U.S. Treasury, Financial Crimes Enforcement Network, *History of Anti-Money Laundering Laws*, https://www.fincen.gov/history-anti-money-laundering-laws (last visited Dec. 6, 2022); U.S. Treasury, Financial Crimes Enforcement Network, *What Is Money Laundering?*, https://www.fincen.gov/what-money-laundering (last visited Dec. 6, 2022).

2. Within Treasury, in addition to FinCEN, the Office of Foreign Assets Control, the Office of the Comptroller of the Currency, and the Internal Revenue Service maintain AML duties. Other regulators including the Federal Reserve, Federal Deposit Insurance Corporation, Securities and Exchange Commission, the National Credit Union Administration and the Commodities Futures Trading Commission carry AML duties. There are also self-regulated organizations that impose AML requirements, including the Financial Industry Regulatory Authority, the New York Mercantile Exchange, and the National Futures Association.

3. The Bank Secrecy Act of 1970 is also called the Currency and Foreign Transactions Reporting Act, Pub. L. No. 91-5081 (1970) and is codified at 12 USC 1829b, 12 USC 1951-19600, 31 USC 5311-5314, and 5316-5336; *see also* 31 CFR Chapter X.

4. *See* FINANCIAL ACTION TASK FORCE, FATF 40 RECOMMENDATIONS (Oct. 2003), http://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

5. *Id.*

6. *See* FINANCIAL ACTION TASK FORCE, FATF IX SPECIAL RECOMMENDATIONS (Oct. 2001), https://www.fatf-gafi.org/content/dam/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf.coredownload.pdf.

7. Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, European Commission, Finland, France, Germany, Greece, Gulf Co-operation Council, Hong Kong, Iceland, India, Ireland, Israel, Italy, Japan, Kingdom of the Netherlands, Luxembourg, Malaysia, Mexico, New Zealand, Norway, Portugal, Republic of Korea, Russian Federation, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the United States. *See* Financial Actions Task Force, *FATF Members and Observers*, https://fatfgaf.org/about/membersandobservers/index.html (last visited Dec. 5, 2022).

8. *See* Financial Action Task Force, *Who We Are*, https://www.fatf-gafi.org/en/the-fatf/who-we-are.html (last visited Dec. 5, 2022).

9. Note, however, on December 11, 2020, as part of the National Defense Authorization Act for Fiscal Year 2021 (NDAA), the U.S. Senate passed the Corporate Transparency Act (CTA) requiring certain corporations and limited liability companies to file a report with FinCEN identifying its beneficial owners. *See* HR 6395, govinfo.gov/content/pkg/BILLS-116hr6395enr. More recently, on September 30, 2022, FinCEN published a highly anticipated rule (the "Final UBO Rule" or the "Final Rule") that implements the beneficial ownership information reporting requirements of the CTA. This rule, which goes into effect in January 2024 does not replace the CDD rule. FinCEN has noted that there are differences between the rules that will be addressed over the coming year.

10. *See* Financial Action Task Force, *Mutual Evaluation of the United States* (Dec. 2016), http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

11. *See* Financial Action Task Force, *Anti-money laundering and Counter-Terrorist Financing Measures: United States, 3rd Enhanced Follow-up Report and Technical Compliance Re-Rating*, (Mar. 2020), https://www.fatf-gafi.org/content/dam/fatf/documents/reports/fur/Follow-Up-Report-United-States-March-2020.pdf.

12. *See* Financial Action Task Force, *Risk-Based Approach Publications*, http://www.fatf-gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc(fatf_releasedate) (last visited Dec. 5, 2022).

13. *See* FinCEN, *What We Do*, https://www.fincen.gov/what-we-do (last visited Dec. 5, 2022); *see also* FinCEN, *The Egmont Group of Financial Intelligence Units*, https://www.fincen.gov/resources/international/egmont-group-financial-intelligence-units (last visited Dec. 5, 2022).

14. *See id*.

15. Wolfsberg Group, *Wolfsberg Group Home Page*, https://www.wolfsberg-principles.com/ (last visited Dec. 5, 2022).

16. Wolfsberg Group, *Wolfsberg Anti-Money Laundering Principles on Private Banking* (2012), https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/10.%20Wolfsberg-Private-Banking-Prinicples-May-2012.pdf.

17. Wolfsberg Group, *Statement on the Suppression of Financing of Terrorism*, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/16.%20Wolfsberg_Statement_on_the_Suppression_of_the_Financing_of_Terrorism_%282002%29.pdf (last visited Dec. 5, 2022).

18. Wolfsberg Group, *Wolfsberg Anti-Money Laundering Principles for Correspondent Banking*, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/8.%20Wolfsberg-Correspondent-Banking-Principles-2014.pdf (last visited Dec. 5, 2022).

19. Wolfsberg Group, *International Due Diligence Repository*, https://www.wolfsberg-principles.com/wolfsberg-group-standards.

20. Please note that the FAQs published in February 2018 were updated in 2020: Wolfsberg Group, *Frequently Asked Questions "FAQs" on Correspondent Banking Questionnaire v2.0* (Apr. 2020), https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%20CBDDQ%20FCCQ%20FAQ%20v2%20Final%20160420_0.pdf

21. *See, e.g.*, Wolfsberg Group, *Wolfsberg Group Standards*, https://www.wolfsberg-principles.com/wolfsberg-group-standards (last accessed Dec. 5, 2022).

22. The Panel of Experts was established pursuant to Security Council Resolution 1874 (2009).

23. The Report is available at https://www.securitycouncilreport.org/dprk-north-korea/.

24. Within Treasury, in addition to FinCEN, the Office of Foreign Assets Control, the Office of the Comptroller of the Currency, and the Internal Revenue Service maintain AML duties. Other regulators, including the Federal Reserve, Federal Deposit Insurance Corporation, Securities and Exchange Commission, the National Credit Union Administration, and the Commodities Futures Trading Commission, carry AML duties. There are also self-regulated organizations that impose AML requirements, including the Financial Industry Regulatory Authority, the New York Mercantile Exchange, and the National Futures Association.

25. *See* Bank Secrecy Act, 31 C.F.R. ch. X (2012) (formerly 31 C.F.R. 103).

26. On September 14, 2020, FinCEN issued a final rule that removed the AML program exemption for banks that lack a federal functional regulator, including, but not limited to, private banks, nonfederally insured credit unions, and certain trust companies. *See* 85 Fed. Reg. 57129, https://www.federalregister.gov/documents/2020/09/15/2020-20325/financial-crimes-enforcement-network-customer-identification-programs-anti-money-laundering-programs. As of December 2020,

BSA financial institutions exempt from the requirement to have an AML program (provided they are not otherwise required to establish an AML program) include (1) pawnbrokers; (2) travel agencies; (3) telegraph companies; (4) seller of vehicles, including automobiles, airplanes, and boats; (5) person involved in real estate closings and settlements; (6) private bankers; (7) commodity pool operators; (8) commodity trading advisors; and (9) investment companies. *See* 31 C.F.R. § 1010.205(b).

27. Money Laundering Control Act, Pub. L. No. 99-570, § 1352, 100 Stat. 3207 (codified as amended at 18 U.S.C. §§ 1956–1957 (2009)).

28. USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, §§ 402–403, 405, 120 Stat. 192 (2006).

29. The U.S. Department of Justice, *Money Laundering and Asset Recovery Section (MLARS)*, https://www.justice.gov/criminal-mlars (last visited Dec. 5, 2022).

30. *Id.*

31. *Id.*

32. *See, e. g.*, 31 C.F.R. § 1010.311 (requirement for financial institutions to file reports of transactions in currency of more than $10,000); § 1010.320 (requirement to report suspicious transactions); § 1010.410(a) (requirement to record cross-border transfers of more than $10,000).

33. *See* 31 C.F.R. § 1020.220.

34. *See id*. §§ 1020.210, 1010.205.

35. FFIEC, *Bank Secrecy Act/Anti-Money Laundering Examination Manual*, https://www.ffiec.gov/press/PDF/FFIEC%20BSA-AML%20Exam%20Manual.pdf (last visited Dec. 5, 2022).

36. *See id.*

37. *See id*.

38. *See* FFIEC, *BSA/AML Exam Manual* (Apr. 2020 Update), https://www.ffiec.gov/press/PDF/FFIEC%20BSA-AML%20Exam%20Manual.pdf

39. *See, e.g.*, *In the Matter of Pinnacle Capital Markets, LLC*, The United States of America Department of the Treasury Financial Crimes Enforcement Network, Number 2010-4, https://www.fincen.gov/sites/default/files/enforcement_action/2020-05-21/Final%20Pinnacle%20Assessment%20for%20FinCEN%20Internet%20with%20Date%20and%20No%20Signature.pdf, stating "As defined by the U.S. Department of State in the INCSR report, higher risk customers include those that may be involved in money-laundering activities, or are connected to jurisdictions that are especially susceptible to money laundering."

40. *See* Transparency Int'l, *Corruption Perception Index 2019*, https://www.transparency.org/en/cpi/2019 (last visited Dec. 5, 2022).

41. *See* U.S. Dep't of Treasury, *Sanctions Programs and Country Information*, https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information (last visited Dec. 5, 2022).

42. *See* FinCEN, *Special Measures for Jurisdictions, Financial Institutions, or Int'l Transactions of Primary Money Laundering Concern*, https://www.fincen.gov/resources/statutes-and-regulations/311-and-9714-special-measures (last visited Dec. 5, 2022).

43. *See* U.S. Dep't of State, State Sponsors of Terrorism, https://www.state.gov/state-sponsors-of-terrorism/ (last visited Dec. 5, 2022).

44. 22 C.F.R. §126.1–126.18.

45. *See* BSA/AML Exam Manual, *supra* note 35.

46. The debate over how and whether to track beneficial ownership of privately held entities operating in the United States dates back to at least 2006 when the issue was the topic of hearings and investigations spearheaded by the Senate Permanent Subcommittee on Investigations. Proponents of sharing such information with the government (at the state level) largely cite the concern that anonymity allows bad actors to use shell companies to engage in certain illicit activity,

including money laundering, terrorist financing, and other financial crimes. On the other hand, sharing such information presents real concerns from a privacy standpoint and cost perspective, and efforts to impose legislation had been met with strong opposition from various groups, including the American Bar Association. Of primary note was the expense of maintaining databases that would be adequately protected from cyberattacks—an equally valid concern in 2022. On December 11, 2020, as part of the 2021 NDAA, the U.S. Senate passed the Corporate Transparency Act requiring certain corporations and limited liability companies to file a report with FinCEN identifying its beneficial owners. *See* H.R. 6395, 116th Cong. (2019-2020) *available at*: https://www.govinfo.gov/content/pkg/BILLS-116hr6395ih/pdf/BILLS-116hr6395ih.pdf (last visited Dec. 5, 2022). On December 7, 2021, FinCEN published a proposed rule to implement the beneficial ownership information reporting requirements as set forth in section 6403(a) of the CTA and to welcome public comment. FinCEN considered public comment and on September 30, 2022, FinCEN issued the Final UBO Rule, which is a significant update to AML laws and regulations.

47. 31 U.S.C.A. § 5336(3)(A)(i)–(ii).

48. Beneficial Ownership Information Access and Safeguards, and Use of FinCEN Identifiers for Entities, 87 Fed. Reg. 77404 (proposed Dec. 16, 2022) (to be codified at 31 C.F.R. pt. 1010) *available at*: https://www.govinfo.gov/content/pkg/FR-2022-12-16/pdf/2022-27031.pdf

49. For example, the SEC Enforcement Manual (Nov. 28, 2017) identifies four broad measures for a company's cooperation: (1) self-policing prior to the discovery of the misconduct, including establishing effective compliance procedures and an appropriate tone at the top; (2) self-reporting of misconduct when it is discovered, including conducting a thorough review of the nature, extent, origins, and consequences of the misconduct, and promptly, completely, and effectively disclosing the misconduct to the public, to regulatory agencies, and to self-regulatory organizations; (3) remediation, including dismissing or appropriately disciplining wrongdoers, modifying and improving internal controls and procedures to prevent recurrence of the misconduct, and appropriately compensating those adversely affected; and (4) cooperation with law enforcement authorities, including providing the Commission staff with all information relevant to the underlying violations and company's remedial efforts. *See* 6.1.2. Framework for Evaluating Cooperation by Companies, https://www.sec.gov/divisions/enforce/enforcementmanual.pdf. FINRA rule 4530(b) requires a member firm to report to FINRA within 30 days after the firm has concluded, or reasonably should have concluded, on its own that the firm or an associated person of the firm has violated any securities-, insurance-, commodities-, financial- or investment-related laws, rules, regulations, or standards of conduct of any domestic or foreign regulatory body or self-regulatory organization. *See* FINRA Regulatory Notice 11-06, http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p122888.pdf.

50. *See, e.g.*, 31 C.F.R. § 1010.520(b) (2012).

51. *Id*.

52. Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual, Appendix F—Money Laundering and Terrorist Financing "Red Flags,"* https://bsaaml.ffiec.gov/manual/Appendices/07.

53. *See* Nat'l Ass'n Sec. Dealers, *Special NASD Notice to Members 02-21 at 10-11* (Apr. 2002), http://www.sec.gov/about/offices/ocie/aml2007/nasd-ntm-02-21.pdf.

54. Financial Crimes Enforcement Network, *Guidance: Recognizing Suspicious Activity—Red Flags for Casinos and Card Clubs* (Aug. 1, 2008), https://www.fincen.gov/resources/statutes-regulations/guidance/recognizing-suspicious-activity-red-flags-casinos-and-card.

55. FINANCIAL CRIMES ENFORCEMENT NETWORK, A MONEY SERVICES BUSINESS GUIDE, https://www.fincen.gov/sites/default/files/shared/prevention_guide.pdf (last visited Dec. 5, 2022).

56. *Id*.

57. *Id*.

58. *See, e.g.*, *supra* note 52.

59. *See* Anti-Money Laundering Program Requirements for Persons Involved in Real Estate Closings and Settlements, 68 Fed. Reg. 17,569 (Apr. 10, 2003) (FinCEN announcing an Advanced Notice of Proposed Rule Making).

60. VOLUNTARY GOOD PRACTICES for LAWYERS to DETECT and COMBAT MONEY LAUNDERing and TERRORIST FINANCING (adopted Aug. 9–10, 2010), https://www.americanbar.org/content/dam/aba/publications/criminaljustice/voluntary_good_practices_guidance.pdf.

61. The FATF Legal Professional Guidance identifies these five categories as activity that should be regulated under domestic anti-money laundering laws and regulations. *See* FINANCIAL ACTION TASK FORCE, RBA GUIDANCE for LEGAL PROFESSIONALS (OCT. 23, 2008), https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Legal-Professionals.pdf.

62. VOLUNTARY GOOD PRACTICES, *supra* note 60, sec. 4.

63. *Id*.

64. U.S. DEP'T of the TREASURY, ANTI-TERRORIST FINANCING GUIDELINES: VOLUNTARY BEST PRACTICES for U.S.-BASED CHARITIES, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/protecting-charities-intro.aspx (last visited Dec. 5, 2022).

65. TREASURY GUIDELINES WORKING GROUP of CHARITABLE SECTOR ORGANIZATIONS and ADVISORS, PRINCIPLES of INTERNATIONAL CHARITY (Mar. 2005), https://home.treasury.gov/system/files/136/archive-documents/tocc.pdf. The charitable sector responded with its own guidelines, available at https://www.icnl.org/wp-content/uploads/Transnational_principles.pdf.

66. Financial Crimes Enforcement Network, Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block.

67. FinCEN, *Advisory on Illicit Activity Involving Convertible Virtual Currency* (May 9, 2019), https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf

68. *See* 31 U.S.C. § 5321(a)(1).

69. *See id*. § 5322.

70. *In the Matter of Eric Powers*, United States Department of the Treasury Financial Crimes Enforcement Network, Number 2019-01, https://www.fincen.gov/sites/default/files/enforcement_action/2020-05-21/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19.pdf.

71. *See id.*

72. *See id.*

73. *In the Matter of Michael LaFontaine*, United States Department of the Treasury Financial Crimes Enforcement Network, Number 2020-01, https://www.fincen.gov/sites/default/files/enforcement_action/2020-05-21/Michael%20LaFontaine-Assessment-02.26.20_508.pdf.

74. *In the Matter of Larry Dean Harmon d/b/a Helix*, United States Department of the Treasury Financial Crimes Enforcement Network, Number 2020-2, https://www.fincen.gov/sites/default/files/enforcement_action/2020-10-19/HarmonHelix%20Assessment%20and%20SoF_508_101920.pdf.

75. Cryptocurrency mixers or tumblers allow customers to send bitcoin to designated recipients in a manner designed to conceal the source or owner of the bitcoin by mixing digital assets to make them more difficult to trace back to the original holder.

5

U.S. Antiboycott Measures

Michael L. Burton[1]

5.1 Overview

Since the 1970s, the United States has maintained two anti-boycott laws that prohibit or penalize U.S. companies and individuals from supporting or participating in boycotts of countries friendly to the United States. As part of the Export Control Reform Act of 2018, the Anti-boycott Act of 2018 updated the statutory basis for the primary set of U.S. anti-boycott regulations.[2] Although these laws are drafted without reference to any particular boycott, their principal target is the Arab League's long-standing economic boycott of Israel. These laws impose far-reaching restrictions on boycott-related actions, agreements, and even the furnishing of information. Penalties for violations can include civil and criminal fines, imprisonment, and the loss of tax credits or export privileges.

What is regulated. Virtually any transaction within U.S. jurisdiction (see the following) involving official foreign government boycotts or restrictive trade practices that the United States does not support.

Where to find the regulations. The U.S. anti-boycott regulations and statutes are contained primarily in (1) Part 760 of chapter 15 of the Code of Federal Regulations; (2) section 999 of the Internal Revenue Code, and (3) Department of the Treasury Guidelines: Boycott Provisions (section 999) of the Internal Revenue Code (IRC).

Who is the regulator. The U.S. anti-boycott laws are administered by the U.S. Department of Commerce, Bureau of Industry and Security (BIS), Office of Anti-boycott Compliance (OAC) and the U.S. Treasury Department, Internal Revenue Service (IRS).

How to get a license/file a report. No licenses are granted under the anti-boycott regulations. Persons receiving boycott requests, however, are required to report them to OAC and the IRS. For OAC, reports of receipts of boycott requests must be filed quarterly on form BIS 621-P for single transactions or BIS 6051P for multiple transactions received during the same calendar quarter (see https://www.bis.doc.gov/index.php/enforcement/oac?id=300). Reports under section 999 of the IRC are filed with annual tax returns on IRS form 5713. This form is available from local IRS offices.

Key website. https://www.bis.doc.gov/index.php/enforcement/oac. See also Section 5.8 later in the chapter.

This chapter is intended to provide the reader with an introduction to and basic understanding of the U.S. anti-boycott laws. These laws are complicated and sometimes counterintuitive. Whether a particular action is permissible can often turn on very subtle variations in language and circumstances. For this reason, it is critical that you consult the regulations for answers to specific anti-boycott issues. The information is not intended nor may it be relied upon as legal advice.

5.2 What Are the U.S. Anti-Boycott Laws?

Although the United States recognizes the sovereign right of each country not to trade with countries to which they are hostile, the U.S. anti-boycott laws are designed to (1) monitor foreign boycotts the United States does not support, and (2) to prohibit or penalize individuals and entities subject to U.S. law from acting in furtherance of more trade distortive forms of boycott activity.

Understanding the differences among primary, secondary, and tertiary boycotts is helpful in conceptualizing the framework of U.S. anti-boycott law.

- Primary Boycott = boycotting country prohibits imports from or exports to the boycotted country.
- Secondary Boycott = boycotting country prohibits companies contributing to the economic or military strength of the boycotted country from trading with the boycotting country.
- Tertiary Boycott = boycotting country prohibits business with companies that conduct business with individuals or entities identified as having a business relationship with the boycotted country (e.g., blacklisted persons).

Generally speaking, the U.S. anti-boycott laws do not prohibit or penalize persons subject to U.S. law from acting in furtherance of primary boycotts. Participation in secondary or tertiary boycotts, however, is prohibited and penalized. Further, unless an exception applies, the U.S. government requires reporting of the request, regardless of the level of the boycott. Thus, even if not prohibited or penalized, primary boycott requests often need to be reported. The U.S. government has an interest in monitoring the boycott and reviewing how persons subject to U.S. law handle those requests, even in those situations where the requested action is within the boycotting country's rights under international law.

While understanding the level of boycott at issue is useful as a conceptual framework, exceptions abound. Whether a specific boycott-related request is prohibited/penalized or reportable depends on (1) the facts of a particular transaction; (2) the transaction being subject to U.S. jurisdiction; (3) which of the two (or both) U.S. anti-boycott laws is implicated; and (4) a detailed review of the relevant regulations, which are replete with sometimes idiosyncratic examples reflecting U.S. foreign policy considerations as applied to a range of actual business scenarios.

(a) The Commerce Department's Anti-boycott Law

As noted earlier, the more sweeping of the two U.S. anti-boycott laws is maintained by the Commerce Department in Part 760 of the U.S. Export Administration Regulations (EAR).[3] The substantive prohibitions and the reporting requirements of the Commerce Department's anti-boycott law apply if (1) the person taking the action in question is a "U.S. person"; and (2) the activity is in the "interstate or foreign commerce of the United States."[4] Jurisdiction will be discussed further later in the chapter.

Under the Commerce Department's anti-boycott provision, the following types of actions are prohibited:[5]

- Refusing to do business with boycotted countries, companies of a boycotted country, nationals of a boycotted country, or "blacklisted" companies
- Furnishing boycott-related information—including information about one's business relationships with a boycotted country, companies of a boycotted country, nationals of a boycotted country, or "blacklisted" companies
- Discriminating against any U.S. person on the basis of race, religion, sex, or national origin
- Evasion of the anti-boycott provisions of the EAR

The Commerce Department's anti-boycott provisions also require U.S. companies each calendar quarter to report the receipt of requests to take any action that has the effect of furthering or supporting the boycott. Boycott-related requests—whether oral or written—are generally reportable regardless of whether the requested action is prohibited or permitted, ***and regardless of whether the recipient complies with the request***. Certain exceptions to the reporting requirements, however, are provided for in the EAR.

The Office of Anti-boycott Compliance (OAC) within the Bureau of Industry and Security of the U.S. Department of Commerce administers and enforces Part 760 of the EAR. OAC is aggressive in its enforcement actions and investigations. Violations of the Commerce Department's anti-boycott regulations are subject to the full range of civil and criminal penalties available under the EAR, including fines, imprisonment, and the denial of export privileges. (See discussion *infra* at 5.6(a)).

(b) The Treasury Department's Anti-boycott Law

In addition to the EAR's anti-boycott rules, under section 999(a)(1) of the Internal Revenue Code, any person (or any member of a "controlled group" including such person) must file reports with the Internal Revenue Service (IRS), if that person has operations in, or relating to, (1) a boycott listed country, or the government, a company, or a national of such country, or (2) any other country (or the government, a company, or a national of such

country) if such person knows or has reason to know that participation in a boycott is a condition of conducting operations in such other country.[6] The U.S. Treasury Department publishes a list of countries believed to be engaged in boycotts and other restrictive trade practices on a periodic basis.[7] The IRS requires persons with operations "in or relating to such" countries to file a boycott report on Form 5713, listing such operations.

Under section 999(a)(2), a taxpayer also must report whether it or any member of a "controlled group" of which it (or such foreign corporation) is a member has participated in or cooperated with an international boycott, or has been requested to participate in or cooperate with an international boycott.[8] When entered into or requested, *as a condition of doing business with a boycotting country or its companies or nationals*, the following types of agreements are subject to tax penalties and IRS reporting requirements:[9]

- Agreements to refuse to do business directly or indirectly within a country that is the object of the boycott or with the boycotted country's government, companies or nationals
- Agreements to refuse to do business with U.S. persons who do business in a boycotted country or with its government, companies, or nationals
- Agreements to refuse to do business with companies owned or managed by individuals of a particular race, religion, or nationality
- Agreements to refrain from employing persons of a particular race, religion, or nationality
- Agreements to refuse to ship or insure products on carriers owned or operated by persons who do not participate in or cooperate with the boycott.

In analyzing anti-boycott issues under section 999, it is important to determine whether (1) there is some agreement or request to agree; and (2) that agreement is a condition of doing business with a boycotting country, its companies, or its nationals. Both elements must be met. That being said, agreements may be inferred from course of conduct and the circumstances surrounding a given transaction.

Like the Commerce Department's anti-boycott regulations, reports are required even if the requested agreement is never reached. Unlike the EAR, however, Form 5713 is filed with the IRS on an annual basis rather than quarterly.

Taxpayers who willfully fail to make a required boycott report may be fined up to $25,000 or imprisoned for not more than one year, or both.[10] Taxpayers that agree to impermissible boycott-related actions may be subject to significant tax penalties by being prohibited from claiming favorable tax treatment with respect to boycott-related income. Depending on a taxpayers operations and corporate structure, the tax consequences can be wide reaching.

(c) Distinctions between the Two U.S. Anti-boycott Laws

It is important to note that the Part 760 of the EAR and section 999 of the IRC contain a number of significant distinctions relating to jurisdiction as well as substance. The U.S. government has provided an unofficial summary of the key distinctions in a chart available at https://www.bis.doc.gov/index.php/documents/enforcement/404-distinctions/file. See Appendix G. It is important to note that subtle variations in the wording of boycott-related requests can result in different legal outcomes between section 760 of the EAR and section 999 of the IRC, requiring case-by-case review.

5.3 To Whom Do the U.S. Anti-Boycott Laws Apply?

(a) Part 760

The EAR's anti-boycott provisions apply to all "U.S. persons" acting in the interstate or foreign commerce of the United States. According to OAC, "The term 'U.S. person' includes all individuals, corporations and unincorporated associations resident in the United States, including the permanent domestic affiliates of foreign concerns. U.S. persons also include U.S. citizens abroad (except when they reside abroad and are employed by non-U.S. persons) and the 'controlled in fact' foreign affiliates of domestic concerns."

Section 760.1(c) of the EAR sets forth a multifactor test for determining when a foreign subsidiary or affiliate of a U.S. domestic concern is deemed to be owned or controlled in fact by the U.S. domestic concern. Subject to rebuttal by competent evidence, a foreign affiliate is presumed to be controlled in fact, and thus a U.S. person, when:

1. The domestic concern beneficially owns or controls (whether directly or indirectly) more than 50 percent of the outstanding voting securities of the foreign subsidiary or affiliate;
2. The domestic concern beneficially owns or controls (whether directly or indirectly) 25 percent or more of the voting securities of the foreign subsidiary or affiliate, if no other person owns or controls (whether directly or indirectly) an equal or larger percentage;
3. The foreign subsidiary or affiliate is operated by the domestic concern pursuant to the provisions of an exclusive management contract;
4. A majority of the members of the board of directors of the foreign subsidiary or affiliate are also members of the comparable governing body of the domestic concern;
5. The domestic concern has authority to appoint the majority of the members of the board of directors of the foreign subsidiary or affiliate; or
6. The domestic concern has authority to appoint the chief operating officer of the foreign subsidiary or affiliate.

To satisfy the jurisdictional requirements of Part 760 of the EAR, the transaction not only must involve a U.S. person but also be within the interstate or foreign commerce of the United States. “U.S. commerce” is broadly defined to include activities relating to the sale, purchase, or transfer of goods or services (including information) within the United States or between the United States and a foreign country are subject to the EAR. Such activities include importing, exporting, financing, freight forwarding, and shipping.

(b) Section 999

The penalty provisions of the Treasury Department’s anti-boycott regulations—which are self-imposed by taxpayers when they file their returns—apply only to U.S. taxpayers. In comparison, the reporting requirements of section 999 are broader and cover not only U.S. taxpayers and U.S. shareholders, but also a range of foreign affiliated companies in which the U.S. ownership can be as little as 10 percent.

The reporting requirements of section 999 require U.S. taxpayers (i.e., any legal or natural person filing a U.S. tax return) to report their own activities as well as the activities of all members of their "controlled groups."[11] The term "controlled group" is defined under the Internal Revenue Code to include parent-subsidiary controlled groups in which a common parent holds a majority interest in one or more "chains of corporations connected through stock ownership."[12] Because the reporting requirements extend to all members of a U.S. taxpayer's controlled groups, U.S. taxpayers are required to report on the activities of their foreign parent companies as well as the activities of other foreign companies in which their foreign parent holds a majority interest. This reporting requirement as to foreign entities applies even if the U.S. taxpayer does not itself hold a direct interest in the foreign company and the foreign company is not involved in U.S. commerce.[13]

The extraterritorial impact of these reporting requirements is mitigated somewhat by a limited waiver under which U.S. taxpayers are excused from having to report the activities of foreign parents and sister corporations that are not otherwise required to report. To qualify for this waiver, however, the U.S. taxpayer must forfeit all deferral, DISC, and foreign tax credit benefits related to operations in countries with unsanctioned boycotts, or show that the benefits derive from operations "separate and identifiable" from boycott-related activities.[14] Even where this waiver is possible, the U.S. taxpayer must still report (1) its own activities, (2) the activities of all other U.S. members of its controlled groups, and (3) the activities of all foreign corporations in which it is a U.S. shareholder (as defined herein).[15]

In addition to the "controlled group" reporting requirements of section 999, U.S. shareholders are required to report the boycott-related activities of all foreign companies in which they hold the requisite ownership interest. U.S. shareholders are defined with respect to foreign companies as U.S. persons owning at least 10 percent of a foreign company's total combined voting stock.[16] Recognizing that minority shareholders may not be able to secure information from foreign companies, this shareholder-based reporting requirement applies only to information that is "reasonably available" to the U.S. shareholder.[17]

5.4 What Are the Reporting Requirements?

Section 760.5 of the EAR requires U.S. persons (including U.S. companies and, in many cases, their foreign subsidiaries) to report the receipt of requests to take any action that has the effect of furthering or supporting the boycott on a *quarterly* basis. The specific deadline for reporting depends on whether the request was received in the United States or abroad. If the request was received in the United States, the report must be filed within one month following the end of the quarter during which the request was received. If received outside the United States, the U.S. person receiving the request has one additional month to report.

- Boycott request received in United States = report within **1 month** following the end of the quarter during which request received
- Boycott request received aboard = report within **2 months** following the end of the quarter during which request received

Boycott-related requests—whether oral or written—are generally reportable regardless of whether the requested action is prohibited or permitted and regardless of whether the recipient complies with the request. A number of exceptions to the reporting requirements are set forth in the EAR. These exceptions are listed here along with additional guidance regarding the reporting requirements of section 760.5 of the EAR.

Section 999 of the Internal Revenue Code requires U.S. taxpayers and members of their "controlled groups" to report any operations in or with any of the following boycotting countries: Iraq, Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, and Yemen. In addition, such taxpayers must report the receipt of any request to enter into an impermissible boycott-related agreement, as defined later, whether or not the request came from one of the aforementioned countries. Reports are filed in conjunction with the filing of the taxpayer's annual return.

5.5 How Do I Report a Boycott-Related Request?

EAR reports are filed quarterly. Form BIS 621-P is used for single requests and Form BIS 6051-P is used for multiple requests. The forms are available from the Department of Commerce's Office of Anti-boycott Compliance (OAC). To obtain these forms, call OAC's Report Processing Unit at (202) 482-2448 or mail a request to U.S. Department of Commerce, BIS/Office of

Anti-boycott Compliance, Room 6098, Washington, D.C., 20230. Reports to OAC may now be filed electronically as well. Additional information on the mechanics of reporting can be found on the OAC website at: https://www.bis.doc.gov/index.php/enforcement/oac?id=300.

Reports pursuant to section 999 are filed annually with a U.S. taxpayer's tax return using IRS Form 5713. This form is available at any IRS office or at www.irs.gov.

5.6 Penalties and Enforcement

(a) Commerce Department

Violations of the EAR's anti-boycott provisions are subject to the full range of civil and criminal penalties available under the EAR, including fines, imprisonment, and denial of export privileges. Criminal violations of the EAR can result in penalties of up to $1 million and/or imprisonment for up to 20 years. The maximum civil penalty for an anti-boycott violation under the EAR is $300,000 per violation (plus inflation adjustments) or twice the amount of the transaction that is the basis of the violation with respect to which the penalty is imposed, whichever is greater. OAC's penalties typically do not reach these levels on a per count basis, but they are significant and compliance breakdowns often involve numerous counts. Multiple violations may be asserted based on a single document. For example, each separate response to an eight-point boycott questionnaire may be treated as a separate count of furnishing boycott-related information.

The Commerce Department recognizes a formal voluntary self-disclosure procedure to self-report anti-boycott violations, which is detailed in section 764.8 of the EAR. Though similar to section 764.5 of the EAR, the anti-boycott voluntary disclosure procedure is distinct from the process for disclosing violations of the export control provisions of the EAR. Section 764.8(a) sets forth BIS's policy on voluntary disclosures and provides, "BIS strongly encourages disclosure to the Office of Anti-boycott Compliance (OAC) if you believe that you may have violated the anti-boycott provisions. Voluntary self-disclosures are a mitigating factor with respect to any enforcement action that OAC might take."

Per section 764.8(b)(3) of the EAR, voluntary self-disclosures to OAC are valid only if OAC receives the disclosure "before it commences an investigation or inquiry in connection with the same or substantially similar information it received from another source." OAC's receipt of a mandatory boycott report pursuant to section 760.5 is treated as information from another source. Fortunately, violations revealed during requests for advice from OAC are not treated as information from another source, but the revelation is not treated as a voluntary self-disclosure. Thus, OAC provides an opportunity to make a voluntary self-disclosure and potentially obtain mitigation after receiving advice from OAC that the conduct in question violated Part 760 of the EAR.

Additional information regarding OAC's penalty practices may be found in Supplement No. 2 to Part 766 of the EAR: Guidance on Charging and Penalty Determinations in Settlement of Administrative Enforcement Cases Involving Antiboycott Matters. It is important to note that OAC operates under separate penalty guidelines than BIS's Office of Export Enforcement. On October 27, 2022, OAC updated and strengthened this Guidance in four significant ways: (1) enhanced penalties (within the existing statutory maximums); (b) reprioritized violation categories to reflect the relative seriousness of offenses; (c) required admissions of misconduct in settlements; and (4) a renewed focus on controlled foreign subsidiaries of U.S. companies.

OAC regularly pursues enforcement actions against companies and individuals for violations of Part 760 of the EAR. Recent cases illustrating the types of violations and range of penalties include the following:

- **Mediterranean Shipping Company (USA) Inc. (Chicago).** January 13, 2021. OAC assessed a civil penalty of $81,000 to settle allegations that, on eight occasions, the company furnished information about business relationships with boycott countries or blacklisted persons involving bills of lading, certificates, and sea waybills involving exports to Libya. MSC-USA also allegedly failed to report boycott-related requests to OAC on two occasions. Significantly, the company also was required to complete an internal audit of its antiboycott compliance program and provide a report to OAC.
- **Kuwait Airways Corporation.** January 14, 2020. OAC assessed a civil penalty of $700,000 to settle allegations that, on 14 occasions,

Kuwait Airways Corporation engaged in prohibited refusals to do business with nationals or residents of a boycotted country when it denied carriage of Israeli passport holders on flights from New York to the United Kingdom.

- **Zurn Industries, LLC.** May 20, 2019. OAC assessed a $54,000 civil penalty against Zurn Industries for 27 failures to report requests to engage in restrictive trade practices or foreign boycotts. The alleged violations related to vessel eligibility certificates received in connection with exports to the United Arab Emirates and Qatar.
- **Citibank, NA.** August 2, 2018. OAC assessed a $60,000 civil penalty against Citibank, NA to settle allegations of 20 furnishings of information about business relationships with boycotted countries or blacklisted persons. The alleged violations arose in connection with related to vessel eligibility certifications in letters of credit from banks in Kuwait, Lebanon, Oman, Qatar, and the United Arab Emirates.
- **Pelco Inc.** February 17, 2017. A civil penalty of $162,000 was levied against Pelco Inc. to settle 32 counts of refusal to do business and 34 failures to report the receipt of boycott-related requests. The alleged violations related to negative declarations of origin, agreements that products would conform “Israeli boycott & UAE regulations,” and agreements that the consignment would not contain any goods manufactured by blacklisted persons.
- **Coty Middle East FZCO (UAE).** September 29, 2016. *Coty Middle East FZCO* agreed to pay $238,000 to settle allegations of 70 counts of furnishing prohibited boycott-related information on 70 occasions furnished to persons in Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Pakistan, Qatar, Saudi Arabia, Syria, UAE, and Yemen, information concerning its business relationships with or in a boycotted country—specifically negative certifications of origin.
- **GM Daewoo Auto & Technology Company (Korea).** January 8, 2010. GMDAT (a wholly owned Korean subsidiary of General Motors Company) paid $88,500 to settle allegations that on 59 occasions it furnished prohibited boycott-related information to entities in Libya in connection with the shipment of Korean origin goods to Libya involving the sale and transfer of title to those goods

through a U.S. affiliate of General Motors for resale through an Egyptian distributor to Libya.

- **Baxter International Inc.** March 1993. This is the leading criminal anti-boycott case, though it also resulted in a significant civil penalty and limited export denial order. Two affiliates of Baxter and one of its officers agreed to pay a total of $6,060,600 in civil penalties to settle allegations of violating Part 760 of the EAR in connection with their efforts to be removed from the Arab League's blacklist. Baxter, its affiliates, subsidiaries, and employees were also subject to a limited denial order prohibiting them from "entering into, negotiating, or extending contracts to export goods or technology to Syria and Saudi Arabia from March 1993 until March 1995." Baxter also pled guilty to a single felony count and was fined $500,000. A corporate whistleblower brought the matter to the U.S. government's attention.

Information regarding other Commerce Department anti-boycott enforcement actions may be found at https://efoia.bis.doc.gov/index.php/electronic-foia/index-of-documents/7-electronic-foia/226-alleged-antiboycott-vilations and https://efoia.bis.doc.gov/index.php/electronic-foia/index-of-documents/7-electronic-foia/225-warning-letters.

(b) Treasury Department

Impermissible agreements to participate in or cooperate with an unsanctioned foreign boycott may result in the denial of certain tax privileges, including denial of foreign tax credits; denial of foreign tax deferral; and denial of the benefits of ETI, FSC, and FSC with respect to boycott-related income. Taxpayers are required to calculate these penalties in connection with the preparation of their tax returns. Detailed guidance on the rather complicated tax penalty calculation methodology is provided in the Department of the Treasury Guidelines: Boycott Provisions (section 999) of the Internal Revenue Code. Willful failures to make required reports are punishable by criminal fines up to $25,000 or imprisonment up to one year, or both. The Internal Revenue Service enforces civil violations of section 999, and the U.S. Department of Justice prosecutes criminal tax law violations.

Section 999 does not provide for a voluntary disclosure process distinct from disclosing other errors on a tax return. Because boycott-related agreements penalized under section 999 are enforced through the imposition of tax penalties, which are treated as confidential taxpayer information, civil cases are not reported.

5.7 Where Can I Find the List of "Boycotting" Countries?

The Department of Treasury publishes this list on a periodic basis. The current list is comprised of Iraq, Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, and Yemen. This list is not exhaustive, and it is not uncommon to receive boycott-related requests from countries not on the official list, such as Bangladesh, Pakistan, Indonesia, Malaysia, and Nigeria. A list of countries with a reputation for generating boycott-related requests is provided in Appendix E.

The Commerce Department does not publish any list of boycotting countries, and the requirements of Part 760 of the EAR do not depend on a list.

5.8 Legal Resources / Where Can I Find Additional Information?

The primary legal resources for U.S. anti-boycott compliance are as follows:

- Part 760 of the U.S. Export Administration Regulations (15 C.F.R. section 760)
- Parts 762 (Record keeping), 764 (Enforcement and Protective Measures) & 766 (Administrative Enforcement Proceedings) of the EAR
- Section 999 of the Internal Revenue Code (26 U.S.C. section 999)
- Department of the Treasury Guidelines: Boycott Provisions (section 999) of the Internal Revenue Code[18]

Additional information and guidance may be found on the OAC website at https://www.bis.doc.gov/index.php/enforcement/oac.

OAC provides general or transaction specific guidance on anti-boycott compliance to the public. They may be contacted at:

U.S. Department of Commerce
BIS/Office of Anti-boycott Compliance, Room 6098

1401 Constitution Ave, NW

Washington, DC 20230
Anti-boycott Advice Line: (202) 482-2381

The Treasury Department will provide copies of Form 5713, the current list of boycotting countries, section 999, and copies of all guidelines. Please contact:

Office of the General Counsel
Room 2015 – Main Treasury Building
Department of the Treasury

1500 Pennsylvania Avenue, NW

Washington, D.C. 20220

The responsible Treasury Department lawyer can also be reached at (202) 622-1945 for informal, nonbinding answers to questions concerning the section 999 of the Internal Revenue Code.

5.9 Compliance Tools and Analytical Framework

Because anti-boycott law is so dependent upon specific examples and complicated concepts, the explanation of which would make for a rather long chapter indeed, Appendixes A though G elaborate upon this chapter and provide some useful compliance tools to the practitioner. It bears reiterating, however, that there is no substitute for carefully analyzing a given set of facts under Part 760 of the EAR and section 999 of the IRC (including the Treasury Department Guidelines). Though dense and somewhat tedious, these sources should answer the lion's share of questions you and your clients are likely to confront. In closing, I offer the following framework to help guide your analysis.

Framework for Analyzing Boycott-Related Requests

Commerce	Treasury
1. Is there a U.S. person (or an owned or controlled foreign affiliate of a U.S. person)?	Is there a U.S. taxpayer or member of its controlled group?
2. Is the transaction within the interstate or foreign commerce of the United States?	Does the taxpayer claim U.S. foreign tax credits or other tax benefits enumerated in section 999?
3. Does the request fall within a prohibition?	Did the taxpayer agree to or receive a request to enter into a boycott agreement?
4. Does the request meet an exception to the prohibitions?	Does the agreement meet an exception to section 999, or has it been deemed not penalized under the Treasury Department Section 999 Guidelines?
5. Even if not prohibited, is the request reportable?	All penalizable agreements or requests to agree are also reportable.
6. Does the request meet an exception to the reporting requirements?	

---

1. Michael L. Burton is a partner at the law firm of Jacobson Burton Kelley PLLC in Washington, DC.

2. On August 13, 2018, the President signed into law the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which includes the Export Control Reform Act of 2018, 50 U.S.C. §§ 4801–4852 (ECRA). The Anti-Boycott Act of 2018 is a subpart of ECRA. While section 1766 of ECRA repeals numerous provisions of the Export Administration Act (EAA), section 1768 of ECRA provides that all rules and regulations that were made or issued under the EAA, including as continued in effect pursuant to the International Emergency Economic Powers Act, and were in effect as of ECRA's date of enactment (August 13, 2018), shall continue in effect according to their terms until modified, superseded, set aside, or revoked through action undertaken pursuant to the authority provided under ECRA.

3. 15 C.F.R. §§ 760.1–760.5.

4. *Id*. § 760.1. "U.S. persons" include owned-or-controlled foreign affiliates of U.S. companies.

5. *Id*. § 760.2.

6. I.R.C. § 999(a)(1).

7. Currently, the countries listed by the Treasury Department as boycotting countries for tax purposes are Iraq, Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, and Yemen. List of Countries Requiring Cooperation with an International Boycott, 87 Fed. Reg. 145 (Jan. 3, 2022). However, "operations" in other countries or with any company or government may be implicated if participation in a boycott is an express or implied condition of conducting such operations.

8. I.R.C. § 999(a)(2).

9. All listed at *id*. § 999(b)(3).

10. I.R.C. § 999(f).

11. *Id*. § 999(a).

12. *Id*. § 999 (defining "controlled group" by referencing I.R.C. § 993(a), which in turn references with modifications I.R.C. § 1563(a)); *see also* Income Tax Regs. § 1.1563-1 (1998).

13. *See, e.g*., Prop. Treas. Reg. § 1.999-1 (guideline A-18), 43 Fed. Reg. 3454, 3457 (1978).

14. *See, e.g*., Prop. Treas. Reg. § 1.999-1 (guideline A-14A), 43 Fed. Reg. 3454, 3456 (1978).

15. *Id*.

16. I.R.C. § 951(b).

17. *See* Prop. Treas. Reg. § 1.999-1 (guideline A-18), 43 Fed. Reg. 3454, 3457 (1978).

18. The 999 Guidelines may be found in the Federal Register (look under the topic "Treasury" on the following dates: 1/25/78, for the original guidelines; 11/19/79, for supplemental guidelines; and 4/26/84, for additional guidelines). *See also* https://www.bis.doc.gov/index.php/documents/enforcement/398-federal-register-43fr3454a-1/file, https://www.bis.doc.gov/index.php/documents/enforcement/399-federal-register-44fr66272g-1/file, https://www.bis.doc.gov/index.php/documents/enforcement/823-treas-guidelines-pt-3/file, https://www.bis.doc.gov/index.php/documents/enforcement/824-treas-guidelines-pt-4/file. The guidelines are also available in compilations such as CCH, Standard Federal Tax Reports, in the notes under I.R.C. section 999 and BNA (Tax Management) Portfolio 345.

Appendix A to Chapter 5

Commerce Department Anti-Boycott Compliance Summary

Prohibitions

The prohibitions outlined herein apply to all U.S. persons and companies, and controlled-in-fact subsidiaries of U.S. companies. A controlled-in-fact subsidiary includes a foreign company that is more than 50 percent owned by a U.S. company or that is otherwise “managed” or controlled by the U.S. company. Accordingly, all foreign affiliates “controlled” by a U.S. company should be treated as a “U.S. person.”
set

Refusals to Do Business

- No U.S. person (including foreign affiliates) may refuse, knowingly agree to refuse, require any other person to refuse, or knowingly agree to require any other person to refuse to do business with or in a boycotted country, with any business organized under the laws of a boycotted country, or with any national or resident of a boycotted country when such refusal is pursuant to an agreement with the boycotting country, a requirement of the boycotting country, or a request from the boycotting country.
- This includes not only specific express refusals but also refusals implied by a pattern of conduct.
- Use of either a boycott-based “blacklist” or “whitelist” constitutes a refusal to do business.
- An agreement to comply generally with the laws of the boycotting country with which it is doing business or an agreement that local laws of the boycotting country shall apply is not, in and of itself, a refusal to do business.
- An agreement is not a prerequisite to a violation since the prohibitions extend to actions taken pursuant not only to agreements but also to requirements of and requests on behalf of a boycotting country.

Discriminatory Actions

No U.S. person (including foreign affiliates) may:

1. Refuse to employ or otherwise discriminate against any other U.S. person on the basis of race, religion, sex, or national origin.
2. Discriminate against any corporation or organization that is a U.S. person on the basis of race, religion, sex, or national origin of any owner, director, or employee.
3. Knowingly agree to take any of the actions just described in 1 or 2 or require another to take such action.

The prohibition applies whether the action is taken by a U.S. person on its own or in response to a request from or requirement of a boycotting country.

Furnishing Information about Race, Religion, Sex, or National Origin

1. No U.S. person (including foreign affiliates) may furnish or agree to furnish information about the race, religion, sex, or national origin of any U.S. person or any owner, director, or employee of any corporation or organization that is a U.S. person.
2. The prohibition shall apply whether the information is specifically requested or is offered voluntarily and whether it is stated in the affirmative or negative.
3. Information in the form of code words or symbols that could identify a U.S. person's race, religion, sex, or national origin comes within the prohibition.

Furnishing Information about Business Relationships

1. No U.S. person may furnish or knowingly agree to furnish information concerning past, present, or proposed business relationships:
    a. With or in a boycotted country;
    b. With any business concern organized under the laws of a boycotted country;
    c. With any national or resident of a boycotted country; or
    d. With any other person believed to be restricted from having any business relationship with or in a boycotted country.

2. The prohibition applies whether the information pertains to a sale, purchase, or supply transaction; a legal or commercial representation; shipping or other transportation transaction; insurance, investment, or any other type of business transaction/relationship.

   It also applies whether the information is directly or indirectly requested or is furnished on the initiative of the U.S. person.
3. It does not apply to the furnishing of normal business information in a commercial context such as would normally be found in documents available to the public (annual reports, catalogs, etc.).
4. If the information is of a type that is generally sought for a legitimate business purpose, it may be furnished even if the information could be used or, without the knowledge of the person supplying it, is intended to be used for boycott purposes.

   However, no information may be furnished in response to a boycott request, even if the information is otherwise publicly available.

Information Concerning Association with Charitable and Fraternal Organizations

No U.S. person (including foreign affiliates) may furnish or knowingly agree to furnish information whether any person is a member of, has contributed to, or is otherwise associated with any charitable or fraternal organization that supports a boycotted country.

Letters of Credit

1. No U.S. person (including foreign affiliates) may implement a letter of credit that contains a condition or requirement regarding compliance with boycott laws or terms that are prohibited; nor shall any U.S. person be obligated to pay such a letter of credit.
2. “Implementing” a letter of credit includes:
   a. Issuing or opening a letter of credit at the request of a customer;
   b. Honoring it by accepting it as being a valid instrument of credit;
   c. Paying, under a letter of credit, a draft or other demand for payment by the beneficiary;
   d. Confirming it; or

e. Negotiating it by voluntarily purchasing a draft from a beneficiary and presenting such draft for reimbursement to the issuer.

3. The prohibition applies only when the transaction to which the letter of credit applies is in U.S. commerce and the beneficiary is a U.S. person.
4. A letter of credit implemented in the United States by a U.S. person located in the United States will be presumed to apply to a transaction in U.S. commerce and to be in favor of a U.S. beneficiary where it specifies a U.S. address for the beneficiary.
5. Letters of credit implemented outside the United States will be presumed to apply to a transaction in U.S. commerce and to be in favor of a U.S. beneficiary where the letter of credit:
    a. Specifies a U.S. address for the beneficiary, and
    b. Calls for documents indicating shipment from the U.S. or otherwise indicating that the goods are of U.S. origin.

Exceptions to the Prohibitions

Import Requirements of a Boycotting Country

In supplying goods or services to a boycotting country, a U.S. person may comply or agree to comply with requirements of the boycotting country that prohibit the import of:

a. Goods or services from the boycotted country, or
b. Goods produced or services provided by any business concern organized under the laws of the boycotted country or by any of its nationals or residents.

Shipment of Goods to a Boycotting Country

1. In shipping goods to a boycotting country, a U.S. person may comply with the requirements of that country that prohibit the shipment of goods:
    a. On a carrier of the boycotted country, or
    b. By a route other than that prescribed by the boycotting country.
2. The exception applies whether the purchaser:

a. Explicitly states the shipment should not pass through a port of the boycotted country, or
b. Affirmatively describes a route of shipment that does not include a port in the boycotted country.

Import and Shipping Document Requirements of a Boycotting Country

1. In shipping goods to a boycotting country, a U.S. person may comply with that country's shipping document requirements with respect to:
   a. Country of origin of goods;
   b. Name of carrier;
   c. Route of shipment;
   d. Name of the supplier of the shipment; or
   e. Name of provider of other services.
2. All such information must be stated in positive terms except for information with respect to the names of carriers or routes of shipment (e.g., the goods are 100 percent U.S. origin).

Compliance with Unilateral and Specific Selection

1. A U.S. person may comply in the normal course of business with the unilateral and specific selection by a boycotting country (national or resident) of carriers, insurers, suppliers of services to be performed in boycotting country, or specific goods provided that:
   a. With respect to services, it is necessary and customary that a not insignificant part of the services be performed within the boycotting country, and
   b. With respect to goods, the items are identifiable as to their source or origin at the time they enter the boycotting country by
      (1) uniqueness of design or appearance, or
      (2) trademark or other identification normally on the items themselves, including their packaging.
2. The exception pertains to what is permissible for a U.S. person who is the recipient of a unilateral and specific selection of goods or services to be furnished by a third person.
   a. It does not pertain to whether the act of making such a selection is permitted.

b. It does not pertain to the U.S. person who is to supply his own goods or services. A U.S. person may fill an order himself even if he is selected by the buyer on a boycott basis.

3. A “specific” selection is one which is stated in the affirmative and which specifies a particular supplier of goods or services.
4. A “unilateral” selection is one in which the discretion in making the selection is exercised by the boycotting country buyer without the assistance of the U.S. person. However, provision of pre-selection/pre-award services such as providing lists of qualified suppliers, subcontractors, or bidders does not alone destroy the unilateral character of a selection, provided such services are not boycott based. Furthermore, provision of such services must be customary practice in non-boycotting countries.
5. A U.S. person may be considered a bona fide resident of a boycotting country depending upon the following factors:
   a. Physical presence in country;
   b. Whether residence is needed for legitimate business reasons;
   c. Continuity and intent to maintain residency;
   d. Whether person is registered to do business or is incorporated in the country or whether he has a valid work visa.
6. If a U.S. person receives from another person located in the United States what may be a unilateral selection by a customer in a boycotting country, and has reason to know that the selection is made for boycott reasons, he has a duty to inquire of the transmitting person to determine who actually made the selection.
7. No U.S. person may comply with any unilateral selection if he has reason to know that the purpose of the selection is to effect discrimination against any U.S. person on the basis of race, religion, sex, or national origin.

Compliance with a Boycotting Country’s Requirements Regarding Shipment of Exports

1. A U.S. person may comply with the export requirements of a boycotting country with respect to shipments or transshipments of exports to:
   a. A boycotted country;

   b. Any business concern organized under the laws of a boycotted country;
   c. Any national or resident of a boycotted country.
2. This exception applies to restrictions a boycotting country may place on direct exports to a boycotted country, on indirect exports, or on exports to residents, nationals, or business concerns of a boycotted country, including those located in third countries.
3. Exception also applies to any restriction on the route of export shipments when reasonably related to preventing them from coming into contact with or under the jurisdiction of the boycotted country.

Compliance with Employment Requirements of a Boycotting Country

1. A U.S. person may comply with immigration, passport, visa, or employment requirements of a boycotting country and with requests for information to ascertain whether such individual meets requirements for employment *provided* he furnish information only about himself and not about any other U.S. person.
2. A U.S. person may not furnish information about its employees or executives but may allow any individual to respond on his own.
3. A U.S. person may proceed with a project in a boycotting country even if other employees or prospective participants are denied entry for boycott reasons; however, no employees/participants may be selected in advance in a manner designed to comply with a boycott.

Compliance with Local Law

1. A U.S. person who is a bona fide resident of a foreign country may comply with local law with respect to his activities exclusively within the foreign country as well as with local import laws.
2. Local laws may derive from statutes, regulations, directives, or other official sources having the effect of law in the host country; exception is not available for presumed policies or understandings unless reflected in official sources.
3. Activities exclusively within the host country include:
   a. Entering into contracts that provide that local law governs;
   b. Employing residents of the host country;

c. Retaining local contractors to perform work within the host country;
d. Furnishing information within the host country.

4. A U.S. person may comply with local import laws provided that:
   a. The items are for his own use or for use in performing contractual services within that country, and
   b. In the normal course of business, the items are identifiable as to their source or origin at the time of entry into foreign country by uniqueness of design/appearance or by trademark/trade name.
5. The bona fide residence of a U.S. company's employee in a foreign country does not confer such residence on the entire company. However, a bona fide resident may take action through an agent outside the country so long as the agent acts at the direction of the resident and not of his own discretion.
6. Goods are for the U.S. person's own use if:
   a. They are to be consumed by him;
   b. They are to remain in his possession to be used by him;
   c. They are to be used by him in performing contractual services for another;
   d. They are to be further manufactured or incorporated into another product for the use of another.
7. However, goods acquired to fill the order of another are not for the U.S. person's own use. Nor does the exception apply to the import of services.

Reporting Requirements

Scope

1. A U.S. person (including a foreign affiliate) who receives a request to take any action that effectively furthers or supports a restrictive trade practice or boycott imposed by a foreign country against a country friendly to the United States or against any U.S. person must report the request to the DOC, Office of Anti-boycott Compliance, and to the IRS. The request may be either written or oral and may include a request to furnish information or enter into or implement an agreement.

2. A request received by a U.S. person is reportable if the U.S. person knows or has reason to know that the request is to enforce, implement, or otherwise further an unsanctioned foreign boycott.
    a. A request such as a boycott questionnaire unrelated to a particular transaction is reportable when the U.S. person has or anticipates a business relationship with or in a boycotting country involving the sale, purchase, or transfer of goods or services in interstate or foreign commerce of the United States.
    b. However, an unsolicited invitation to bid containing a boycott request is not a reportable request where the U.S. person does not respond to the invitation or other proposal.
3. The following specific requests are *not* reportable:
    a. To refrain from shipping goods on a carrier flying the flag of a particular country or which is owned or chartered by a particular country.
    b. To supply a positive certification as to country of origin of goods.
    c. To supply a positive certification as to name of supplier or manufacturer of goods or provider of services.
    d. To comply with laws of another country except where the request expressly requires compliance with boycott laws.
    e. To supply information about oneself or family member for immigration, visa, or employment purposes.
    f. To supply certification indicating destination of exports.
    g. To supply certificate by the owner that a vessel, aircraft, truck, or other vehicle is eligible to enter a particular port or country pursuant to the laws of that port or country.
    h. To supply a certificate from an insurance company stating that it has a duly authorized agent or representative within a boycotting country.

Manner of Reporting

1. Each reportable request must be reported; however, if more than one document containing the same request is received as part of the same transaction, only the first request need be reported.
2. According to the Regulations, each U.S. person receiving a reportable request must report it; however, he may designate another

to report on his behalf. All requests received by any employee of the Company shall be reported through the Legal Department.

Examples of Prohibited and Reportable Requests or Requirements

In connection with the sale of goods or services covered by the anti-boycott regulations, the Company and its affiliates may not:

- Give or agree to give any information about the Company's business relationships with a boycotted country or with blacklisted persons, for example, "we have no business relations with Israel" or "the Company does not maintain an office or a branch in Israel."
- State that Company is not the mother company, sister company, subsidiary, or branch of a blacklisted company.
- Certify that "the Company is not a company boycotted by the Ministry of Customs and Imports, Israel Boycott Office, State of (boycotting country) and that it is not in any way affiliated to such company."
- Refuse to do business with a boycotted country or with a blacklisted person because of his or its relationship with the boycotted country, if done by agreement, requirement, or request from a boycotting country, for example, "the vessel (or insurance carrier) is not blacklisted."
- Agree to do business only with a person who is approved or "whitelisted" by a boycotting country.
- Give information as to the blacklist status of another person.
- State the origin of goods in negative terms, for example, "the goods covered by this invoice are not of Israeli origin, they contain no Israeli components, materials, or capital."
- Agree to comply with a provision of another country's law that expressly requires compliance with that country's boycott laws.
- Respond to a boycott questionnaire from a central boycott office with regard to a specific transaction or if you do business with a boycotting country or anticipate doing business with that country.
- Submit the Company's Annual Report if it is submitted in response to a boycott related request.
- Certify that goods will not be shipped on a vessel that is ineligible to enter boycotting country's waters.

- Certify that “the company is permitted to trade with Arab Countries.”
- Certify that “the goods” nor the packing bear a six-pointed star emblem.”

The preceding list of examples is not exhaustive; it is prudent to report any potential boycott-related requests to export compliance personnel or legal counsel for review.

Examples of Permitted and Non-Reportable Requests or Requirements

The following specific requests are not reportable. However, any requests not falling squarely within one of these areas should be submitted to export compliance personnel or legal counsel for review.

The Company and its affiliates may:

- Refrain from shipping goods on a carrier flying the flag of a boycotted country or which is registered or owned by a boycotted country.
- Supply positive certification as to country of origin of goods.
- Supply positive certification as to name of supplier or manufacturer of goods or provider of services.
- Comply with the laws of another country except where the request expressly requires compliance with boycott laws.
- Supply information about oneself or a family member for immigration, visa, or employment purposes.
- Supply certification indicating destination of exports.
- Supply a certificate by the owner that a vessel is eligible to enter a particular port or country pursuant to the laws of the port or country.
- Supply a certificate from an insurance company stating that it has a duly authorized agent or representative within a boycotting country.

Additionally, an unsolicited invitation to bid containing a boycott request is not reportable if the U.S. person does not respond to it.

However, all of the preceding requests must be stated in the positive, for example:

Reportable: Request for certification that the exported

(prohibited) goods are not of (boycotted country) manufacture.

Not Reportable: Request for certification that the exported

(not prohibited) goods are of U.S. manufacture.

Application to Foreign Affiliates of U.S. Companies

The anti-boycott rules apply to all "U.S. persons" who engage in "activities in U.S. Commerce." A U.S. person includes individuals; U.S. corporations; and "controlled-in-fact"[1] foreign branch offices, subsidiaries, and affiliates. All of the Company's foreign affiliates are "controlled-in-fact" affiliates. Thus, application of the boycott regulations depends upon whether the transaction constitutes an activity in U.S. Commerce.

Activities in U.S. Commerce

The law applies only to the interstate or foreign commerce of the United States. This has been defined very broadly and can include activities of "controlled in fact" branch offices, affiliates, or subsidiaries, no matter where located, of U.S. companies that deal with third parties located outside the U.S.

Activities of the Company's foreign affiliates which are U.S. persons are deemed to be "Activities in U.S. Commerce" if a transaction is between such subsidiary and a person or entity outside the United States involving goods (or services) acquired by the U.S. person subsidiary from a person or entity in the United States, under any of the following circumstances:

1. If the goods (or services) were acquired for the purpose of filling an order from a person outside the United States;
2. If goods (or services) were acquired for incorporation into, refining into, reprocessing into, or manufacture of another product for the purpose of filling an order from a person outside the United States; or
3. If the goods were acquired and ultimately used, without substantial alteration or modification, in filling an order from a person outside the United States (whether or not the goods were originally acquired for that purpose).

Goods and services are considered to be acquired for the purpose of filling an order with a person outside the United States when:

1. Goods are purchased from a U.S. source by the foreign subsidiary upon receipt of an order from the customer outside of the United

States, with the intention that those goods go to the customer;
2. Goods are purchased by the foreign subsidiary from a U.S. source in order to meet the needs of specified customers outside the United States pursuant to understandings—even though not for immediate delivery; or
3. Goods are purchased from a U.S. source by the foreign subsidiary based on anticipated needs of specified customers.

“Activities Outside United States Commerce”

1. A transaction between a Company foreign affiliate and a person outside the United States, not involving the purchase or sale of goods or services to or from a person in the United States, is not an activity in the United States Commerce.
2. It should be noted that even if goods are acquired by the affiliate from the U.S., such goods will not be considered “Activities in U.S. Commerce” *if* the following two conditions are met:
   (a) Such goods were acquired by the subsidiary without reference to a specific order from or transaction with a person outside the United States; and
   (b) Such goods were further substantially manufactured, incorporated into, refined into, or reprocessed into another product.

Final determination of whether the goods involved in a particular transaction are connected with “Activities in U.S. Commerce” should be made only after consultation with legal counsel and review of the regulations.

---

1. The definition of a controlled-in-fact subsidiary or affiliate is slightly different under DOC and IRS regulations. Under DOC regulations, U.S. companies include, but are not limited to, foreign affiliates where the U.S. company owns 50 percent or more of the foreign affiliate’s voting stock. Under IRS regulations, the ownership interest threshold is only 10 percent.

Appendix B to Chapter 5

Treasury Department Anti-Boycott Summary

Section 999 of the Internal Revenue Code requires U.S. taxpayers to report their operations in boycotting countries and penalizes taxpayers who *agree* to "participate in or cooperate with" an unsanctioned foreign boycott by denying them certain tax benefits. Reports are filed in conjunction with the filing of the taxpayer's annual return.

I. Reporting Requirements

A. Must report operations in or with boycotting countries included on list published by Treasury.
   1. "Operations" include any type of business transaction, regardless of whether it generates revenue.
   2. Treasury has identified the following as "boycotting" countries for purposes of section 999: Iraq, Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, and Yemen.
   3. In addition to these countries, boycott requests in connection with businesses in other countries may be reportable as well.

B. Must report any request to enter into any impermissible boycott-related agreement, as defined next in section II.

C. Must report receipt of requests to participate in or cooperate with the boycott, even if agreement not reached.

II. Impermissible Agreements

The following are impermissible agreements to "participate in or cooperate with" a boycott:

A. Agreements to refuse to do business in Israel, or with Israel, Israeli companies, or Israelis.
B. Agreements to refuse to do business with U.S. persons who do business in Israel, or with Israel, Israeli companies, or Israelis.
C. Agreements to refuse to do business with companies owned or managed by individuals of a particular race, religion, or nationality.
D. Agreements to select or retain corporate directors of a particular race, nationality, or religion.
E. Agreements to refrain from employing persons of a particular race, religion, or nationality.
F. Agreements to refuse to ship or insure products on carriers owned or operated by persons who do not participate in or cooperate with the boycott. But may agree that goods will not be shipped on an Israeli vessel.
G. Agreements that local laws, including boycott laws, will "apply" to a transaction are *not* penalized, but agreements to "comply" with local laws (with some exceptions) *are* penalized.

III. Exceptions

The following types of agreements are permissible under section 999:

A. Agreements to comply with prohibitions on the importation of Israeli goods into a boycotting country.
B. Agreements to comply with prohibitions on the export of boycotting country goods to Israel.

IV. Penalties

A. For participating in or cooperating with the boycott: denial of certain tax privileges, including denial of foreign tax credits; denial of foreign tax deferral; and denial of the benefits of DISC, FSC, and ETI with respect to boycott-related income.

B. For failure to make required reports: fines up to $25,000 or imprisonment up to one year, or both.

Appendix C to Chapter 5

U.S. Anti-Boycott Law Issue Spotting Summary

U.S. companies, taxpayers, and their foreign affiliates may be subject to U.S. anti-boycott laws, which prohibit the Company from engaging in, or agreeing to engage in, certain activities relating to unsanctioned non-U.S. boycotts, primarily the Arab League boycott of Israel.

You should review transactions for terms that could raise anti-boycott compliance issues. While it is permissible to comply with a limited subset of boycott-related contract terms and requests, *all such terms and requests (written or oral) should be reviewed by qualified legal counsel as soon as they are identified and before agreeing to the request*.

- Common Prohibitions. Actions prohibited under U.S. anti-boycott
- laws include the following: Refusing to do business with Israel, Israeli companies, or Israelis; in Israel; or with "blacklisted" companies.
  - Furnishing boycott-related information—including information about one's business relationships with Israel, Israeli companies, Israelis, or "blacklisted" companies.
  - Providing negative certificates of origin (e.g., product not from Israel) or vessel eligibility certificates (e.g., vessel not blacklisted).
  - Discriminating against any U.S. person on the basis of race, religion, sex, or national origin. Furnishing such information also may be prohibited.
  - Agreeing, orally or in writing, to do any of the preceding.

- Failing to report a reportable boycott-related request within the established legal timetables.

- Common Boycott Terms. Terms often used in boycott-related
- requests include the following: “Jewish,” “Hebrew,” “Israel,” “Israeli,” or “goods originating in a country boycotted by” a boycotting country.
  - “Boycott,” “boycotted,” “blacklist,” “black list,” “boycott list,” or “Israel Boycott Office.”
  - Certification that a vessel is “eligible to enter the ports” of a boycotting country.
  - Certification that an insurer is “permitted to do business” in a boycotting country.
  - Prohibition on the use of “six-pointed stars” on packaging.
  - Agreement to “comply with” or “abide by” the laws of a boycotting country, regardless of whether laws concerning the boycott of Israel are expressly mentioned. (In contrast, an acknowledgment that the laws of a boycotting country shall
  - “apply” is permissible.) Key Business Functions. Those business functions most likely to encounter boycott-related requests in
  - international business transactions include the following: Sales & Marketing / Trading—for example, tenders, RFQs, offers, contracts, oral requests.
  - Contracts Administration—for example, contract documents or general terms and conditions.
  - Shipping / Logistics / Scheduling related to vessels—for example, shipping documents, charter party agreements, and vessel eligibility certificates.
  - Credit / Treasury—for example, letters of credit or other financing documents.
  - Legal—for example, any of the above, agreements, or other legal documents.

Appendix D to Chapter 5

Countries That May Require Compliance with, Furthering of, or Support of an Unsanctioned Foreign Boycott The following chart lists a number of countries that support the boycott of Israel or other unsanctioned foreign boycotts and sometimes issue boycott-related requests. For this reason, you should be particularly alert to anti-boycott compliance issues when transacting business involving the following countries.

Algeria Bahrain Bangladesh People's Republic of China (boycotts Taiwan) India (boycotts Pakistan) Indonesia Iran

Iraq*

Kuwait*

Lebanon*

Libya*

Malaysia Mauritania Nigeria Oman
Pakistan (boycotts India and Israel) Qatar*

Saudi Arabia*

Somalia Sudan

Syria*
United Arab Emirates Yemen, Republic of *

Countries other than those just listed might impose a boycott that the United States does not support, in which case, any requests made or actions sought may be subject to the U.S. anti-boycott laws.

*****The U.S. Treasury Department has determined that these countries have official policies supporting an unsanctioned foreign boycott, which take the form of secondary or tertiary boycotts (i.e., boycott that prohibit trading with persons and entities that choose to do business with Israel as opposed to prohibitions against direct trading with Israel).

Appendix E to Chapter 5

Anti-Boycott “Savings Clause”

The use of a general anti-boycott “savings clause” along the lines set forth here can help prevent companies from inadvertently agreeing to a boycott-related request. The request may nonetheless be reportable.

> *“Notwithstanding any other provision of this Agreement, no Party shall take or be required to take any action inconsistent with or penalized under the laws of the United States or any applicable foreign jurisdiction**[**, including without limitation the anti-boycott laws administered by the U.S. Commerce and Treasury Departments**]**.”*

Appendix F to Chapter 5

U.S. Anti-Boycott Law Jurisdictional Summary

Directly covered by U.S. anti-boycott laws	**Companies incorporated or based in the U.S.**	**Foreign branches/ offices of U.S. companies**	**Foreign entities wholly or majority-owned by a U.S. person**	**Foreign entities minority-owned but effectively controlled by a U.S. person**	**Foreign entities not owned or controlled by a U.S. person; foreign nationals**	**U.S. persons (U.S.citizens and permanent residents)**	**Foreign national employees or agents of covered person or company**
Commerce	Yes	Yes	Yes, if transaction is in the "interstate or foreign commerce of the United States"	Yes, if transaction is in the "interstate or foreign commerce of the United States"	No	Yes, with limited exceptions for U.S. persons who are *bona fide* residents of a boycotting country	Actions can be imputed to the U.S. company
Treasury	Yes	Yes	Yes, if a member of taxpayer's "controlled group"	Yes, if a member of taxpayer's "controlled group"	Yes, if a member of taxpayer's "controlled group"	Yes, if a member of taxpayer's "controlled group"	Actions can be imputed to the U.S. taxpayer

Appendix G to Chapter 5

Comparison of Commerce and Treasury Anti-Boycott Laws & Regulations/Guidelines

(Note: This table is an illustrative summary and is not a substitute for statutory and regulatory provisions. Specific questions should be referred to the experts at the Departments of Commerce and Treasury.)

1. Authorities	**Commerce**	**Treasury**
Statutory provisions	Section 8 of the Export Administration Act of 1979, as amended, 50 U.S.C. app. §§ 2401—2420 (2000), International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–1707 (2000), the Anti-Boycott Act of 2018, Part II of the ECRA, Title XVII, Subtitle B of Pub. L. 115-232, 132 Stat. 2208, provides the current statutory basis for OAC's boycott-related administration and enforcement.	"Ribicoff Amendment" to the Tax Reform Act of 1976, adding § 999 to the Internal Revenue Code.
Regulatory provisions	Part 760 "Restrictive Trade Practices and Boycotts" of the Export Administration Regulations (15 C.F.R. Part 760) (2008)	Treasury Guidelines (TG)

2. Principal Features		
To whom applicable?	U.S. persons, including individuals who are U.S. residents and nationals, businesses, and "controlled in fact" foreign subsidiaries, with respect to activities in the interstate or foreign commerce of the U.S.	Any U.S. taxpayer or member of a controlled group which includes such taxpayer. Also includes U.S. shareholders of foreign companies. Not limited to activities in U.S. commerce.
Intent required?	Yes, for prohibitions. ("intent to comply with, further or support an unsanctioned foreign boycott")	No.
Form of implementation?	The Export Administration Regulations contain prohibitions, with certain limited exceptions.	Denial of certain tax benefits for boycott agreements.
Sanctions?	Criminal and civil penalties and/or denial of export privileges.	Denial of tax benefits such as foreign tax credit and foreign subsidiary deferral benefits. If the U.S. taxpayer has no such tax benefits, there is no sanction—but still has to report.
Reporting requests?	Required to report receipt of boycott-related requests on a quarterly basis on BIS Form 621-P.	On IRS Form 5713, required to report annually operations in, with, or related to boycotting countries and any boycott-related requests and agreements. Plus operations and requests of entire controlled group in, with, or related to boycotting countries.
	Reporting of requests on multiple transaction basis permitted on BIS Form 6051-P.	Reporting of operations required on a country-by-country basis. Boycott requests and agreements must also be reported.
	Reports publicly available.	Reports kept confidential as part of tax return.
	Failure to report can lead to imposition of sanctions (even if there is no violation of law's prohibitions).	Failure to report can subject taxpayer to fines and criminal proceedings.
3. Principal Differences in Treatment of Conduct		
a. "Vessel Eligibility"	Permitted if furnished	Can constitute boycott agreement

Certificates	[only] by owner, master, or charterer of the vessel [not an agent]; exporter may request and pass on such a certificate. No restrictions on such certificates for shipments to Saudi Arabia since the Saudi government does not consider the requirement to be boycott-related under its laws. Not reportable.	which results in denial of certain tax benefits unless certificate is requested by Saudi Arabia, which has explained that it applies only to maritime matters such as the condition and safety standards of the vessel.
b. Local Law Clauses in Contractual Documents:		
• Agreement to comply generally with laws and regulations of a boycotting country –	Permitted	Penalized
• Agreement that laws of a boycotting country shall apply –	Permitted	Not penalized
• Agreement to comply with boycott laws of a boycotting country –	Prohibited	Penalized
• Agreement that boycott laws of a boycotting country shall apply –	Prohibited	Not penalized
c. Furnishing Information	Furnishing and/or agreeing to furnish certain boycott-related information prohibited.	Not penalized, as § 999 penalizes agreements to refrain from doing business, not furnishing information. However, an agreement to furnish boycott-related information at a later date will be penalized.

Please note that this table highlights certain key distinctions between the two sets of anti-boycott laws but should not be relied upon as a substitute for reviewing Part 760 of the EAR and the Treasury Department's Section 999 Guidelines.

6

Handling Violations

Wendy Wysong, Ali Burney, Hena Schommer, Nicholas Turner, and Anthony Pan[1]

6.1 Overview

As the U.S. government's use of civil monetary penalties to punish corporate defendants has grown, so, too, has its use of criminal penalties in cases involving willful violations, accompanied by the possibility of heavy fines, asset forfeiture, and imprisonment of responsible individuals. Equally significant are the collateral consequences that can attach to violations, including restrictions on, or suspension or denial of, a company's export privileges—a threat that overhangs negotiations with the government in these cases—or imposition of a costly compliance monitorship.

The manner in which a company addresses a potential violation is, in many ways, as important to the outcome as the seriousness of the underlying conduct. A company needs to investigate potential violations quickly and thoroughly, keeping in mind that a key determinant of the level of liability will be whether the violation was willful. A finding of willfulness may very well transform an administrative enforcement matter into a criminal case, particularly when the matter involves a U.S. national security law. Thus, a company needs to conduct its internal investigation with an eye to the possibility of either a civil or criminal resolution, or both.

This chapter provides an overview of the numerous U.S. agencies that are responsible for the enforcement of economic sanctions and export controls; the steps involved in conducting a thorough internal investigation of potential violations; how voluntary self-disclosures (VSD) should be utilized and the process for submitting them; strategies to consider when crafting a global settlement; possible defenses to sanctions and export control allegations; and case studies that highlight these issues.

6.2 Economic Sanctions and Export Controls Enforcement Overview

Multiple agencies within the U.S. government are responsible for the regulation and enforcement of economic sanctions and export controls. The primary regulatory agencies include:

- Department of Commerce's Bureau of Industry and Security (BIS), which administers the Export Administration Regulations (EAR),[2] pursuant to the Export Control Reform Act of 2018 (ECRA);[3]
- Department of State's Directorate of Defense Trade Controls (DDTC), which administers the International Traffic in Arms Regulations (ITAR),[4] pursuant to the Arms Export Control Act (AECA);[5] and
- Department of Treasury's Office of Foreign Assets Control (OFAC), which implements economic sanctions regulations,[6] pursuant to the International Emergency Economic Powers Act (IEEPA),[7] the Trading With the Enemy Act (TWEA),[8] and various other congressional statutes.

The primary agencies with economic sanctions and export controls enforcement authority are:

- BIS, through its Office of Export Enforcement (OEE);
- DDTC, through the Compliance and Civil Enforcement and Law Enforcement Liaison teams within the Office of Defense Trade Controls Compliance (DTCC);
- Department of Homeland Security, through U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE);
- Department of Justice (DOJ) through its National Security Division, in coordination with the Federal Bureau of Investigation (FBI) and the U.S. Attorneys' offices around the country;
- OFAC, through its Sanctions Compliance and Evaluation Division (for financial institution respondents) and Compliance and Enforcement Division (for all other respondents);
- Department of Commerce's Census Bureau (Census), through CBP's enforcement mechanism; and
- With respect to financial institutions, the U.S. Federal Reserve (the Fed), the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and various state-

level banking regulators, such as the New York Department of Financial Services (DFS).

These agencies have wide-reaching jurisdiction, which impacts both U.S. and non-U.S. companies. Jurisdiction among the agencies often overlaps, which can lead to inconsistencies in enforcement due to competing priorities and differing interpretations of laws and regulations. Multiple agencies may have an interest in investigating and penalizing the same violation under different regulations.

When a company discovers a potential violation, the company should consider and seek to address all of the agencies that may have jurisdiction. A company must be careful to ensure that violations of each regulatory regime are uncovered and, where appropriate, disclosed to and resolved with all of the relevant agencies simultaneously. Overlooking an agency and having to face additional penalties and collateral consequences later can complicate settlement negotiations down the road.

6.3 Internal Investigations

(a) Initial Analysis and Assessment

There are many ways in which a potential economic sanctions or export control violation can be uncovered, including a routine internal audit, whistleblower report, media investigation, receipt of a subpoena, or execution of a search warrant by government agents. When a potential violation is uncovered, the company should begin to address the issue by (1) immediately stopping ongoing potential violations; (2) conducting an initial assessment of the likelihood, scope, and significance of any potential violations; (3) implementing steps necessary to mitigate harm from the potential violation; (4) deciding who will lead the investigation, including whether to retain outside counsel; and (5) preserving relevant documents and information, including system data.

During this initial stage, the company should also consider how best to manage the risk of government involvement. In some cases, the government may already be aware of the potential violation, while in other cases, the company should consider whether and when to disclose it voluntarily, as described in Section 6.5. In either situation, the company’s preliminary

actions will be subject to scrutiny and will impact, and perhaps determine, the ultimate resolution.

(i) Stopping the Potential Violations

Upon discovering a violation, the most critical step is to immediately stop any potentially unlawful conduct. A carefully considered but swift response to potential violations helps stop any illegal conduct and prevents further violations. It can also demonstrate the company's commitment to compliance. This is particularly important in cases where regulatory or enforcement authorities may later scrutinize the company's actions. One of the first questions an agency may ask is whether the company took measures to protect against any further violations. A company's ability to demonstrate that it responded thoroughly and in a timely manner when it became aware of the potential violations will aid in establishing that the company is committed to remediation and ongoing compliance with the law.

A recent DDTC case illustrates the risks of continuing to export goods during the pendency of an agency review. Keysight Technologies, a California-based company, continued to export its electronic test software, which it had self-classified as EAR99, while awaiting the outcome of a DDTC jurisdiction and classification dispute.[9] Ultimately, DDTC determined the software to be ITAR-controlled and, in the consent agreement, listed the continuing export of the software as an aggravating factor, required the appointment of a Special Compliance Monitor for three years, and imposed a fine of US$6.6 million, of which US$2.5 million was suspended to cover remedial expenses.

Thus, at a minimum, during the pendency of an investigation, a company should stop any deliveries of goods, software, data, or services and halt any transactions that are the subject of the potential violation. Depending on the facts and circumstances of the investigation, the company may also need to recover items that have been shipped illegally, although in some situations retrieval and return of the items would be viewed as an additional violation unless authorized by the U.S. government.[10]

The company may also need to suspend its relationship with any counterparties implicated by allegations of misconduct. Again, this is a step with potential consequences and may necessitate a wind-down period that would require government authorization. In cases that present potential

willful or reckless behavior (including willful blindness), the company should consider suspending any employees or contractors involved in the violation or removing them from positions within the company where they could continue to engage in prohibited activity, pending further investigation. However, this, too, may have consequences under local employment law and/or jeopardize their cooperation in the internal investigation or any subsequent government investigations.

How a company responds to knowledge of a potential violation is also important if the initial report was raised by an employee-initiated whistleblower complaint. By demonstrating that it took the allegation seriously, the company can decrease the likelihood that the complainant will report the conduct outside of the company, whether to the media or to the government. Keeping knowledge of a complaint or a potential violation within the company enables the company to maintain control over the initial steps of the investigation, rather than allowing third parties, such as enforcement agencies, to drive the scope and timing of the investigation.

(ii) Initial Evaluation of Alleged Conduct

In parallel with its efforts to stop any potentially illegal conduct, the company should begin to evaluate the facts of the case against applicable economic sanctions and export control regulations to determine the likelihood that a violation has occurred and whether a more thorough internal investigation is, in fact, warranted. The company may conclude that an informal inquiry is all that is required to understand and address the issue. However, even informal investigations must be carefully documented with a view to justifying the investigative steps and findings, if the matter is later subject to a government investigation. Meanwhile, an investigation undertaken without the assistance of counsel may not benefit from the attorney-client privilege, which could protect communications and documents related to the investigation from disclosure.

In order to ensure that the initial evaluation is thorough and complete, the company should, among other things:

- Determine the scope of the potential violation in terms of subject matter (what controlled products or prohibited transactions were involved), regimes (what regulations may have been breached), timing (when did potential violations occur, when were they

discovered, and when were they stopped), parties (what individuals, organizations, and third parties may have been involved), and geography (in particular, what countries may have received unauthorized material or services);
- Attempt to establish whether the violation was willful, reckless, or negligent;
- Ascertain whether and at what level management was involved, whether it was systemic or the work of an employee acting without authorization, and was the management willfully blind;
- Understand how the violation occurred and, preliminarily, what its root causes were;
- Evaluate the credibility of the information provided; and
- Identify compliance mechanisms that did not work.

The company must analyze the facts gathered through the investigation under the appropriate economic sanctions and export controls regime. This analysis is often difficult because the regulations are subject to frequent amendments, the same terms can be used and defined inconsistently across the different regulations, and different agencies may interpret and apply the regulations differently to the same conduct. Specialized knowledge of both the regulations and how they are applied by the relevant agencies is required to accurately conduct this analysis.

Once a company has completed its initial evaluation, it will be in a better position to determine whether and how to proceed with the investigation. Regardless of the decision, the company should document its reasons for either concluding the matter after an initial inquiry or continuing with further investigatory steps. This documentation will be particularly important if the company’s decision not to conduct a full internal investigation comes under scrutiny later by regulators or enforcement agencies.

As the company proceeds with its internal inquiry, every effort should be made to keep the details closely held until the company determines whether it will disclose its findings to the government. Accordingly, the company should involve the fewest personnel needed to carry out the preliminary investigation and should not disclose more information than is necessary in internal corporate communications, such as document retention notices and internal reports, during this period. A steering committee may

be established to oversee the investigation and to limit the flow of information inside the company.

(iii) Initial Mitigation

Once a company has determined that it may have violated applicable economic sanctions or export control regulations, it should take reasonable steps to minimize the potential harm from the violation. Depending on the circumstances, such steps may include requesting that controlled items be quarantined or, in appropriate cases, returned or destroyed; if possible, negating the national security value of the controlled items through technical or other means; and informing relevant regulatory or national security agencies of the violation so they can take steps themselves to minimize its impact. In some cases, discussed *infra* at Section 6.5(a), immediate notification of the agency is mandatory and failure to do so constitutes an additional violation. Taking such steps can both minimize the seriousness of the violation and demonstrate to the enforcement agencies the company's overall commitment to compliance.

(iv) Deciding Who Will Lead the Investigation

In determining who should conduct the internal investigation, a company should weigh questions of expertise, resources, confidentiality, independence, objectivity (and the perception thereof), and cost.

It may be appropriate for in-house counsel, compliance staff, or internal auditors to lead the investigation if the alleged violations are limited in nature and number and were clearly the result of inadvertent mistakes. In-house counsel often have an understanding of the applicable economic sanctions or export control laws and should have the advantage of a deep knowledge of the company's personnel, systems, and operations. However, investigations conducted by compliance staff or internal auditors are not necessarily covered by the attorney-client privilege or attorney work-product doctrine.

If there are indications that the conduct at issue is widespread, criminal in nature (i.e., deliberate and willful), or that management is implicated, a company should carefully consider retaining outside counsel to conduct the investigation. Reasons for this include the following.

First, by hiring outside counsel that is independent and objective, and perceived as such by the government, a company can credibly assert that it should be allowed to conduct the investigation itself without being subjected to an intrusive and disruptive government investigation, which often involves the use of search warrants or the grand jury process.

Second, the attorney-client privilege and work-product doctrine are most likely to apply to communications and materials related to the investigation when they are prepared by or with the assistance of outside counsel. This is especially relevant in cross-border investigations involving countries where the attorney-client privilege may not apply to communications with in-house counsel.

Third, outside counsel can serve as a buffer between the company and the government and provide a single point of contact for all stakeholders. Using outside counsel as the primary interlocutor with the government can also achieve certain strategic goals, particularly during settlement negotiations where counsel may be seen as retaining some degree of independent judgment not colored by the company's or any individual employee's defensive position in the discussions.

Fourth, outside counsel with expertise in economic sanctions and export controls honed through government or industry experience may have a better understanding of the regulatory nuances and intricacies than local prosecutors with limited experience in this area or federal agents with a broader scope of enforcement. Similarly, if the case involves a criminal prosecution, a company should make sure to consult expert criminal counsel.

Finally, almost by definition, economic sanctions and export control violations involve non-U.S. jurisdictions, which can implicate data privacy statutes, bank secrecy regulations, employment laws, blocking statutes, national security, confidentiality rules, and other relevant national laws. Outside counsel can help determine whether there are non-U.S. legal issues and can coordinate this advice with qualified local counsel.

(v) Preserving Documents

A company embarking on an internal investigation or facing the prospect of an external investigation should develop a plan to preserve relevant evidence. It should immediately suspend any automatic document or information destruction processes to preserve all communications and

documents that could be relevant to the investigation and take steps to preserve such information on servers, back-up tapes, hard drives, mobile devices, and other similar platforms, including any historical information that may be relevant to the investigation. Failure to do so could hamper the investigation and, in severe cases, result in obstruction of justice charges.

A company should also identify employees who may possess relevant documents and distribute document retention notices to them. These notices should be carefully worded to keep investigation details confidential. The instructions should direct employees (also known as information or data "custodians") not to destroy any relevant documents (both hard copy and electronic) in their offices or elsewhere that are in their possession and control. The notices should also require an acknowledgment and certification of compliance by the custodians, which should be maintained in the investigation files. In the event that relevant documents are not maintained, it will be important for a company to demonstrate that it did everything possible to prevent their destruction.

(b) Conducting the Investigation

If the initial analysis demonstrates a likelihood of violations of law, a full internal investigation typically requires the following steps: (1) protection of legally privileged materials; (2) collection, review, and analysis of relevant documents and transaction data; and (3) substantive interviews of relevant employees and third parties.

(i) Attorney-Client Privilege and Attorney Work-Product Doctrine

Prior to conducting any investigation, a company should consider how to preserve legal privilege throughout the investigation.

The attorney-client privilege protects only confidential communications between a client and an attorney with the purpose of obtaining advice from the attorney in his or her capacity as a legal professional, and the contents of communications between a lawyer and the client made in the course of representing the client. In order for the attorney-client privilege to apply, the primary purpose of the communication must be to seek or provide legal advice. Communications are not privileged if the sole or dominant purpose of the communication is business advice, and privilege may not always protect dual-purpose (i.e., business/legal) communications.

The attorney work-product doctrine protects oral and written communications prepared by a party or its representatives in anticipation of litigation. The protection covers paralegals, assistants, clerks, staff, litigation support firms, and others if their work product is done at the direction of an attorney on behalf of the client. However, because this doctrine is not a privilege, but a qualified immunity from disclosure, it is not absolute. Courts apply a balancing test in assessing whether the doctrine protects against the disclosure of attorney work product by weighing the public interest in disclosure against the privacy rights of the party.

The following are some practical recommendations for preserving privilege and work product: (1) always mark privileged documents "Privileged & Confidential," and, where appropriate, "Attorney-Client Communication" or "Work Product," or both; (2) be clear in communications that the person is seeking legal advice; (3) whenever possible, have outside counsel, rather than company lawyers, prepare any necessary documents, including memoranda, drafts, emails, and notes of conversations or interviews incorporating the counsel's impressions; (4) counsel should be present at all interviews, and only counsel should take notes; (5) if counsel retains the services of outside vendors or consultants to assist with the investigation, the vendor or consultant should execute an appropriate confidentiality agreement with counsel (not the client) to maintain the confidentiality of any work-product materials.

Privileged documents should not be voluntarily disclosed to a government agency without (1) drafting an appropriate reservation of rights to assert privilege; (2) receiving recognition from the recipient agency of such reservation; (3) requesting confidentiality; and (4) receiving assurance from the agency recipient of confidential treatment. If the foregoing is obtained verbally with the agency, it should be confirmed in a formal letter to the agency (for example, in a cover letter forwarding privileged documents as attachments).

(ii) Document Control, Collection, and Analysis

The company may collect the relevant documents using its own internal processes; however, using outside counsel or third parties provides a stronger investigation record when disclosing to U.S. government agencies. Moreover, external counsel will provide advice on the effect of non-U.S. data protection laws, which could be implicated by the mere act of

collecting the documents even before their analysis. A company may need local counsel's opinion as to the appropriate method for collecting the documents (e.g., whether the custodian's consent must be sought).

Part of the investigation record should include written document preservation and collection notices to all document custodians (in addition to the initial document retention notices). To identify additional custodians, consider every department that might be involved in an economic sanctions or export controls violation. Initial scoping interviews may ensure that all possible custodians are identified and all documents and information arguably relevant to the investigation are collected.

Analysis of the documents may require the services of a litigation support firm to electronically scan and upload hard copy documents, along with the collection of electronic documents. Working with the company and its counsel, the litigation support firm will develop a search methodology, perhaps using a list of keywords, to ensure that the document search and analysis are suitably comprehensive and thorough. The list of keywords may ultimately be shared with the government to ensure that it meets their expectations.

Once analyzed, the relevant documents can be used as the basis for substantive interviews.

(iii) Conducting Interviews

In addition to substantive interviews of all employees involved with the misconduct at issue, counsel should also interview individuals who can provide information about the company's compliance program. Those interviewed by counsel should also include senior management to determine, among other things, whether they understood their responsibility for setting the compliance "tone from the top" (or middle) and whether they may have been directly involved in the potential violation.

If the government is or will be involved, there is a potential that any interview memoranda will be disclosed during the course of the investigation, although the government is restricted from conditioning cooperation credit on waiver of the attorney-client privilege in most cases. Accordingly, the memoranda should not include editorial comments or case strategy.

To prevent the misunderstanding that company counsel represents the interviewee in connection with the investigation, the interview memoranda

should document that counsel delivered an *Upjohn*[11] warning at the beginning of the interview and that the interviewee acknowledged that he or she understood it. If an employee's interests are adverse to the company's interests, the individual may need to retain separate counsel. In addition, union employees may be entitled to have a union representative present.

At a minimum, counsel should use interviews to collect and probe the following: (1) the facts surrounding the violation, including the identities of everyone involved and reporting lines, to gain an overall understanding of the issue; (2) information regarding the potentially export-controlled item or prohibited transaction at issue, including any technical specifications, components, and licensing history; (3) the extent to which the parties involved have knowledge of economic sanctions, export controls laws, and the company's relevant compliance procedures, particularly as they relate to the specific item or transaction at hand; and (4) the remedial measures taken following discovery of the violation, including how additional violations were prevented, and whether any disciplinary actions occurred or were planned.

Interviews conducted outside the United States must recognize and accommodate local legal requirements, language barriers, and customs. Local employment laws may require the involvement of local counsel or may limit the conditions under which the interview may take place. Logistics such as witness safety and comfort, recordkeeping, and document handling will also present challenges. Keep in mind the possibility of nondisclosure agreements and ensure that such agreements are waived by management to ensure that employees are free to provide complete answers during the interview process and throughout the investigation.

6.4 Remediation

The sufficiency of the remedial measures a company takes to correct violations and prevent their recurrence is as important to the government as the rigor of the investigation into the historical conduct. This is clear from DOJ's explicit inclusion of a corporation's remedial efforts, including the implementation of an effective compliance program, replacement of managers involved in the misconduct, and discipline of wrongdoers in its Principles of Federal Prosecution of Business Organizations.[12]

While completing its internal investigation, a company should make sure that it has addressed internal control deficiencies. This includes updating relevant policies and procedures, improving internal controls based on the root cause analysis, and documenting the company's heightened efforts to ensure their effective communication to all employees through regular trainings or other means.

Where the investigation reveals that particular individuals are responsible for violations of law, the company should consider taking disciplinary action, in consultation with local human resources, union representation, and employment law counsel. Discipline of employees responsible for negligent or willful violations can help demonstrate the company's commitment to compliance. In more serious cases, terminating the employment of such individuals may be appropriate. In some cases, the government may expect the company to cooperate in its investigation of an individual's misconduct in order to receive maximum cooperation credit.

In making employment decisions, however, the company should keep in mind the effect that termination would have on its overall compliance objectives. Termination of employment and other substantial employee discipline can have significant implications for the investigation (e.g., that individual's willingness to cooperate or availability for subsequent U.S. government interviews) and beyond (e.g., what impact would termination have on other employees' willingness to disclose potential economic sanctions and export controls violations). If the employee being considered for termination was involved in disclosing the potential violation internally, care must be taken to avoid any appearance that termination is intended as punishment for the disclosure or to otherwise discourage whistleblowing.

The government often includes in its settlement documents a description of the mitigation credit given to a company in recognition of the remediation undertaken following discovery of the violation. In most cases, agencies give significant mitigation credit for remedial measures taken by companies in response to violations. In one such case, DDTC recognized a company's extensive remedial compliance measures, which included "conducting multiple compliance audits, expanding ITAR training, creating a fully-documented compliance program, and increasing staff resources devoted to day-to-day compliance."[13] DDTC gave the company significant mitigation credit in its settlement and "determined that an administrative

debarment would not be appropriate and that additional remediation with outside monitoring was unnecessary."

6.5 Voluntary Self-Disclosure

(a) Determination of Whether to Self-Disclose

A company should evaluate whether to voluntarily self-disclose a violation to the government at various points during an investigation. This may happen early in the process, if the company quickly concludes it is likely that a violation occurred. The government generally gives maximum mitigation credit for *timely* voluntary self-disclosure (which can be as high as 100 percent of the maximum penalty in certain cases); therefore, the opportunity should not be lost.[14]

When determining whether to make a voluntary self-disclosure (VSD), the first question is whether the law requires disclosure. VSDs of potential economic sanctions or export controls violations may be required in certain circumstances, including, but not limited to the following:

- The ITAR imposes a requirement to immediately notify DDTC where the underlying conduct involves a potential violation of the ITAR and a proscribed country is involved.[15]
- Disclosure would be necessary if a company seeks authorization to proceed with a particular transaction with knowledge that a violation had occurred, was about to occur, or was intended to occur (e.g., the company has been requested to engage in any transaction involving an item that was illegally exported). Failure to disclose in certain circumstances could violate General Prohibition 10 or EAR Section 764.5(f).[16] For example, if a company needs to proceed to dispose of, or otherwise deal with items involved in a violation of the EAR, it must request authorization, and prior to doing so, it should disclose the violation.[17]
- Disclosure may be necessary in order to avoid making false, misleading, or incomplete statements to the U.S. government on or in support of export license submissions, or in connection with other actions. Failure to disclose information material to a license

application may be a violation itself and may invalidate licenses issued as a result.[18]
- The terms of a prior settlement, agreement, or compliance monitorship with the U.S. government may mandate ongoing disclosure of new misconduct.

Also note that the BIS policy regarding voluntary self-disclosure "strongly encourages disclosure to OEE if you believe that you may have violated the EAR, or any order, license or authorization issued thereunder."[19] While this does not mandate disclosure, BIS may effectively penalize failure to do so.

Similarly, DOJ "encourages companies to voluntarily self-disclose all potentially willful violations" of primary U.S. export control and sanctions regimes.[20] In keeping with this policy, DOJ applies a presumption that the disclosing company will receive a non-prosecution agreement and will not pay a fine, other than disgorgement of any profits obtained as a result of the violation.

From the beginning, a company must also carefully analyze the other factors that affect the risks and benefits of disclosure. These may include:

- The risk that the government will discover the violation on its own, and whether the discovery is imminent. The discovery of a violation by the government in the first instance can negate a company's chance to obtain full credit for voluntary disclosure and will often undermine trust between the agencies and the company. Government agencies are increasingly likely to discover violations as a result of enhanced whistleblower protections, interagency and cross-border collaboration, and automated import and export data. Financial institutions are an increasingly important source of information concerning their customers' violations;
- If there is a possibility that non-disclosure could create a national security risk (e.g., if government assistance is required to recover a sensitive item destined for dangerous hands), immediate disclosure is also advisable;[21]
- The risk that failure to disclose will allow a systemic compliance weakness to continue, resulting in potentially more serious violations in the future;

- The risk that the company may not devote the same resources to investigating and remediating a matter that is not disclosed to the authorities, and that undisclosed violations may be taken less seriously by company management and employees than violations that the company knows are subject to potential government penalty;
- The benefit of consistency in the company's internal processes. It can be difficult in practice to establish justifiable standards in a corporate compliance program for when to disclose and when to stay silent. Companies often find it easier to commit to full disclosure in all cases rather than to establish processes for deciding when disclosure is not in the company's interest; and
- The benefit of developing trust with regulators through the VSD process is central to any company's compliance program.

While the aforementioned realities often support a decision to voluntarily disclose, there may be circumstances, particularly in EAR and OFAC compliance, where the potential risks of disclosure outweigh the value of disclosing. In such cases, if the company decides against submission of a VSD, it should conduct a thorough investigation, document its findings and reasons for not disclosing the potential violation, and ensure that its remediation program is sufficiently robust to address the underlying causes of the violation to prevent a recurrence.

Self-disclosure often reduces the risk that the government will seek criminal penalties, or reduces the severity of penalties sought, as long as the agencies determine that the disclosure was truthful, complete, and voluntary.[22] However, the government's assessment of the disclosure is discretionary and subjective. Therefore, companies should make disclosures knowing that there is a possibility of prosecution where the facts and circumstances warrant. Despite assurances of lenient treatment for voluntary self-disclosures, the government can and does investigate, prosecute, and impose penalties where it believes there is a compelling reason for doing so.[23] Even if no penalties are imposed, the government keeps a record of the violation disclosed, which can affect the particular agency's treatment of future violations.

A company should be aware that its submission of legally privileged documents as part of a VSD may waive the attorney-client privilege, not only as to the VSD itself, but potentially to the entire subject matter of the

VSD. In addition, in order to protect against disclosure of the VSD to outside parties, including under a Freedom of Information Act (FOIA)[24] request, the disclosure should indicate as appropriate that it includes confidential proprietary commercial, or financial information and be marked accordingly. Assertions of FOIA protection can be challenged by interested third parties, and in litigation, only those portions of a submission that actually contain confidential information will likely be protected from public disclosure.

The company should also consider whether, when, and how to coordinate with third parties who may be involved in the potential violation, such as exporters, freight forwarders, suppliers, intermediate consignees, end users, and financial institutions. Violations usually involve more than one party, and coordination can often be helpful in conducting an investigation and submitting a fulsome disclosure to the regulators. As stated earlier, however, the decision to coordinate with third parties should be made after careful consideration of the consequences, including the need to maintain privilege, the risk that such third parties may seek to cast blame on the company, and the danger that they may undermine the company's penalty mitigation efforts by informing an agency before the company is ready to submit its VSD.

In preparing a VSD, a company should consult the relevant agency's specific procedures and evaluative methodologies set forth in the agency's regulations and on their websites.[25]

(b) OFAC

If OFAC determines that a self-disclosure is "voluntary," the potential administrative penalty amount would be reduced by 50 percent, and in many cases, there is no penalty applied.[26]

OFAC narrowly defines "voluntary" to exclude information that would otherwise be available to OFAC or contained in a report that is required of another participant in a transaction (such as an intermediary bank in a funds transfer), regardless of whether or when the report is ultimately filed.[27] Nonetheless, cooperation with OFAC may lead to substantial penalty mitigation, even if the disclosure does not qualify under OFAC's definition of voluntary.

If a company decides to disclose a violation, it is generally advisable to notify OFAC of the issue as soon as it is discovered by filing an initial notice of VSD. This prevents the possibility that OFAC will become aware of the issue before a full VSD can be made, potentially negating the opportunity for VSD mitigation credit.

OFAC requires initial VSDs to be followed up with a final VSD report containing full details needed for the case's adjudication within "a reasonable time."[28] What is reasonable depends on the circumstances, as OFAC does not have a regulatory deadline. Nevertheless, OFAC practitioners seek to file an initial disclosure quickly, generally within 60 to 90 days of discovery of a potential violation. Any special circumstances should be discussed on an ongoing basis with an OFAC case officer.

The final VSD report should address all relevant factors present in the case that could affect the severity of a potential administrative penalty, including the parties/transactions involved, the results of the investigation, and remedial response, and other factors described in OFAC's Enforcement Guidelines.[29] These include aggravating and mitigating factors such as willfulness, recklessness, concealment, whether there was a pattern of conduct, prior notice, management involvement, awareness of the conduct at issue (actual knowledge or reason to know), harm to sanctions objectives and the implications for U.S. policy, the benefit received by the sanctions target, the timing of the violation (just after new regulations are issued or old regulations are revoked), license eligibility, enforcement activity by other agencies, the deterrent effect of penalization on the rest of the industry, humanitarian activity and individual characteristics (the company's size, sophistication, financial conditions, sanctions history), effectiveness of the compliance program, and the remedial response.

OFAC has attempted to impart compliance guidance to industry as part of its settlement announcements, one factor which may influence its decision to pursue an enforcement action in response to a VSD.[30] All of its enforcement actions since the start of 2018 have included significant compliance commitments, exemplifying the agency's current informal mantra of "better compliance through enforcement."

If the disclosing party intends to negotiate a settlement following the filing of a final VSD, it should request that OFAC not issue a Pre-Penalty Notice (PPN) and that settlement negotiations immediately commence so that the potential charges can be discussed. Negotiation of a settlement may

still occur if a PPN has been issued, provided that the time for a Penalty Notice has not expired.

Besides issuance of a penalty, other potential outcomes for an OFAC enforcement investigation include (1) no action; (2) an administrative subpoena where further information is required; (3) a Cautionary Letter warning the respondent to be more vigilant against future breaches; (4) a formal Finding of Violation that documents the determination but without further penalty; (5) a criminal referral; or (6) other administrative action, such as an OFAC license denial, suspension, modification or revocation, or issuance of an OFAC Cease and Desist Order.[31]

(c) BIS

BIS provides a 50 percent reduction in the base penalty for VSDs in most cases, with possible full penalty suspension for VSD cases with a combination of mitigating factors, such as cooperation.[32] Without a VSD, mitigation will generally not exceed 75 percent of the base penalty.[33] To be deemed voluntary, the disclosure must be received before any government agency obtains knowledge of the "same or substantially similar information from another source."[34] BIS considers the same factors that OFAC considers, detailed earlier in determining whether to pursue penalties in any particular case, and in what amount. VSD and other mitigation credit can be completely outweighed in some cases by aggravating factors from this list.

BIS advises that an initial notification should be submitted by the disclosing party "as soon as possible after violations are discovered."[35] The initial notification should identify the disclosing party and describe the general nature and extent of the violations. Upon submitting the initial notification, the disclosing party should then conduct a thorough review or investigation of relevant similar transactions, which BIS recommends should cover a period of five years prior to the date of the initial notification.

Once the review is completed, the disclosing party must then submit a final VSD, which must include a narrative account of the violations, supporting documentation, and a certification of truth and accuracy by the disclosing official with authority to bind the company. BIS has a 180-day deadline for persons who have submitted an initial notification to complete and submit the final narrative report to OEE.[36] The director of OEE has

discretion to extend this 180-day deadline if U.S. government interests would be served by an extension or upon a showing by the party making the disclosure that more time is reasonably necessary to complete the narrative account.[37]

Section 764.5(c)(3) of the EAR provides a list of what the narrative account should address, including (1) the nature of the review conducted and measures that may have been taken to minimize the likelihood that violations will occur in the future; (2) the kind of violation involved; (3) an explanation of when and how the violations occurred; (4) the complete identities and addresses of all parties involved; (5) license numbers; (6) a description, quantity, value (in U.S. dollars), and Export Control Classification Number of the item(s) involved; and (7) any mitigating circumstances.

Under section 764.5(f), it is possible (and may be required) to request permission from BIS to engage in certain transactions related to unlawfully exported items.[38] If the request is granted, future activities with respect to those items that would otherwise violate section 764.2(e) will not constitute violations. However, even if permission is granted, the person making the disclosure "is not absolved from liability for any violations disclosed nor relieved of the obligation to obtain any required reexport authorizations."

(d) DDTC

In order for a disclosure to be considered voluntary by DDTC, the disclosing party must submit its disclosure before any government agency obtains knowledge of the "same or substantially similar information from another source."[39] In addition, DDTC "strongly encourages" disclosure and may consider the submission of a VSD to be a mitigating factor.[40] Unlike OFAC and BIS, however, DDTC will consider the failure to submit a VSD to be an aggravating factor when determining the disposition of a case. DDTC often resolves VSDs without imposing any penalties at all—saving the imposition of penalties for more egregious cases threatening U.S. national security, cases demonstrating some important legal issue, cases where DDTC believes the exporter acted willfully or with gross negligence, and cases that DDTC views as undermining DDTC's authority or interpretation of the ITAR.

As noted earlier, DDTC requires that the disclosing party submit an initial notification "immediately after a violation is discovered" followed by a thorough review and final disclosure within 60 calendar days of the initial disclosure.[41] While DDTC will consider granting an extension after the disclosing party provides a justification in writing, unreasonable delay may result in the disclosure not qualifying as "voluntary."

DDTC provides specific instructions regarding what should be included in a VSD, including (1) identification of the disclosing party and a point of contact; (2) a precise description of the violations and the exact circumstances surrounding the violations; (3) the complete identities and addresses of all parties involved; (4) license numbers, exemptions, or other applicable authorizations; (5) a description, quantity, and U.S. Munitions List (USML) category of the hardware, technical data, or defense service involved; and (6) corrective actions taken and how they are designed to prevent similar violations from occurring in the future.[42]

DDTC also provides a list of factors to be addressed in the VSD, including whether the violation was intentional or inadvertent, the parties' familiarity with the laws and regulations, prior AECA administrative or criminal action, and the compliance measures that were in place at the time of the violation. The VSD should also address whether the violation puts U.S. national security or foreign policy interests at risk, whether a license likely would have been granted for the transaction if requested, and any root causes of the violation uncovered during the investigation. The VSD must include any supporting documentation and a certification of truth and accuracy by an empowered official or senior officer.

(e) DOJ

Like the other U.S. agencies, DOJ also considers whether a company made a VSD when determining whether to take enforcement action and when assessing monetary penalties. DOJ is guided in this respect by section 9.28.000 of the Justice Manual (formerly called the U.S. Attorneys' Manual), which details the general "Principles of Federal Prosecution of Business Organizations."[43] Among a list of "General Factors" DOJ prosecutors will consider, is "the corporation's timely and voluntary disclosure of wrongdoing" when considering whether to pursue a criminal enforcement action.

In particular, in December 2019, DOJ's National Security Division (NSD) revised its policy for business organizations regarding voluntary self-disclosures of export control and sanctions violations, building on its October 2016 VSD Guidance.[44] The 2019 DOJ VSD Policy "signals the Department's continued emphasis on corporate voluntary self-disclosure, rewarding cooperating companies with a presumption in favor of a non-prosecution agreement and significant reductions in penalties."[45] Importantly, the 2019 DOJ VSD Policy identifies the actions required by a company in order for DOJ to deem a disclosure voluntary: (1) disclosure prior to an imminent threat of disclosure or government investigation;[46] (2) disclosure within a reasonably prompt time after becoming aware of the offense; and (3) disclosure of all relevant facts known to it, including all relevant facts about individuals substantially involved in or responsible for the misconduct at issue.

To receive credit for full cooperation, the 2019 VSD Policy requires:

- Disclosure of all facts relevant to the wrongdoing at issue, including all facts gathered during the internal investigation, with specific source attribution, not a narrative, unless protected by the attorney-client privilege; rolling production; and all known facts regarding third-party criminal conduct;
- Proactive cooperation and identification of evidence not in the company's possession;
- Disclosure of documents and information, including identification of overseas documents, facilitation of third-party production, and translation. The company bears the burden of establishing any local prohibitions on disclosure due to data privacy, blocking statutes, or other foreign laws.
- Deconfliction of witness interviews (agreeing to allow the government to interview witnesses before the company's legal team); and
- Facilitation of interviews of current and former officers, employees, and agents with relevant information even if located overseas (subject to individual Fifth Amendment rights).

DOJ focuses on VSDs as a factor in order to encourage companies to conduct internal investigations as part of their compliance programs. However, despite this goal and the widely held view that companies who

voluntarily disclose to the U.S. agencies will not face criminal prosecution, both the case history and DOJ's position as stated in the Justice Manual make clear that "prosecution may be appropriate notwithstanding a corporation's voluntary disclosure."[47] All of the administrative agencies reserve, and some have exercised, their discretion to refer VSD violations to DOJ for criminal prosecution, even while denying the likelihood of their doing so.[48]

Whereas in the past, potential export control violations would be disclosed only to the civil agencies (e.g., OFAC, BIS, DDTC), now companies must consider much earlier in the process whether to also disclose to DOJ or risk losing VSD credit. As explained in the 2019 DOJ VSD Policy, "when a company identifies potentially willful conduct, but chooses to self-report only to a regulatory agency and not to DOJ, the company will not qualify for the benefits of a VSD under this Policy in any subsequent DOJ investigation."[49]

(f) Summary of Voluntary Self-Disclosure

Regardless of the procedures and methodologies required by the respective government agency, any disclosures that are made to the government must be truthful and complete, as any false or misleading statements can serve as the basis for separate criminal charges that are unrelated to the underlying conduct.

VSDs should present every applicable mitigating circumstance and preemptively address any aggravating factors. The disclosing company does not want to end up in a situation where numerous aggravating factors are discovered by the government and used against it in assessing the final penalty. VSDs should also include what remedial measures have been taken since discovering the violation and remedial measures that are promised in the VSD need to be completed and not forgotten after the VSD is filed, as agencies may ask for proof of their completion. Finally, during the investigation and at the time of determining whether to disclose, the company should consider all violations in related subject areas (i.e., anti-money laundering, customs, or anti-bribery and corruption laws).

Counsel representing a company that has made a disclosure is encouraged to maintain an ongoing dialogue with government counsel and enforcement agents. Through that dialogue, information about the scope of

the government investigation, the potential targets, and the government's point of view can often be obtained, which can inform the course of the company's internal investigation. Depending on the gravity of the disclosure, it may be helpful to meet with all of the relevant agencies to ensure their reviews are coordinated and that a simultaneous resolution with each is possible.

However, if a company decides to proceed on the question of disclosure, it should ensure that its policies and procedures are reasonably designed to prevent a recurrence of the violations and that all remedial measures promised in the disclosure are accomplished.

6.6 Global Settlements

In settling cases involving economic sanctions and export controls violations, companies and their counsel must consider all relevant agencies, administrative and criminal, that may be involved, given the overlap in regulatory authority. Settlement negotiations may include DDTC, BIS, OFAC, and in some cases, Census, the Department of Defense, DOJ, various USAOs and local prosecutors, and the relevant banking agencies (DFS, OCC, the Fed). Each agency has its own agenda, interests, priorities, and timing, which will determine whether it will defer to another agency's actions or insist on an additional penalty.

Moreover, companies and their counsel must be aware of the collateral consequences that may accompany a conviction or settlement, even if the case is settled without imprisonment or a fine. For example, a criminal conviction may result in federal or overseas contract debarment or denial of export privileges—potentially catastrophic consequences that counsel unfamiliar with economic sanctions or export controls may be unaware of until they jeopardize a carefully structured settlement.

Throughout the investigative phase and during settlement discussions, companies should try to communicate with all relevant agencies, as these agencies may or may not be communicating amongst themselves. Defense counsel should coordinate the global settlement, as agencies generally have neither the authority nor the interest to bind each other—or even to bind departments within the same agency. Thus, representations made by one enforcement authority regarding another's position on the resolution of the case should not be relied upon and should be separately confirmed. No

agency can speak for another, but some agencies can be encouraged to utilize their leverage to obtain a final resolution with all the relevant agencies. Including all of the agencies in the settlement discussions may result in a single fine joined by all of the agencies or even suspension of an agency's fine in light of the penalty exacted by others.

On the other hand, not including a relevant agency in the settlement discussions can have disastrous consequences. There are examples of a successfully negotiated settlement among several entities threatened by a late arriving agency that was not invited to the initial discussions and that insisted on separate fines and undertakings.

The maximum penalties set forth in the statutes and regulations are the starting point for a company's calculations as to the possible penalties.[50] Keep in mind that the ultimate fines could be multiples of the maximum statutory penalty, since the maximum may be applied per violation. Alternatively, the fines could be based on a figure that is twice the value of each transaction. The laws provide for various penalty calculation methodologies, all of which the agencies use in their discretion. Counsel can compare the case at hand with previous settlements reached with the relevant agencies by using the agencies' published settlements on their websites or in the Federal Register.[51] After calculating the base penalty considering all of these methodologies, companies should also consult BIS's and OFAC's respective Enforcement Guidelines which set forth other factors used in determining appropriate penalties.[52]

When considering how to structure a settlement, a company should consider all potential outcomes, including suspension of all or part of any penalty in recognition of the company's financial position, or if part of the penalty is directed to improving compliance measures. Compliance monitors and external audits may also be part of the settlement package and must be carefully considered before a settlement is reached. The total fees and costs of a compliance monitor and external audits, which the company must absorb in addition to the fines and penalties, can be considerable, as can the remedial measures required to resolve any additional compliance risks identified during the monitorship or audit.

If the agency insists on a denial of export privileges, a company should ensure that the denial is tailored to the particular risk posed by the specific item, country, or business unit involved. However, the company must recognize the reality that appearing on a denial list, even in a limited way,

can still have a negative impact on its business as many compliance-conscious customers and suppliers globally will be hesitant to transact with a listed company, regardless of the listing scope.

6.7 Possible Defenses and Mitigation

In some ways, the complexities of the laws and regulations governing economic sanctions and export controls can work in favor of a company seeking a defense. As a company learns the facts during an investigation, it may become clear that the potential violation was caused by an inadvertent mistake due to an honest misunderstanding of complex, inconsistent, and oft-amended laws. It may even be that there was no violation at all, due to a misinterpretation of the company's conduct by the government, a mistaken licensing determination or classification, or an overlooked amendment to the denied parties lists or the regulations. It is critical to review the regulations that were in place at the time of the violation as well as subsequently, as a case could have less appeal and is a questionable use of scarce enforcement resources, if the restriction the company is accused of violating has been lifted.

Jurisdiction, definitions, classifications, and the various agency lists all should be considered in mounting a defense.

(a) Challenges to the Charges

(i) The Government's Investigation

In developing a defense to a possible economic sanctions or export control violation, a company should review the government's investigation, including how the alleged violation was discovered and how it was determined to be a violation. Experience and familiarity with this complex regulatory area varies among the agencies, as some investigations are undertaken by agents that are on a rotational system and do not devote their career to enforcing this body of law. Additionally, some career agents have little experience with criminal investigative procedures, since so many cases are the result of VSDs that are settled quickly. Accordingly, counsel should review the possible improper use of attorney-client privileged information, and information obtained through illegal searches, particularly during warrantless border searches. (Given the inherent likelihood of

international travel in these cases, employees must be warned about traveling into and from the United States while carrying documents in hard copy or that are accessible on laptops and other electronic devices.)

Counsel should carefully examine search and arrest warrants, interview memoranda, criminal complaints, and indictments. Again, due to the complexity of the laws and, until recently, the scarce number of these cases in federal court, drafting mistakes can be detected and used to protect against overreaching. In one case known to the authors, an indictment that carefully detailed the relevant complex export control laws was dismissed after the jury was sworn because it did not state the element of intent.

Finally, a careful review of the applicable regulations themselves is important, particularly when they have been amended recently. There are changes in definitions, interpretive guidance, license exceptions, jurisdictional elements, and enforcement theories that should be considered. This is especially true in light of the ever-shifting regulatory landscape of economic sanctions and export controls that can be difficult to track, especially if rules have been amended, reformed, or suspended since the potential violations occurred.

(ii) Licensing Determinations and Classifications

Many export control and economic sanctions cases rise and fall on the determination by the relevant agency that a license was required and was not obtained. Determining whether an item requires a license typically involves a mix of engineering and legal analysis, which must be confirmed in order to assess whether a violation occurred.

Independent assessment is made difficult by the line of authority establishing that the agency's classification of an item is not itself subject to challenge.[53] However, that authority only limits challenges to the underlying classification of a type of item, not the applicability of that classification to the particular item involved in the transaction.[54] Accordingly, counsel should always request the underlying rationale for any licensing determination.

There is also a chance that the government has made inconsistent licensing determinations and classifications for a particular type of item, particularly if the requests are submitted by different parties. Licensing officers within the same agency have issued inconsistent opinions as to whether a specific item requires a license. To the authors' knowledge, this

has led parties in at least one instance to deliberately seek numerous determinations for the same item in an attempt to generate inconsistent classifications. Another disturbing example of the problems caused by inconsistent government licensing determinations occurred in *United States v. Roth*, discussed in further detail later in the chapter, in which four separate expert witnesses for the government testified to four different interpretations of the AECA's application to the defendant's conduct.[55]

Because the licensing officer would be a crucial expert witness at trial, defense counsel should seek to speak with the officer and examine the notes from the licensing determination at the earliest opportunity to test its validity. Counsel should also locate expert witnesses, perhaps former employees of the relevant licensing agency, to examine the licensing determination as early as possible.

It should also be noted that early in the investigation stage, parties can file their own classification requests with BIS or commodity jurisdiction requests with DDTC. By filing their own requests early in the case—prior to the agency itself making a licensing determination—the parties ensure that they present all the evidence needed to support a favorable licensing determination. Moreover, the parties get the opportunity to interact more directly with the classification personnel and sometimes even supply additional information that can inform the licensing review and assist in a comprehensive review by the agency.

(iii) Denied Party or Entity List Transactions

When the alleged violation is a transaction with a restricted party included on one of the various government lists,[56] possible defenses may be based on the frequent amendments to the lists, the inaccurate identification of the parties, and, in some cases, the limited nature of prohibited activities or the fact that the transaction was not subject to U.S. jurisdiction.

Defense counsel should closely scrutinize the particular entity's listing, including all of the surrounding details, the date of listing in comparison to paperwork underlying the transaction, how the party was described, and the rationale for the listing. A company should be able to describe the measures it took to avoid dealing with a prohibited party, including its screening procedures for business partners and customers. If the prohibited party misled the company as to its identity or restricted status, the company may have a valid defense to criminal charges. Transacting business with a

prohibited party is, however, a strict liability offense and a company may be subject to administrative penalties regardless of knowledge. Accordingly, cooperation with the government may be the best mitigation.

(b) Culpability Challenges

If it is clear that a violation of the economic sanctions and export controls regulations occurred, every effort must be made to determine whether the company or particular individuals acted willfully or recklessly in violating those laws. If the government feels that the violations were deliberate or willful, the case could be prosecuted criminally and will involve much higher penalties and the possibility of imprisonment for culpable individuals. By contrast, liability in administrative cases does not turn on intent and is subject to a strict liability standard.

In criminal cases, where the government must prove intent and willfulness, its burden of proof is heavy, particularly in view of the complexity of the economic sanctions and export control laws.

In the 2019 DOJ VSD Policy, DOJ stated that, in economic sanctions and export control cases, the NSD uses the definition of willfulness set forth in *Bryan v. United States*,[57] a case involving not economic sanctions or export controls, but a federal firearms licensing statute. DOJ said under *Bryan* that "an act is willful if done with the knowledge that it is illegal. The government, however, is not required to show the defendant was aware of the specific law, rule, or regulation that its conduct may have violated."[58] Thus, a criminal prosecution can be based solely on an employee's knowledge that he was doing something unlawful, without knowing which particular law he was breaking.

The Supreme Court, however, has not ruled on the meaning of "willfulness" in the criminal provisions of economic sanctions and export control statutes so while some circuits have applied the intent standard used in *Bryan* to such cases,[59] other courts have adopted a heightened standard that requires specific intent to violate a known legal duty in this context.[60] An argument can be made, therefore, that the economic sanctions and export control laws and regulations are "highly technical statutes" and a heightened standard of intent should apply. There are a series of factors relevant to the determination of intent, including a company's licensing history for a particular item, the quality of the training a company provides

to its employees, an employee's experience in economic sanctions and export controls, the sophistication of the employee, and the complexity of the licensing requirements. However, in *United States v. Roth*,[61] the Sixth Circuit dismissed the defendant's argument that the prosecution had to prove that the defendant knew that the items exported were on the USML, rather than simply knowing that the underlying action was unlawful.[62] The Court held that the AECA "only requires knowledge that the underlying action is unlawful."[63] The court contrasted export control laws to tax laws, which require specific intent because they can be unintentionally violated by uninformed citizens, whereas "exporting defense articles can only be achieved by educated parties with atypical access to proprietary military weapons, systems, and data."[64]

Beyond the very real possibility of a misinterpretation of these complex laws, a defendant's reliance on flawed legal advice would indicate a lack of willfulness and diminish the appeal of a case in a prosecutor's eyes, as well as in the eyes of a judge and jury. In addition, several cases involving the TWEA and the Cuban sanctions program demonstrate the willingness of courts to consider the context of the defendants' activities in assessing intent (although they have been decided in a federal court circuit that has applied a heightened intent standard).[65]

More information for these and other defenses under the AECA and IEEPA (and, by inference, ECRA) are provided in the American Law Reports.[66]

(c) Mitigating Circumstances

In administrative cases where a company knows that it has committed a violation of the economic sanctions or export controls laws and is unable to defend its conduct, relevant guidance recognizes several mitigating factors that companies should still raise, including:

- Submitting a VSD;
- Having an effective economic sanctions and export controls compliance program in place or instituting a program to reduce the likelihood of future violations;
- Concluding that the violation was an isolated occurrence, involved a small portion of the company's business or resulted from a good-faith

misinterpretation of the regulations;
- Noting that the agency likely would have granted authorization if requested;
- Emphasizing that there were no prior violations, settlements, warnings, or similar;
- Cooperating with the government investigation; and
- Showing that the violation did not cause the type of harm at which the regulations were aimed.[67]

While all of these factors can have a mitigating effect on penalties imposed by the various agencies, each agency follows its own guidelines for imposing charges. For example, in 2016, BIS amended its Enforcement Guidelines identifying aggravating, mitigating, and general factors (which could be either aggravating or mitigating).[68] A company's adoption of new or more effective controls to prevent reoccurrence of violations in the future can be a mitigating factor when, or if, it comes to a regulator's imposition of penalties.

6.8 Case Studies

The following are recent export control prosecutions that highlight particular issues discussed earlier:[69]

(a) ***United States v. Ali Sadr Hashem Nejad ("Sadr")***

The U.S. government's criminal case against Sadr, a U.S. resident, related to a large construction project in which an Iranian company owned by Sadr's father built low-income housing in Venezuela and was paid in U.S. dollars by the Venezuelan government for those legitimate construction services. The construction company was privately owned and neither Sadr nor his father nor any of the companies involved was tied to the Iranian government, or designated as a Specially Designated National (SDN) by OFAC. The project payments were sent from Venezuela's foreign banks to bank accounts of two non-Iranian companies in Switzerland, and no money was ever transferred to or through Iran. In the indictment, the prosecution referred to these two non-Iranian companies as "shell" companies.

The prosecutors argued that Sadr caused the prohibited export of financial services from the United States to Iran based solely on correspondent banking transactions: the instantaneous electronic "clearing" by U.S. intermediary banks of foreign bank-to-bank wire transfers, which purportedly benefitted companies and individuals in Iran. Sadr testified that he thought the sanctions applied to the Iranian government, SDNs, and certain military, nuclear or petroleum-related transactions, not to private businessmen doing business outside Iran who kept their assets outside Iran. The prosecutors did not accept this argument, and ultimately, the jury convicted on five of the six counts in the indictment.

However, this was not the end of the case. Post-trial *Brady* disclosures by the U.S. government of evidence in the government's possession showed that the prosecutors had failed to disclose material exculpatory evidence, including evidence demonstrating that OFAC itself had not initiated enforcement proceedings against Sadr or anyone associated with the project, despite knowing of the bank transactions years before DOJ initiated its investigation. This evidence showed that OFAC apparently made an informed decision not to pursue Sadr or the intermediary banks, notwithstanding its full knowledge of DOJ's allegations and its theory of prosecution, thus, indicating possible difference of opinion within the government as to the seriousness of the conduct and the ambiguity of the law.

Following these disclosures, the government decided not to oppose Sadr's motion for a new trial and sought instead to drop the case. In response, the Court demanded an explanation for this unusual request and a full accounting of the government's disclosure violations and misrepresentations to the court.

On July 17, 2020, the Court dismissed the indictment with prejudice in an extraordinary order that ended the case. This case raised important tactical issues in handling a government prosecution. OFAC's decision not to pursue the allegations could have been influential in convincing DOJ not to pursue the case to trial, in framing the defense strategy at trial,[70] and certainly, for cross-examining the OFAC case official who testified that OFAC viewed these as clear violations and had OFAC known of the transactions, under its strict liability policy, an investigation would have been required. As a tip: when the regulatory agencies are not part of the

DOJ investigation, pretrial inquiries about their absence may yield helpful information about the validity of the case.

(b) *United States v. Eric Baird*[71]

Eric Baird, the former CEO of a Florida-based package consolidation and shipping service, Access USA, pled guilty on December 12, 2018, to one charge of smuggling[72] and on December 20, 2018, agreed to pay BIS a fine of $17 million, the largest administrative penalty imposed on an individual ($7 million was suspended), and to accept a five-year denial order.[73] The company had previously settled with BIS for $27 million, with all but $10 million suspended, in February 2017.

According to BIS, Baird developed and oversaw Access USA's business model, which offered non-U.S. customers a U.S. address from which to purchase U.S.-origin items and a "personal shopper" service to disguise non-U.S. sales as domestic sales and altered values and descriptions of exported items (e.g., describing firearm laser sights as "tools and hardware") to assist their customers in evading export controls. When warned by the Chief Technology Officer that he knew "we are WILLINGLY AND INTENTIONALLY breaking the law" (emphasis in original) by reducing the value of items by 25 percent, Baird said they could stop, if "warned by the government." BIS highlighted Baird's individual involvement in the company's deceptive practices. Not only did BIS send a message about individual culpability, BIS also focused on the importance of shipping and freight forwarding companies taking sufficient compliance steps to "prevent potentially dangerous items from reaching the hands of [U.S.] adversaries."[74]

(c) *United States v. FLIR Systems, Inc.*[75]

After a lengthy investigation and negotiation, in April 2018, the State Department and FLIR Systems, Inc. settled numerous ITAR charges. The charges include the unauthorized export of ITAR-controlled defense articles, technical data, and defense services to non-U.S. employees overseas; failure to obtain or comply with required export authorizations; failure to report fees and commissions related to the sale of defense articles; misrepresentations or omissions of material facts in ITAR license

applications; and recordkeeping violations. The 347 proposed charges could have resulted in civil penalties of almost $400 million, as well as debarment.[76]

Instead, FLIR and DDTC entered into an agreement resulting in a reduced civil penalty of $30 million, which could be further offset by $15 million for pre- and post-settlement compliance costs.[77] The settlement also included imposition of an external monitor, compliance enhancements, and two external audits. The ultimate penalty and waiver of temporary debarment indicates the value DDTC places on cooperation.

The *FLIR* case illustrates a number of key trends in DDTC enforcement. First, the case appears to have begun in response to a series of voluntary disclosures that DDTC saw as evidence of systemic compliance issues, including repeated disclosures of the same type of violation. When disclosing potential violations of U.S. export control laws, it is important to consider and address any root causes underlying those violations, and to follow through on all corrective actions offered in the disclosure.

Second, many of the alleged violations involved transfers of technical data and defense services to non-U.S. employees of FLIR affiliates based outside the United States. Of the 23 industry settlements in ITAR enforcement since 2010, 16 have involved alleged transfers of technical data as a prominent element of the charges.[78] This case emphasizes the need to manage access by non-U.S. employees to that data, and to ITAR-controlled defense articles as a whole.

Third, the proposed charging letter cites FLIR's alleged lack of a well-developed export compliance program and senior management oversight as aggravating factors. The penalties may have been lower if FLIR had been able to demonstrate those elements in its response to DDTC's investigation.[79]

Finally, the *FLIR* settlement illustrates DDTC's ability to dramatically increase a company's ITAR risk exposure by adding recordkeeping and "fee and commission" reporting violations to basic unauthorized export charges. When considering a suspected violation, companies should include the potential for such ancillary violations in their internal investigation and manage the compliance risk they pose accordingly.

(d) *United States v. ZTE Corporation*[80]

In March 2017, ZTE entered a guilty plea and agreed to pay a total of $892,360,064, with an additional $300 million suspended, to DOJ, BIS, and OFAC in a global settlement, resolving a six-year investigation.[81] This remains the largest penalty ever imposed in an economic sanctions and export controls investigation, and followed BIS's decision to place ZTE on its Entity List even while the company was already cooperating and negotiating with the government, the first time BIS has exercised such authority to force cooperation, but not the last. That action cut off the company's access to critical U.S.-origin components and technology during the pendency of negotiations. The outcome of the negotiations, therefore, depended on BIS agreeing to issue the first-ever Temporary General License, conditioned on BIS's satisfaction with the company's ongoing cooperation.

The combined global settlement required, among other things, that ZTE plead guilty to three criminal counts (an IEEPA violation, obstruction of justice, and false statements), to accept seven years of corporate probation and an independent corporate compliance monitor for three years, and to cooperate fully with other investigations by U.S. law enforcement authorities. Additionally, BIS imposed a Suspended Denial Order, which could be triggered for any noncompliance with the agreement and which could result in the addition of ZTE to BIS's Denied Persons List (as well as the imposition of the additional suspended $300 million penalty).

A little under one year later, in March 2018, ZTE notified BIS that it had made false statements in two letters submitted to BIS regarding disciplinary action taken by the company against 39 employees. Although these misstatements were unrelated to economic sanctions and export controls violations—a fact missed by most subsequent media reports—BIS nonetheless activated the Suspended Denial Order, adding ZTE to the Denied Parties List. This imposed even more severe restrictions on ZTE's access to U.S.-origin components and technology, crippling ZTE's operations. To be removed from the BIS Denied Parties List, ZTE entered into a Superseding Settlement Agreement with BIS for an additional $1,761 million penalty, $400 million of which was suspended and placed into escrow by ZTE immediately after settlement.[82] ZTE also agreed to an additional monitor or "independent special compliance coordinator" reporting directly to BIS for a ten-year probationary period. During the ten-year period, ZTE remains subject to a Suspended Denial Order that can be

reimposed if ZTE does not fully comply with all the terms of the Superseding Settlement agreement.

The ZTE penalties speak to the egregiousness with which U.S. regulators and enforcement agencies viewed its conduct. According to DOJ, "while the investigation was ongoing, ZTE resumed its business with Iran and shipped millions of dollars' worth of U.S. items there. ZTE also created an elaborate scheme to hide the data related to these transactions from a forensic accounting firm hired by defense counsel to conduct a review of ZTE's transactions with sanctioned countries."[83] Thereafter, there was little margin for error or benefit of the doubt given to ZTE for what amounted to an oversight in imposing the full measure of employee discipline.

This case demonstrates that non-U.S. companies must be aware of the arsenal available to U.S. government agencies to further their investigations or enforcement objectives. Indeed, the BIS Entity List was used to encourage a non-U.S. entity to cooperate, notwithstanding legitimate jurisdictional and legal challenges and potentially conflicting foreign laws on state secrets and data privacy.[84] The subsequent placement on the BIS Denied Parties List was, yet another, use of the "stick" available to BIS to punish behavior it characterized as egregious, resulting in a second record-breaking settlement and an additional monitorship—both costly consequences to non-compliance with U.S. laws for a non-U.S. company.

A non-U.S. company should weigh carefully its strategy and approach to a U.S. government investigation, particularly while the investigation is ongoing. It is important to be absolutely truthful with the facts and to discuss and fully understand all potential outcomes resulting from corporate decisions.

(e) *United States v. Schlumberger Oilfield Holdings Ltd.*[85]

On September 27, 2021, Cameron International Corporation, a Houston, Texas-based subsidiary of Schlumberger, a Dutch oil and gas parts service provider, agreed to pay $1,423,766 to settle OFAC charges relating to services it provided in approving five contracts authorizing a Romanian subsidiary to provide goods to Russian energy firm Gazprom-Neft Shelf for an Artic offshore oil project in violation of the Ukraine-related sanctions. The same day, a former subsidiary of Schlumberger, Schlumberger Rod Lift (SRL), based in Frisco, Texas, agreed to pay $160,000 to OFAC to settle

potential liabilities relating to facilitating a shipment from Canada to a joint venture in China, and ultimately to Sudan.

Two of the Cameron contracts were approved prior to Schlumberger's acquisition of the company in April 2016 and three were approved thereafter, all of which came to light in connection with a post-acquisition compliance review and integration. The SRL conduct began in December 2015, shortly after Schlumberger had pled guilty in March 2015, paid $232,708,356 to DOJ and BIS, and agreed to a three-year period of probation for allegedly conspiring to violate IEEPA by willfully facilitating illegal transactions and engaging in trade with Iran and Sudan; in August 2016, Schlumberger also received a Finding of Violation from OFAC for the same conduct. After the 2015 and 2016 settlements, which were widely publicized, Schlumberger provided lengthy sanctions training, including a case study involving facilitation by U.S. persons.[86] The probationary period was extended following disclosure of the Cameron contracts for an additional year, and the company did not receive credit for voluntary disclosure since the terms of probation required disclosure. However, the company was given credit for cooperation despite the aggravating factor that the violations occurred despite the training while the company was on probation.

The *Schlumberger* cases demonstrate coordination between the U.S. agencies, successor liability for continuing conduct, and the potential liability of U.S. persons conducting prohibited activities through non-U.S. entities. Also noteworthy was the agencies' willingness to credit the company for cooperation, but not self-disclosure.

(f) *United States v. Fokker Services B.V.*[87]

The entry of the settlement against Fokker garnered significant media attention after a U.S. district court judge refused to accept DOJ's proposed Deferred Prosecution Agreement (DPA) with the company. Although the district court judge was reversed on appeal and ultimately accepted the DPA, the case presents important lessons regarding VSDs and the impact of focusing on compliance and remediation.

In 2010, Fokker voluntarily disclosed to OFAC and BIS that it had possibly violated U.S. economic sanctions and export controls laws by selling aircraft parts to customers in Iran, Sudan, and Burma (Myanmar).

Despite the agencies' stated general practice not to refer voluntarily disclosed violations for criminal prosecution due to the potential chilling effect on self-disclosures, BIS denied that the case qualified for VSD credit, and referred the case to DOJ. Both DOJ and OFAC disagreed with BIS's position regarding VSD credit, and agreed that Fokker had self-disclosed and deserved mitigation credit following a four-year investigation in which Fokker cooperated fully with the U.S. agencies to reach a settlement agreement. The agreement was based on the total value of the illegally exported aircraft parts, many of which were low value and subject to low EAR controls.

After the DPA was agreed, the district court judge criticized it, saying the $21 million penalty did not fully capture the illicit activity, DOJ did not include penalties for individual actors, the 18-month probationary period was too brief, and an independent monitor should have been imposed rather than allowing self-reporting to ensure compliance. Both Fokker and DOJ appealed, and the appeals court struck down the lower court's decision, remanding it for further consideration. The judge subsequently accepted the DPA on remand.

While the case is notable for its procedural history in the D.C. federal courts, the case is also an illustrative example of how a company effectively cooperated and immediately implemented significant remedial steps, which allowed it to minimize long-term company commitments to DOJ (e.g., a monitor) and won DOJ's public praises for its "noteworthy" and "exemplary" compliance program.[88]

(g) *United States v. Weatherford International Limited*[89]

In November 2013, Weatherford, a Swiss oil services company, and four of its subsidiaries, agreed to pay penalties totaling $100 million for economic sanctions and export controls violations, including $48 million pursuant to a DPA, $2 million in connection with the guilty pleas of two of the subsidiaries and $50 million to BIS. A $91 million penalty to OFAC was deemed satisfied by payment of the fines to DOJ and BIS. This global export controls settlement was part of a combined larger Foreign Corrupt Practices Act (FCPA) settlement, which was resolved with an additional DPA with the parent company, guilty pleas by other subsidiaries, and a settlement with the U.S. Securities and Exchange Commission, resulting in

additional criminal and civil fines and other penalties, bringing the total penalties to $252 million.

According to DOJ, Weatherford and some of its subsidiaries and U.S.-based-management participated in foreign subsidiaries' unlicensed export or re-export of U.S.-origin goods to Cuba, Iran, Sudan, and Syria generating approximately $110 million in revenue from its illegal transactions.[90]

The *Weatherford* case is an example of the overlap in regulatory enforcement, where agents and prosecutors originally focused on one regulatory regime uncovered violations of other criminal laws. This convergence of compliance weaknesses in a company's anti-corruption controls and its economic sanctions and export controls compliance program is not unusual, and there are other cases where such overlapping enforcement has occurred. Accordingly, companies conducting internal investigations of economic sanctions and export controls noncompliance may wish to consider if there may be connected or tangential bribery, money-laundering, customs, anti-trust, or other violations.

(h) *United States v. BAE Systems plc*[91]

The investigation and prosecution of British-based defense contractor BAE Systems plc is another example of the overlap between U.S. regulatory enforcement regimes, and also illustrates interactions between U.S.-enforcement authorities and those from other jurisdictions. The 2010 U.S. and UK criminal settlements arose from a long-running investigation of alleged corruption in various BAE deals. The UK Serious Fraud Office (SFO) was forced to abandon much of its initial investigation of corruption allegations under geopolitical pressure. The DOJ investigation then came to the fore, and resolved allegations of impropriety with a settlement and guilty plea in February 2010. The U.S. Department of State, which was not a party to the DOJ settlement, resolved its own investigation more than a year after the DOJ settlement. Ultimately, the company paid over $500 million in criminal and administrative fines as a result of these investigations.

As part of the U.S. settlement, BAE pled guilty to conspiracy to make false statements to the Departments of Defense and State under the AECA based on: (1) false representations made regarding the due diligence and compliance measures BAE said were in place to handle its newly-acquired

defense businesses in the United States, which were circumvented for payments made to agents through offshore shell companies; and (2) failure by BAE to proactively inform a third party of payments made to secure sales of that party's products, causing the third party to submit false export applications to DDTC.[92] According to the State Department, those payments were required to be disclosed as part of the ITAR licenses that authorized the sales.

Soon after the plea agreement was announced, DDTC issued an administrative hold on most of BAE's export licenses so DDTC could consider whether to take additional action against the company. Although the hold was subsequently withdrawn, DDTC delayed its issuance of licenses for many BAE programs for the next year, until BAE entered into a Consent Agreement with DDTC and agreed to pay $79 million in penalties over the next four years. DDTC ultimately charged BAE under the ITAR's brokering and fee and commission reporting regulations and related recordkeeping requirements[93] mandated by ITAR Parts 129 and 130.[94]

The *BAE* case demonstrates the importance of cooperation across jurisdictional authorities when undertaking an investigation, considering whether to disclose, and structuring a settlement. Moreover, this case illustrates an additional overlap between the FCPA and the ITAR, besides the mutual compliance weaknesses that led to the Weatherford prosecution. The *BAE* case highlights the deliberate integral regulatory overlap in the ITAR's brokering and fee and commission provisions which seek to advance the FCPA's anti-corruption objectives in the context of defense trade. Because failure to report is easier to prove than bribery, prosecutors likely will continue to avail themselves of this regulatory overlap. Once again, counsel should assess the potential for anti-corruption violations in relation to both the ITAR and the FCPA when conducting an internal investigation in either context.

This case demonstrates DDTC's discretion in using both novel interpretations of the regulatory text and admittedly imprecise assumptions about the underlying facts. In ITAR practice, a company can rarely count on effective judicial oversight due to DDTC's extensive discretion to interpret the ITAR. In fact, there is judicial deference given to all of the regulatory regimes outlined earlier.

(i) *United States v. Latifi*[95]

In the cases against Alex Latifi and his company, Axion Corp, and against Professor John Reece Roth,[96] the defense challenged the U.S. government's assertion of willfulness to violate the ITAR. The acquittal of Latifi and Axion is an example of an effective defense at trial, while Professor Roth's challenge on the issue of intent was ultimately unsuccessful at trial and on appeal.

Latifi was charged with knowingly and willfully exporting technical drawings of a Black Hawk helicopter component to China without a DDTC license, making false representations to the U.S. Army, and submitting false test reports.[97] In October 2007, Latifi waived a jury trial and after witness testimony, the judge granted the defense's motion for acquittal.

According to Latifi's defense counsel, the dismissal was granted because the technical drawings given to Latifi by the government that were allegedly illegally transferred to China did not contain AECA warnings, were labeled "unclassified" and "uncontrolled," and did not indicate that the Department of Defense, rather than the manufacturer, owned the drawings —all of which negated any possible notice to contractors that the drawings contained export-controlled information. Moreover, evidence was introduced that the U.S. government had sold the Black Hawk helicopters and its components to China, making the drawings unnecessary for reverse engineering, and that the drawings themselves were widely available on the internet.

The government's documents failed to put Latifi on notice and may have misled him into thinking that they were unrestricted such that the government could not carry its burden of proving intent. This case highlights the importance of conducting a thorough investigation of the facts and of challenging the government's contention that an item is controlled under export control laws.

(j) *United States v. Pulungan*[98]

Doli Syarief Pulungan successfully appealed his AECA conviction for willfully attempting to export defense articles (riflescopes) without a license. In overturning the conviction based on the lack of requisite intent, the Seventh Circuit also confirmed that the classification of an item as

"manufactured to military specification" by an agency is subject to challenge. The Court stated that the agency's "claim of authority to classify any item as a 'defense article,' without revealing the basis of the decision and without allowing any inquiry by the jury, would create serious constitutional problems."[99] The Court also expressed concern that an unnamed official using unspecified criteria "that is put in a desk drawer, taken out only for use at a criminal trial, and immune from any evaluation by the judiciary, is the sort of tactic usually associated with totalitarian regimes" and stated that the government "must operate through public laws and regulations."[100]

This case highlights the importance of both regulatory and legal arguments in defending an export control case and offers avenues for the defense to challenge an agency's licensing determination or classification decision where it lacks proper foundation.

(k) *United States v. Anming Hu*

In February 2020, DOJ lost a high-profile trial against a University of Tennessee, Knoxville engineering professor Anming Hu, who allegedly hid his relationship with a Chinese university while receiving funding from NASA, and was charged with three counts of wire fraud and three counts of making false statements.[101] This case was part of a DOJ program, the so-called China Initiative, which was designed to crack down on economic espionage and unauthorized technology transfers.[102] In actuality, few of the cases brought pursuant to the China Initiative involve actual technology transfers but rather result in plea deals based on false statements or wire fraud.[103] The jury in Hu's trial deadlocked in a three-day deliberation in June 2021 after the defense counsel exposed the investigating agent's conflicted testimony and the government's failure to prove intent. When the prosecutors re-filed the charges, the Judge acquitted Hu of all charges in September 2021.[104] Judge Varlan wrote in a 52-page memorandum opinion, which serves as a guide for challenging such cases, that "the government has failed to provide sufficient evidence from which any rational jury could find, beyond a reasonable doubt, that defendant had specific intent to defraud NASA by hiding his affiliation with BJUT [Beijing University of Technology] from UTK [University of Tennessee, Knoxville]."[105]

Notably, in regard to the wire fraud charge, the Court held that there was "no evidence that defendant had a scheme to *defraud* NASA." The Court pointed to the fact that although the defendant had not disclosed his links to BJUT in forms submitted to the University of Tennessee, his affiliation was well-known and there was no evidence to suggest that this failure to disclose was made with the intent to defraud NASA. The Court also noted that the forms submitted to the University of Tennessee were submitted years before the request for NASA funding, which in any event was submitted by another professor and not by the defendant.

In regard to the false statements charge, the Court's opinion stated that "because the government failed to adequately prove that defendant understood that his affiliation with BJUT violated NASA's China Funding Restriction, the Court concludes that no rational jury could find beyond a reasonable doubt that defendant knew that the certifications that he caused UTK to submit with the invoices for disbursement of funds under the JPL Subcontract were false."[106]

The major lesson from this case is that although criminal statutes provide prosecutors with additional tools for enforcement, they also require the prosecution to show knowledge and intent. This provides an opportunity for the defense, especially when it comes to the defendant's intent.

6.9 Conclusion

Navigating the labyrinth of economic sanctions and export controls laws requires a plan to address the consequences of violations should they occur. Quick and thorough investigations and informed analysis of the regulations and relevant statutes are key. If a company decides to voluntarily disclose or to settle a case, attention should be paid to the intricacies of each regulatory regime to ensure the most advantageous result. Finally, in mounting a challenge to the charges, the most important elements of an effective defense strategy include analyzing the highly complex statutory and regulatory framework, examining the assumptions made by the government, investigating the factual underpinnings of the case—especially in regard to intent—and creating a record of compliance to bolster the case for a favorable settlement.

1. Wendy Wysong and Ali Burney are Partners in Steptoe & Johnson's Hong Kong office. Since this Handbook was updated, Hena Schommer has moved to Hewlett Packard Enterprise as Global Trade Counsel, Nicholas Turner has moved to HSBC as a Managing Associate General Counsel in the Financial Crime Legal Advisory—Global Legal Function, and Anthony Pan has moved to the World Bank as Counsel, Integrity Compliance Specialist, Integrity Compliance Office, Integrity Vice Presidency (INT). Steptoe is grateful to these companies for allowing us to recognize their contributions to the ABA Export Controls and Economic Sanctions Handbook.

2. 15 C.F.R. pts. 730–774, as codified by ECRA (Aug. 13, 2018).

3. H.R. 5040, 115th Cong.

4. 22 C.F.R. pts. 120–130.

5. 22 U.S.C. § 2778.

6. 31 C.F.R. pts. 500–598.

7. 50 U.S.C. §§ 1701–1708.

8. *Id.* app. § 16.

9. U.S. Dep't of State, Directorate of Defense Trade Controls, In the Matter of: Keysight Technologies Inc. (2021), https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=98ebc0e51b35b0d0c6c3866ae54bcb80.

10. For similar reasons, a company should consider carefully before informing the recipient or other third parties about the potential breach, as this could alert unauthorized recipients to the sensitivity of material they received.

11. Upjohn Co. v. United States, 449 U.S. 383 (1981). An *Upjohn* warning should explain that the lawyer represents the company, not any individual employee, and therefore, the attorney-client privilege belongs to the company, not the employee, such that the company need not ask the employee for permission to disclose information that the employee provides in the interview.

12. *See* U.S. Dep't of Justice, Justice Manual (Justice Manual) § 9-28.1000 Restitution and Remediation (2018), https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-28.010.

13. Press Release, U.S. Dep't of State, State Department Concludes Settlement of Alleged Export Violations by Bright Lights USA, Inc. (Sept. 12, 2017), https://2017-2021.state.gov/state-department-concludes-settlement-of-alleged-export-violations-by-bright-lights-usa-inc/index.html; *see also* Proposed Charging Letter from Arthur Shulman, Acting Dir., Directorate of Def. Trade Controls, U.S. Dep't of State, to Daniel A. Farber, President, Bright Lights USA, Inc. (2017) https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=715d7289db99db0044f9ff621f961939. In the cases involving FLIR Systems, Inc. and Darling Industries, Inc., the respondents' mitigation measures were seen by the State Department as less comprehensive, resulting in a more modest level of mitigation. *See* Proposed Charging Letter from Jae E. Shin, Dir. of Compliance, Office of Def. Trade Controls Compliance, U.S. Dep't of State, to Gary Darling, President, Darling Indus., Inc. (2019), https://www.pmddtc.state.gov/?id=ddtc_kb_article_page&sys_id=384b968adb3cd30044f9ff621f961941.

14. Voluntary disclosures that are not considered to be timely filed may receive reduced cooperation credit, or none at all. The ITAR encourages disclosure "immediately after a violation is discovered." 22 C.F.R. § 127.12(c)(1). Voluntary disclosures filed more than a month or two after the violation is discovered are generally accorded less mitigation credit. *See, e.g.*, Shin, *supra* note 13, where the respondent was alleged to have disclosed the violation almost two years after discovery. DDTC treated this "delayed disclosure" as an aggravating factor in its penalty assessment.

15. 22 C.F.R. § 126.1(e)(2) ("Any person who knows or has reason to know of a proposed, final, or actual sale, export, transfer, reexport, or retransfer of [defense] articles, services, or data [to any embargoed or restricted country without proper authorization] must immediately inform the Directorate of Defense Trade Controls.").

16. *See* 15 C.F.R. §§ 736.2(b)(10), 764.2(e), 764.5(f). *See* Section 6.5(a) for a discussion of section 764.5(f) (GP-10 letters).

17. *See* 15 C.F.R. § 764.5(f)(1).

18. *See* 18 U.S.C. § 1001; *see, e.g.*, 15 C.F.R. § 764.2(g).

19. 15 C.F.R. § 764.5(a).

20. U.S. DEP'T of JUSTICE, Export CONTROL and SANCTIONS ENFORCEMENT policy for BUSINESS ORGANIZATIONS (Dec. 13, 2019) (2019 DOJ VSD Policy), https://www.justice.gov/nsd/ces_vsd_policy_2019/download; U.S. Dep't of Justice, United States Attorneys' Offices Voluntary Self-Disclosure Policy (Feb. 22, 2023), https://www.justice.gov/usao-sdny/press-release/file/1569411/download.

21. Please note that there are disclosure obligations under securities laws and state regulations if business with sanctioned countries would be material to investors, if potential violations of economic sanctions and export controls would be financially material, or in certain specific circumstances involving certain transactions with Iran and other designated entities. *See* Securities Exchange Act of 1934, 13(r). The Office of Global Security Risk of the Securities and Exchange Commission (SEC) monitors the required SEC filings of U.S. and non-U.S. companies that disclose business activities involving U.S.-sanctioned countries.

22. *See, e.g.*, 2019 DOJ VSD Policy, *supra* note 20.

23. *See, e.g.*, U.S. DEP'T of TREASURY, ACTEON GROUP OFAC SETTLEMENT (2019), https://home.treasury.gov/system/files/126/20190411_acteon_webpost.pdf. Although this case qualified as a VSD, OFAC found the violations to be egregious and penalized the company $227,500 and imposed compliance commitments.

24. 5 U.S.C. § 552.

25. *See* 15 C.F.R. § 764.5; 15 C.F.R. pt. 766 (Supp. 1) (BIS); 22 C.F.R. § 127.12 (DDTC); 31 C.F.R. pt. 501 app. A (OFAC); 2019 DOJ VSD Policy, *supra* note 20.

26. *See* 31 C.F.R. pt. 501 app. A.

27. *See id.* app. A(I)(I).

28. *Id.*

29. *Id.* app. A.

30. *See* U.S. DEP'T of TREASURY, A FRAMEWORK for OFAC COMPLIANCE COMMITMENTS (2019), https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf ("OFAC recommends all organizations subject to U.S. jurisdiction review the settlements published by OFAC to reassess and enhance their respective [sanctions compliance programs], when and as appropriate"); *see, e. g.*, *Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Kollmorgen Corporation; Foreign Sanctions Evaders Determination*, U.S. DEP'T of TREASURY (Feb. 7, 2019), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20190207.

31. 31 C.F.R. app. A(I)(I).

32. 15 C.F.R. pt. 766 (supp. 1).

33. *Id.*

34. *Id.* § 764.5(b)(3).

35. *Id.* § 764.5(c)(1).

36. *Id.* § 764.5(c)(2)(iii).

37. If a company is requesting additional time under 15 C.F.R. § 764.5(c)(2)(iii), it should explain (1) whether it began its investigation promptly; (2) whether it has been diligently investigating the facts and preparing its final disclosure; (3) whether it has taken appropriate interim compliance measures to mitigate harm and prevent a recurrence of the violation; and (4) its proposed timeline for completing the investigation.

38. *See supra* note 17.

39. 22 C.F.R. § 127.12(b)(2).

40. *Id.* § 127.12(a).
41. *Id.* § 127.12(c)(1).
42. *Id.* § 127.12(c)(2).
43. Justice Manual, *supra* note 12. At the time of publication, DOJ has not clarified whether and how the new United States Attorney's Offices' Voluntary Self-Disclosure Policy ("USAO VSD Policy"), issued February 23, 2023, will impact the NSD VSD Policy, but the principles are largely the same. See https://www.justice.gov/usao-sdny/pr/damian-williams-and-breon-peace-announce-new-voluntary-self-disclosure-policy-united. For more information about the USAO VSD Policy, see https://www.steptoe.com/en/news-publications/investigations-and-enforcement-blog/dojs-new-corporate-enforcement-policy-for-the-criminal-division-and-its-impact-on-cases-handled-by-other-divisions.html.
44. 2019 DOJ VSD Policy, *supra* note 20.
45. Press Release, Department of Justice Office of Public Affairs, Department of Justice Revises and Re-issues Export Control and Sanctions Enforcement Policy for Business Organizations (Dec. 13, 2019), https://www.justice.gov/opa/pr/department-justice-revises-and-re-issues-export-control-and-sanctions-enforcement-policy.
46. The 2019 DOJ VSD Policy adds a helpful footnote to this: "If a company makes a disclosure before it becomes aware of an ongoing non-public government investigation, the company will be considered to have made a voluntary self-disclosure." 2019 DOJ VSD Policy, *supra* note 20, at n.6.
47. *Id.*
48. Despite some statements by BIS officials to the contrary, the *Fokker* case, discussed in further detail in Section VIII, should be seen as a cautionary tale of a VSD resulting in a criminal referral and penalty for a company. *See* United States v. Fokker Services B.V., 79 F. Supp. 3d 160 (D.D.C. 2015), *rev'd*, 818 F.3d 733 (D.C. Cir. 2016).
49. 2019 DOJ VSD Policy, *supra* note 20.
50. The relevant penalties to be considered include those set forth under IEEPA, 50 U.S.C. § 1705; AECA, 22 U.S.C. §§ 2778–2780; and TWEA, 31 C.F.R. § 501.701 (all as frequently amended and adjusted for inflation); ECRA, H.R. 5040, 115th Cong. (2018); and 18 U.S.C. § 3571 (the alternative criminal fine provision). Note that penalty provisions are frequently amended, and penalty amounts are adjusted for inflation.
51. *See Civil Penalties and Enforcement Information*, U.S. DEP'T of TREASURY (Nov. 2, 2021, 4:30 PM), http://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx; BUREAU of INDUSTRY and SECURITY, ELECTRONIC FOIA (Nov. 2, 2021, 4:30 PM), https://efoia.bis.doc.gov/index.php/electronic-foia/index-of-documents/7-electronic-foia/227-export-violations; *Penalties & Oversight Agreements*, U.S. DEP'T of STATE (Nov. 2, 2021, 4:30 PM), https://www.pmddtc.state.gov/?id=ddtc_kb_article_page&sys_id=384b968adb3cd30044f9ff621f961941; U.S. DEP'T of JUSTICE, NAT'L SECURITY DIVISION (Nov. 2, 2021, 4:30 PM), http://www.justice.gov/nsd/.
52. *See* 15 C.F.R. pt. 766 (supp. 1); 31 C.F.R. pt. 501, app. A
53. *See* 22 C.F.R. § 120.2 ("The Arms Export Control Act (22 U.S.C. §§ 2778(a) and 2794(7)) provides that the President shall designate the articles and services deemed to be defense articles and defense services for purposes of this subchapter. . . . [Such] designations [] are made by the Department of State with the concurrence of the Department of Defense."); *see also* United States v. Martinez, 904 F.2d 601, 602 (11th Cir. 1990) (citing Baker v. Carr, 369 U.S. 186, 217 (1962)) ("The question whether a particular item should have been placed on the Munitions List possesses nearly every trait that the Supreme Court has enumerated traditionally renders a question 'political.'"); United States v. Helmy, 712 F. Supp. 1423, 1434 (E.D. Cal. 1989) and cases cited therein (explaining that given the sensitive national security concerns involved ". . . congressional failure to codify a meaningful opportunity to challenge the listing determinations made under the AECA or the EAA either before or after prosecution is not a violation of the defendants' constitutional rights."). *But see*

United States v. Pulungan, 569 F.3d 326, 328 (7th Cir. 2009) (explaining that the agency's "claim of authority to classify any item as a 'defense article,' without revealing the basis of the decision and without allowing any inquiry by the jury, would create serious constitutional problems"), discussed in detail later in the chapter at Section 6.8(j).

54. *See Pulungan*, 569 F.3d at 328 (explaining that the ITAR "deals with attributes rather than names"; therefore, the authority to designate articles and services only applies to those attributes listed on the USML and not specific names or models of those items).

55. Petition for Writ of Certiorari at 8, Roth v. United States, 565 U.S. 815 (2011) (Mem.) (No. 10-1220), 2011 WL 1336432, at *8.

56. *Consolidated Screening List*, export.gov (Nov. 2, 2021, 4:45 PM), https://www.export.gov/article2?id=Consolidated-Screening-List.

57. 524 U.S. 184 (1998).

58. 2019 DOJ VSD Policy, *supra* note 20, at n.2.

59. *See, e.g.*, United States v. Bishop, 740 F.3d 927 (4th Cir. 2014) (holding general knowledge that the conduct was illegal is sufficient to convict a person of a willful violation of U.S. export laws); United States v. Mousavi, 604 F.3d 1084, 1093 (9th Cir. 2010) ("[T]he term 'willfulness' requires the government to prove that the defendant was aware of the legal duty at issue, but not that the defendant was aware of the specific statutory or regulatory provision. . . . In light of these precedents, we conclude there is no basis for requiring the government to prove that a person charged with violating IEEPA and the ITR was aware of a specific licensing requirement."); United States v. Electro Glass Prods., 298 Fed. App'x 157, 160 (3d Cir. 2008) (quoting United States v. Tsai, 954 F.2d 155, 160 n.3 (3d Cir. 1992), *cert. denied*, 506 U.S. 830 (1992)) ("[T]he 'willfulness' element of the AECA is established '[i]f the defendant knew that the export was in violation of the law.' The Government does not need to prove the basis of that knowledge, or that the defendant was aware of the licensing requirement."); United States v. Homa Int'l Trading Corp., 387 F.3d 144, 147 (2d Cir. 2004) ("[T]o establish a 'willful' violation of a statute, the Government must prove that the defendant acted with knowledge that his conduct was unlawful." (alteration in original)); United States v. Quinn, 403 F. Supp. 2d 57, 61, 64 (D.D.C. 2005) ("The Court cannot accept defendant's view of the scienter requirement for the charged offenses. To do so would produce an absurd result: A defendant could readily admit that he knew his exact conduct was illegal, but could nonetheless avoid criminal liability by convincing a jury that he did not know precisely *why* his conduct was illegal because he was unfamiliar with the specific licensing requirement. . . . [T]he 'legal duty' of which the government must establish that defendants had knowledge does not include within its scope the OFAC licensing requirement, and therefore the government is not required to produce evidence that defendants possessed such specific knowledge in order to obtain a conviction here."); United States v. Dien Duc Huynh, 246 F.3d 734, 742–43 (5th Cir. 2001) (holding that there was sufficient evidence to support a conviction for willful violation of the Vietnamese trade embargo, where the defendant "knew that there was an embargo in place against Vietnam, and [a witness] testified that [the defendant] told him he was shipping goods to Vietnam by way of Singapore because of the embargo.").

60. *See, e. g.*, United States v. Piquet, 372 Fed. App'x 42, 49–50 (11th Cir. 2010) (holding that "[t]he government must prove specific intent for a substantive offense under § 2778," and that the 'requirement of willfulness connotes a voluntary, intentional violation of a known legal duty" and thus does not cover "innocent or negligent errors."); United States v. Elashyi, 554 F.3d 480, 505 (5th Cir. 2008), *cert. denied*, 558 U.S. 829 (2009) (holding that the *Bryan* standard applies in considering willfully dealing in property of a Specially Designated Terrorist, while requiring the government to prove that the defendants knew licenses were required with respect to the EAR violations).

61. 628 F.3d 827 (6th Cir. 2011), *cert. denied*, 565 U.S. 815 (2011) (Mem.).

62. In 2014, the court granted Professor Roth's motion to vacate his conviction for wire fraud and ordered that he be resentenced on the remaining convictions. United States v. Roth, Nos. 3:08–CR–

69–TAV–HBG–1, 3:12–CV–08–TAV, 2014 WL 29096 (E.D. Tenn. Jan. 2, 2014).

63. 628 F.3d at 835.

64. *Id.*

65. *See* United States v. Macko, 994 F.2d 1526, 1532 (11th Cir. 1993) (reasoning that the defendants' engagement in exporting, the fact that the regulations were widely and publicly available, and the defendants' attempts to hide their contacts with Cuba were illustrative in finding willfulness to violate the statutes). *But see* United States v. Frade, 709 F.2d 1387, 1391–92 (11th Cir. 1983) (reversing convictions of priests for assisting Cuban refugees in the Mariel boat lift because general awareness of unlawfulness was insufficient under TWEA).

66. *See* Fern L. Kletter, *Validity, Construction, and Application of Criminal Penalty Provision of Arms Export Control Act (AECA), 22 U.S.C.A. § 2778(c)*, 92 A.L.R. Fed. 2d 387 (2015); Barbara J. Van Arsdale, *Validity, Construction, and Operation of International Emergency Economic Powers Act, 50 U.S.C.A. §§ 1701 to 1707*, 183 A.L.R. Fed. 57 (2003).

67. *See* 15 C.F.R. pt. 766 (supp. 1); 22 C.F.R. § 127.12; 31 C.F.R. pt. 501, app. A.

68. *See* 15 C.F.R. pt. 766 (supp. 1).

69. Other summaries of export control cases may be found in the BIS publication "Don't Let This Happen to You!" and in DOJ's "Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases." *See* BUREAU of INDUS. & SEC. EXP. ENF'T, U.S. DEP'T of COMMERCE, DON'T LET THIS HAPPEN to YOU!: ACTUAL investigations of EXPORT CONTROL and ANTIBOYCOTT VIOLATIONS (last updated on Oct. 14, 2022), https://www.bis.doc.gov/index.php/documents/enforcement/1005-don-t-let-this-happen-to-you-1/file; NAT'L SEC. DIV., DEP'T of JUSTICE, SUMMARY of MAJOR U.S. EXPORT ENFORCEMENT, ECONOMIC ESPIONAGE, TRADE SECRET and SANCTIONS-RELATED CRIMINAL CASES (last updated Nov. 2019), https://www.justice.gov/nsd/page/file/1044446/download.

70. See Memorandum in Support of Defendant's Post-Trial Motion for Judgment of Acquittal or in the Alternative for a New Trial, United States v. Ali Sadr Hashemi Nejad, No 1:18-cr-00224, at 85 (AJN) (May 1, 2020), gov.uscourts.nysd.490694.336.

71. *In the Matter of Eric Baird*, 647 Norsota Way Sarasota, FL 34242; Respondent; 16-BIS-0002, 83 Fed. Reg. 65,340 (Dec. 20, 2018).

72. *See* Press Release, Dep't of Justice, Former Florida CEO Pleads Guilty to Export Violations and Agrees to Pay Record $17 Million to Department of Commerce (Dec. 14, 2018), https://www.justice.gov/usao-mdfl/pr/former-florida-ceo-pleads-guilty-export-violations-and-agrees-pay-record-17-million.

73. *In the Matter of Eric Baird*, 83 Fed. Reg. 65,340.

74. *See supra* note 72.

75. *In the Matter of FLIR Systems Inc.*, U.S. DEP'T of STATE, DIRECTORATE of DEFENSE TRADE CONTROLS, https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=1c78debfdb2d1b4044f9ff621f961988.

76. *See* Proposed Charging Letter from Michael F. Miller, Acting Deputy Assistant Sec'y, U.S. Dep't of State, to James J. Cannon, Chief Exec. Officer, FLIR Sys., Inc. (2018), https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=b67812ffdb2d1b4044f9ff621f961983.

77. *In the Matter of FLIR Systems Inc.*, *supra* note 75.

78. A list of DDTC's enforcement cases since 1978 can be found at *Penalties & Oversight Agreements*, U.S. DEP'T of STATE, DIRECTORATE DEF. TRADE CONTROLS (Nov. 2, 2021, 4:30 PM), https://www.pmddtc.state.gov/?id=ddtc_kb_article_page&sys_id=384b968adb3cd30044f9ff621f961941.

79. Compliance program deficiencies are called out as an aggravating factor in most of DDTC's recent proposed charging letters. *See, e.g.*, Jae E. Shin, *supra* note 13; Arthur Shulman, *supra* note 13; Proposed Charging Letter from Sue Gainor, Dir., Office of Def. Trade Controls Compliance, U.S.

Dep't of State, to Suzanne Wright, Chair of Bd./President, Microwave Eng'g Corp. (2016), https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=afedba89db99db0044f9ff621f9619f7.

80. Judgment, United States v. ZTE Corp., No. 3:17-cr-00120-K-1 (N.D. Tex. Mar. 22, 2017).

81. *See* Press Release, U.S. Dep't of Justice, ZTE Corporation Agrees to Plead Guilty and Pay over $430.4 Million for Violating U.S. Sanctions by Sending U.S.-Origin Items to Iran (2017), https://www.justice.gov/opa/pr/zte-corporation-agrees-plead-guilty-and-pay-over-4304-million-violating-us-sanctions-sending; U.S. Dep't of Treasury, Office of Foreign Assets Control, Settlement Agreement (2017), https://home.treasury.gov/system/files/126/20170307_zte.pdf; U.S. Dep't of Commerce, Bureau of Industry, Settlement Agreement (2017), https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/1659-zte-settlement-agreement-signed/file.

82. *See* U.S. Dep't of Commerce, Bureau of Industry and Security, Superseding Order (2018), https://efoia.bis.doc.gov/index.php/documents/export-violations/export-violations-2018/1181-e2556/file.

83. Press Release, U.S. Dep't of Justice, *supra* note 81.

84. BIS now uses the threat of the Entity List to force cooperation or face destruction, even in non-BIS enforcement actions. *See, e.g.*, Addition of an Entity to the Entity List, 15 C.F.R. pt. 744 (2018) (adding Fujian Jinhua Integrated Circuit Company to the Entity List). Docket No. 181010930–8930–01] RIN 0694–AH67, https://www.govinfo.gov/content/pkg/FR-2018-10-30/pdf/2018-23693.pdf. Besides BIS, other agencies have added companies to their restricted lists to encourage cooperation with DOJ investigations where jurisdiction is otherwise lacking. *See, e.g.*, U.S. Dep't of Energy, U.S. Policy Framework on Civil Nuclear Cooperation with China (imposing a presumption of denial on licenses to export technology to China General Nuclear (CGN) "until the U.S. Government is satisfied with CGN engagement on its indictment" for allegedly conspiring to steal U.S. nuclear technology) (Oct. 11, 2018), https://www.energy.gov/nnsa/articles/us-policy-framework-civil-nuclear-cooperation-china.

85. Plea Agreement, United States v. Schlumberger Oilfield Holdings, Ltd, No. 1:15-cr-00041 (D.D.C. Mar. 24, 2015) (No. 15-41).

86. Press Release, U.S. Dep't of Treasury, OFAC Settles with Schlumberger Rod Lift, Inc. for Its Potential Civil Liability for an Apparent Violation of the Sudanese Sanctions Regulations (Sept. 27, 2021), https://home.treasury.gov/system/files/126/20210927_SRL.pdf.

87. 79 F. Supp. 3d 160 (D.D.C. 2015), *rev'd*, 818 F.3d 733 (D.C. Cir. 2016).

88. Government's Supplemental Memorandum in Support of Deferred Prosecution Agreement Reached with Fokker Services B.V., United States v. Fokker Services B.V., 79 F. Supp. 3d 160 (D.D.C. 2015) (No. 1:14-cr-00121-RJL) (July 18, 2014).

89. United States v. Weatherford Int'l Ltd., No. 4:13-cr-00733 (S.D. Tex. Nov. 26, 2013).

90. *See* Press Release, U.S. Dep't of Justice, Three Subsidiaries of Weatherford International Limited Agree to Plead Guilty to FCPA and Export Control Violations (Nov. 26, 2013), https://www.justice.gov/opa/pr/three-subsidiaries-weatherford-international-limited-agree-plead-guilty-fcpa-and-export.

91. U.S. Dep't of State, Directorate of Defense Trade Controls, In the Matter of: BAE Systems plc (2011), https://www.pmddtc.state.gov/compliance/consent_agreements/pdf/BAES_CA.pdf.

92. Information at 6–8, United States v. BAE Systems plc, No. 10-cr-00035 (D.D.C. Feb. 4, 2010), https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2011/02/16/02-01-10baesystems-info.pdf.

93. Proposed Charging Letter from the U.S. Dep't of State to David Parkes, Co. Sec'y, BAE Sys. plc (May 2011), https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=a85d7205db15df00d0a370131f9619d9.

94. *Id.* at 5–6.
95. United States v. Latifi, No. 5:07-cr-00098-IPJ-PWG (N.D. Ala. Oct. 31, 2007).
96. 628 F.3d 827. *See* discussion earlier in the chapter, in Section 6.7(b).
97. Gov't Trial Memorandum at 7–10, United States v. Latifi, No. 07-cr-00098-IPJ-PWG (N.D. Ala. Oct. 31, 2007).
98. 569 F.3d 326 (7th Cir. 2009).
99. *Id.* at 328.
100. *Id.*
101. Press Release, U.S. Dep't of Justice, Researcher at University Arrested for Wire Fraud and Making False Statements about Affiliation with a Chinese University (Feb. 27, 2020), https://www.justice.gov/opa/pr/researcher-university-arrested-wire-fraud-and-making-false-statements-about-affiliation.
102. DOJ Press Release, Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage (Nov. 1, 2018), https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-espionage.
103. *See* Peter J. Toren, *Department of Justice's "China Initiative:" Two Year Recap* (Jan. 3, 2021), https://petertoren.com/2021/01/department-of-justices-china-initiative-two-year-recap/.
104. United States v. Hu, 3:20-CR-21-TAV-DCP-1 (E.D. Tenn. Sept. 9, 2021).
105. *Id.*
106. *Id.*

7

Export Controls and Economic Sanctions in the European Union

John Grayston and Peter Gjørtler[1]

7.1 The European Union

EU export controls and sanctions differ in several significant respects from U.S. export controls and sanctions, with which readers may be more familiar. Some of the most significant differences include:

- First and foremost, the United States is for these purposes a single country with a single set of institutions and bodies administering export control and sanctions matters. There may well be many such U.S. bodies but, in comparison, the EU operates its export control and sanctions regime with and through 27 member states, each one of which has its own foreign policy concerns and priorities. EU rules there may be, but implementation and enforcement are distinctly national procedures.
- Second, the United States is a very significant player in both the world of commerce and a leading nation in the manufacture of both military and dual-use items. This provides a clear focus for its administration of both sets of rules. In comparison, only some of the EU member states are significant players in the manufacture of and trade in military and dual-use items. This means that for a significant number of member states, the practical importance of these rules is much reduced with no or limited tradition of applying export controls or sanctions measures.

- Third, in the area of sanctions, the EU is a relative newcomer to the adoption and implementation of its own sanctions. The United States has a much longer track record in this area and, in particular, has been more willing to take a more openly extraterritorial approach to their adoption and enforcement.
- Fourth, as a result of the preceding, the United States has clearer and more consistent foreign policy than the EU. In addition, it regards sanctions and export controls as vital tools to enforce such policy objectives. In contrast, although the EU does now have a foreign policy coordination function, this works very much as a tool to create common ground between member states who often maintain and pursue significantly different national outlooks.
- Fifth, the way in which export controls and sanctions are administered in the United States involves greater complexity but more transparency than those applied by the EU.
- Finally, the United States has a well-earned reputation for much more vigorous enforcement and for imposing much higher financial penalties for breach than those applied by member states in the EU.

This chapter covers three main topics: EU rules on export controls for military items, EU export control rules for dual-use items, and EU sanctions. However, in order to understand the complexities of the EU system, we need to start with a section describing in more detail what the EU is and how it works in the areas of export controls and sanctions, areas that are the extreme edges of its competencies.

7.2 Overview

(a) What Is the European Union?

The EU currently has 27 individual member states. They are as follows: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.

Although outside the EU, the following countries have a close association with the EU: through the European Economic Area agreement

(EEA), Iceland, Liechtenstein, and Norway; and through the European Free Trade Agreement and various bi-lateral agreements, Switzerland. Finally, as a result of Brexit and the end of the Transition Period on December 31, 2020, the United Kingdom became a third country outside the EU but, at least initially, with laws and procedures identical to those of the EU. Unless otherwise stated, all of these countries are treated as third countries by the EU for the purposes of export control and sanctions.

As the EU legal order depends on the conferral of powers on the EU by the member states, the constitutional documents are of fundamental importance when considering whether or not the EU has the powers and if so using which procedures to take action. The EU works through the institutions set up under the treaties creating the EU—mainly the Treaty on the European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). For these purposes, the most important institutions are the EU Council, the EU Commission, and, from the lawyer's perspective, above all, the EU Court of Justice (CJEU).

The control of exports is an area in which the legal base or right to take action at the EU level has been contested, and despite considerable changes over the years remains partial rather than complete. The nature of the jurisdiction of the EU over export controls and sanctions can be summarized as follows:

- Control of exports of military goods remains a matter for national jurisdictions but with the EU providing the means to establish some basic level of harmonization of national measures.
- Since 1995, the EU has had the competence to legislate on export controls of dual-use goods.
- In relation to sanctions, since the adoption of the Treaty of Lisbon in 2009, EU member states have been able, through the procedures of the Common Foreign and Security Policy (CFSP), to coordinate the implementation of both international United Nations sanctions as well as increasingly the adoption of unilateral or additional EU measures.

(b) The Scope of EU Powers

The EU faces the same issue as most federal unions in deciding whether an issue is subject to state or federal law and thereby which body has the

power to take legislative action. In a federal union, that question is usually subject to the provisions of the federal constitution. For the EU this process involves a delicate balance between the fundamental treaties of the EU and the constitution of each member state. It is generally accepted that in cases of doubt or dispute, it is for the CJEU to interpret the boundaries of Union law and member state law. For the practitioner, this means that the question of whether an issue is subject to EU law is primarily to be interpreted on the basis of the EU treaties, that is, the Treaty on the EU (TEU) and the Treaty on the Functioning of the EU (TFEU), as well as the Charter on Fundamental Rights (EU Charter), which has the same legal value as the treaties. To this may be added the EU secondary legislation, essentially comprising Regulations, Directives, and Decisions, which all depend on the EU treaties for their validity.

(c) The Limits of EU Powers

As the competence of the member states is residual, it follows that any competence that has not been conferred upon the EU (whether exclusively or shared) remains within the exclusive competence of the member states. As a consequence, the principle of legality requires that each piece of EU legislation must state explicitly, in its preamble, the legal basis upon which it has been adopted, since it may otherwise be found constitutionally invalid for reasons of legal certainty.

CFSP is a special policy area outside the normal EU legislative procedure, where the member states also have a right of initiative, and where the European Parliament does not act as a co-legislator. Furthermore, the legal acts of the CFSP are, in principle, not subject to the jurisdiction of the CJEU. An exception is made for CFSP decisions that impose sanctions upon individuals, as the TFEU requires that in addition to a CFSP decision, a regulation must be adopted by the Council of Ministers to implement the decision within the EU. That regulation may be challenged by the persons concerned before the CJEU, and it has been accepted that the challenge may also address the legality of the CFSP decision.

(d) Different Forms of EU Measure

Once legislation has been adopted by the EU legislator, it will normally take effect from the publication in the Official Journal of the European Union

(OJEU), which is published free of charge and is now available only online.

The most federal EU measure is the regulation. Regulations derive their legal effects from EU law and are directly application in EU member states without the need for any implementing measures. Regulations may nevertheless require additional member state legislation, such as establishing the laws to impose criminal sanctions for violations of the EU regulation.

Directives are still very much EU measures, although they are slightly less federal. Directives direct, that is, require, member states to take national measures to implement the substantive provisions of EU law that have been agreed and set out in the text of the Directive.

Decisions of the EU institutions must normally be notified individually to their addressees and they are, as such, only binding upon the addressees. Decisions are often published in the OJEU for information purposes. Publication in the OJEU may also be used as a substitute for individual notification if the addressee cannot be reached or located.

These are the classical legislative measures adopted by EU institutions. To these we need to add a growing list of nonbinding “soft law” measures, which go by names that include “guidelines,” “explanatory notes,” “Best Practices,” and even “mere” opinions.

Guidelines set out the way in which the author, normally an EU Institution, interprets the procedures and substantive rules to be applied to give effect to existing policies or legislative measures. The Institutions need to do so without usurping the ultimate power of the CJEU, which is the only institution that has the power to interpret and provide rulings on the application of EU law.

Although Guidelines are not be legally binding provisions of EU law, in practice they can indeed become as rigid and binding as the most tightly drafted legal measures. Member states administrations striving to implement complex provisions of EU law do tend to regard such guidance as authoritative, even where the language of the guidance itself shows that this was not intended. On the other hand, the role of the EU particularly in the area of sanctions policy is one of coordination of national actions. Resorting to the use of soft law is therefore very necessary in order to secure greater consistency of application of EU measures across EU member states.

In particular, here we would specifically mention: the EU Council's "EU Best Practices for the Effective Implementation of Restrictive Measures"[2] and then the Opinions and Guidelines adopted by the EU Commission, most recently, for example, the "Commission Opinion of 19 June 2020 on Article 2 of Council Regulation (EU) No 269/2014" (sanctions against actions undermining the territorial integrity of the Ukraine).[3]

(e) The EU Customs Union

Of all the areas of activity of the EU, perhaps the most important for a work on export controls and sanctions are the rules creating the EU customs union. Within the customs union goods move freely across national borders without any customs event arising. At the external border of the EU, a uniform set of customs rules and procedures is applied to all exports and imports, including in particular the application of uniform customs duties through the application of the EU Common External Tariff.

This means that the same customs rules govern trade to and from third countries to all 27 member states. While all customs procedures are established at an EU level, actual imports and exports are managed by national customs services in each of the member states.

Thus, from inside the EU, when goods move between member states there will be no export and therefore no export control.[4] However for the United States, each such internal movement is still considered to be a movement from one third country to another third country, thereby engaging for example the rules on the re-export of dual-use goods.

(f) Where to Find the Legislation

As mentioned earlier, EU legislation mainly comes into effect through publication in the OJEU, which is now only published in an electronic format and on a daily basis (https://www.ojeu.eu/). Access to the publications of the OJEU is available through EurLex (https://eur-lex.europa.eu/homepage.html), which also covers case law of the CJEU.

Additionally, the judicial decisions of the CJEU are published on the website of the CJEU at https://curia.europa.eu/jcms/jcms/j_6/en/, which may also be reached through the website https://europa.eu/european-

union/law/find-case-law_en. Although rulings are translated into each of the EU's official languages, rulings will be immediately available in at least the language of the case and in French, the official internal working language of the CFEU.

In EurLex, each document also has a unique reference number, which may facilitate searches, and which is inherited from the preceding Celex database. The number is composed of the sector (1 for EU treaties, 3 for legislation, 5 for preparatory works, and 6 for case law), followed by the year of the act (four digits, year of submission for case law), a descriptor (R for Regulation, D for Decision, L for Directive, C for Court of Justice, and T for General Court) and the running number of the act (submission number for case law). References to specific articles, paragraphs, and subparagraphs may be added to the number in order to focus research.

(g) Key Websites

As set out earlier, the key website for practitioners seeking information about EU legislation and case law is EurLex (https://eur-lex.europa.eu/homepage.html), but equally important for case law is the website of the CJEU, where a search form is available (https://curia.europa.eu/jcms/jcms/j_6/en/).

For background information about legislative policy, past, present, and future, the websites of the EU Commission (https://ec.europa.eu/info/index_en) and the European Parliament (https://www.europarl.europa.eu/portal/en) are important. Additional information may be found at the website of the Council of Ministers (https://www.consilium.europa.eu/en/), as well as at the individual websites of the various bodies, offices, and agencies of the EU.

A number of private companies provide regular information on the activities of the EU. These include Agence Europe (www.agenceeurope.eu/en/about.html) and EURACTIV (www.euractiv.com).

7.3 EU Export Controls for Military Items

(a) What Is Regulated by the EU?

The ability of the EU to act in the area of military export controls would seem to be constitutionally limited given the language of Article 346 TFEU, which provides as follows:

> [A]ny Member State may take such measures as it considers necessary for the protection of the essential interests of its security which are connected with the production of or trade in arms, munitions and war material.

Member states generally considered that this provision excludes EU action in the areas of defense and the control of military goods. Notwithstanding, the EU and its member states have responded to the needs of commerce and efficiency by using the EU machinery to adopt a series of measures that provide some degree of harmonization of military export controls. In relation to military goods, the following are the key measures adopted by or through the EU:

- Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment;
- Directive 2009/43/EC on simplifying terms and conditions of transfers of defense-related products within the Community;
- Common Position 2003/468/on the control of arms brokering; and
- Common EU Military List.

(b) Where to Find the Regulations

(i) Common Position 2008/944/CFSP

The principal EU measure in relation to military items is the Common Position 2008/944/CFSP,[5] which sets out common rules concerning the export of military goods and technology. The objective of the Common Position is to push member states toward more consistent "European" application of their national rules.

At the heart of the Common Position is the creation of a list of eight criteria that are to be used by all member states when assessing applications for export licenses for military goods or technology.

Criterion One	International obligations
Criterion Two	Human rights

Criterion Three	Internal situation
Criterion Four	Regional stability
Criterion Five	Security of friends and allies
Criterion Six	Attitude to terrorism
Criterion Seven	Risk of diversion
Criterion Eight	Sustainable developments

The enforcement of these rules is essentially a political matter and concerns are frequently raised over a lack of consistency, failure to apply the procedures of the Common Position, the lack of any EU enforcement measures, and a general lack of transparency of the procedures.

Article 346 provides the answer. Decisions on military exports are matters for member states. It is not unusual, therefore, to find that exports from one member state may be denied whilst the same or similar items will receive approvals to export from another member state.

(ii) Intra-EU Defense Transfers

Directive 2009/43/EC simplifies terms and conditions of transfers of defense-related products within the Community.[6]

In terms of the usual rules and procedures of the EU, movements of goods or the provision of services within the EU are not considered to be exports. However, as defense falls outside the scope of the EU, these standard provisions of the Single Market do not apply to movements of defense items. Thus, all movements between EU member states of defense items are considered to be exports for the purposes of export control.

The title of the Directive gives the game away: it is about simplification of different national systems, not about creating a single set of national rules and procedures on dealing with military exports. Nevertheless, it is a most welcome addition.

In relation to intra-EU transfers, the Directive provides that prior authorization is required for the transfer of defense-related products between member states. The corollary to this commitment is that those member states, through whose territory the defense-related products pass, are not to require a further authorization. Bearing in mind that some member states impose both import and export license requirements for the

movement of military items, prior to the adoption of this measure, a movement would involve import and export license procedures for all member states through which an item was transported. The effect of the legislation is that only one transfer license is required to move goods from one member state to another irrespective of the number of member states through which the goods pass.

For the rest, the types of transfer licenses available (individual global or general), the conditions applied in the licenses, and the procedures to be followed are matters for each member state. Accordingly, significant differences in license and procedure will still exist.

(iii) Common Position 2003/468/CFSP of 23 June 2003 on the Control of Arms Brokering[7]

The purpose of the EU Common Position 2003/468/CFSP is to "control arms brokering in order to avoid the circumvention of UN, EU or OSCE embargoes on arms exports." Member states commit to creating a clear framework to control brokering activities, with core provisions being mandatory but with further provisions being optional only.

Arms brokering for which a license is required is defined as:

- Negotiating or arranging transactions that may involve the transfer of items on the EU Common List of military equipment from a third country to any other third country; or
- Buying, selling, or arranging the transfer of such items that are owned by a person or entity from a third country to any other third country.

Without going into the provisions of the Common Position the great detail, one of the illuminating elements is the distinction drawn as to the scope of coverage of the measures. The Common Position states in Article 2 that in relation to brokering activities, member states must "take all the necessary measures to control brokering activities taking place within their territory." Additionally, Article 2 calls on member states "to consider controlling brokering activities outside of their territory carried out by brokers nationally resident or established in their territory." Such additional controls are not however mandatory requirements. As a result, some member states assert the right to control brokering on an extraterritorial basis, whereas others do not.

Member states may also adopt rules to require arms brokers to register on an official register and/or to require such brokers to be licensed.

In terms of enforcement, member states are required by Article 6 to "establish adequate sanctions, including criminal sanctions, in order to ensure that controls on arms brokering are effectively enforced."

(iv) EU Common Military List

The EU Common Military List defines all those products that are considered to be military items and therefore subject to the procedures set out in Council Common Position 2008/944/CFSP.

The list is based on the definitions established under the Wassenaar Agreement and is, therefore, generally updated on an annual basis.[8]

In 2019, the EU Council updated the provisions of the Common Military List, which although remaining part of the political process under the EU Common Foreign and Security Policy was strengthened because:

> the Council recalls its commitment to *strengthening the control of the export of military technology and equipment* and to *reinforce cooperation and promote convergence* in the field of export of military technology and equipment within the framework of the Common Foreign and Security Policy. It does this through the setting, upholding and implementation of *high common standards* for the management of transfers of military technology and equipment by all member states (emphasis in original text).[9]

As confirmed earlier, it is the national controls on military exports that determine whether and, if so, what sorts of licenses can be applied for or used directly without further application. In general terms, all such national controls within the EU member states focus on the primary trigger of export control procedures being the export from the member state of the military item or technology.

When comparing these national regimes with the U.S. regime, we can see that the EU member states do not seek to extend the scope of their controls to cover the bread and butter subjects of U.S. export controls, namely, the rules on re-exports and on deemed exports. Although the more detailed comments set out later on the position for dual-use goods (see Section 7.4) are of general relevance to the position under military controls also, the practical reality is that these issues have to be assessed on a country by country basis.

(c) Who Is the Regulator?

If we consider the term “Regulator” to mean the entity capable of granting or rejecting license applications, then in all cases this will be the competent national export control authority, as the EU plays no role in the day-to-day licensing decisions in relation to specific exports.

National regulations will identify the Regulator or Regulators.

In terms of EU legislative initiatives, as these measures are adopted under the CFSP provisions of the EU Treaties, it would be best to regard the regulator (i.e., the entity proposing new measures) as being the EU Council of Ministers (i.e., the member states) and the European External Action Service (EEAS).

(d) How to Get a License

Transfer, brokering, and export license applications must be made on a national basis to the competent national authority.

(e) Key Website(s)

Key websites are essentially always the website of the national export control organization.

7.4 EU Dual-Use Controls

(a) European Union—Overview

The EU has had the powers to regulate the control of dual-use goods since the mid-1990s.

The EU’s first regulation on dual-use goods was adopted in 1994 (Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods). The current version of the EU legislation is contained in Regulation 2021/821 setting up a Union regime for the control of exports, brokering technical assistance, transit and transfer of dual-use items (“Regulation 821” or EUDUR).[10]

Regulation 821 entered into force on September 9, 2021, replacing Regulation 428/2009, which, even though amended substantially, had remained in force for more than a decade.

Being a regulation, the rules set out in Regulation 821 apply directly in national law as a matter of EU law. Thus, in theory, no additional implementing measures are needed. However, in addition to certain binding provisions, Regulation 821 also includes many provisions that provide options for member states to follow if they wish. This added to the fact that all licensing and all enforcement is national means that Regulation 821 does not provide that comprehensive federal structure of controls that is enjoyed by the United States.

(b) Where to Find the Regulations?

The text of Regulation 821 is very new nut has already been amended twice, with a consolidated version published for information purposes in the OJEU.[11]

The EU practice of adopting an annual updating regulation to Annex 1, the annex that lists which items are considered to be dual-use, means that the current version of Annex 1 is not that included with the text of Regulation 821. This can be found in Commission Implementing Regulation 2022/1, which entered into force on January 7, 2022.[12]

For general reference, the website of the EU Commission provides access to all relevant documents.[13]

(c) Who Is the Regulator?

EUDUR makes clear that the administrative application and enforcement of the EU rules on the export of dual-use items are to be carried out by the national authorities in the relevant member states. So, on a purely practical basis, the regulator will be the relevant national export control authority. Thus, as there are currently 27 EU member states,[14] there are at least 27 regulators in the EU. We have to say “at least” because in some member states, more than one authority is involved in the regulatory procedure, and in Belgium, competence for export control is managed at a regional rather than national level, so Belgium has three regulators, one for each of its regions.

A list of the current national authorities is published periodically by the EU Commission.[15]

In addition, saying that there are only national regulators is a bit of an oversimplification, as this does not recognize the role played by the European Commission in promoting the use of the Union General Export Authorizations (UGEAs). In a very real sense, these UGEAs are some of the only purely federal parts of the EUDUR. These general licenses are created by Article 12 EUDUR and are available to be used directly, subject to conditions, by all traders and exporters in all member states. So, at least in relation to the UGEAs, we should recognize that the EU Commission is also at least in part a regulator.

Finally, in its role of coordinator of EU policy and within the context of the EU Commission's work to bring greater consistency to the application of EUDUR, the EU Commission has started to publish guidance documents aimed at securing better consistency of application among the member states' national authorities.

(d) How to Get a License

Licenses are issued by the "competent" national export control authority.

To identify the competent national authority, we look to see where the exporter is established. If the exporter is not established in the EU, then we look at the member state where any of the contracting parties is established.

The definition of exporter is complex, being more than identifying the person who makes the export declaration. The exporter is defined for export control purposes as "the person who at the time the export declaration is accepted holds the contract with the consignee in the third country and has the power of determining the sending of the item outside the customs territory."[16]

This means that the exporter and therefore the competent national authority may be based in a member state other than that where the goods are located and from where the goods are exported. As a result, the EUDUR contains detailed rules imposing requirements on the lead national authority to inform and consult with all other member states involved in a proposed export. While necessary, these requirements impose additional procedural burdens which tend to prolong the often already lengthy licensing procedures.

(e) Structure of the Laws and Regulations

(i) International Treaties

The EU member states are members of the international agreements and conventions dealing with the control of dual-use items. These include the Australia Group, the Missile Technology Control Regime, the Nuclear Suppliers Group, the Wassenaar Arrangement, and the Chemicals Weapons Convention.

The EU itself is not a member of these groups but in addition to working through the member states may also have observer status.

(ii) EU Laws on Dual-Use Controls

As stated earlier, the EUDUR sets out the provisions of EU law on dual-use goods. The main provisions of the regulation are set out in 32 (28) articles divided into ten (eight) chapters. The figures in parentheses show by way of comparison the numbers for Regulation 428. The chapter headings provide a useful overview of the content:

Chapter 1	Subject and Definitions
Chapter 2	Scope
Chapter 3	Export Authorisation and Authorisation for Brokering Services/Technical Assistance
Chapter 4	Amendment of Lists of Dual-use items and Destinations
Chapter 5	Customs Procedures
Chapter 6	Administrative Cooperation/Implementation/Enforcement
Chapter 7	Transparency, Outreach, Monitoring
Chapter 8	Control Measures
Chapter 9	Cooperation with 3rd Countries
Chapter 10	Final Provisions

These ten chapters and 32 articles are contained in the first 24 pages of the regulation. The remaining 437 pages are made up of the technical annexes, most notably the list of dual-use items in Annex I.

(iii) The EU Control List

The list of items subject to control is set out as Annex I to the EUDUR.

Annex I reflects, principally, the designations of dual-use items made by the international treaties and agreement referred to earlier. The annual updating of Annex I allows the EU rules to adapt to the changes made to these international agreements.

It is important to note that EUDUR also confirms that member states can maintain their own national control lists, which identify those non-Annex I items which are subject to dual-use export authorization requirements when exported from that member state.

(f) What Is Regulated: Scope of the EUDUR

Dual-use items are defined in Article 2(1) as:

> items, including software and technology, which can be used for both civil and military purposes, and includes items which can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery including all items which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices.

The Dual-Use Regulation then goes on to impose authorization requirements in relation to two lists of products: those contained in Annex I and those in Annex IV. Although the EUDUR always refers to the term "authorization," we will use the terms "authorization" and "license" interchangeably.

Article 3 contains two provisions: first it imposes a requirement for the prior authorization for export of dual-use items listed in Annex I; second, it confirms that an authorization may also be required by the member states in certain circumstances for exports of dual-use items not listed in Annex I.

These circumstances are set out in Articles 4, 5, 9, and 10 and can be summarized as follows.

In terms of procedure:

- Non-Annex I products may require a license where the exporter is informed by the national authorities that the items are or may be intended for a specified use.
- An exporter must notify the competent national authority in cases where it is aware of such intended use.

- Member states may however increase the scope of the obligation on exporters by requiring them to notify the national authority in cases where they merely suspect such an intended use.

In terms of the specified uses:

- Article 4 covers (1) Weapons of Mass Destruction uses, that is, “for use in connection with the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological or nuclear weapons or other nuclear explosive devices, or the developments, production, maintenance or storage of missiles capable of delivering such weapons”; or (2) for a defined military end use where the purchasing country is subject to an arms embargo; and (3) for use as parts or components for military items exported in breach of export controls.
- Article 8 extends the provisions of Article 4 to cover the provision of technical assistance that is or may be used for one of the Article 4 end uses.
- Article 5 concerns the export of cybersurveillance items that are to be used “in connection with internal repression and/or the commission of serious violations of human rights and international law.”
- Article 9 allows member states to control the export of any items on the grounds of public security, including the prevention of terrorism or for human rights considerations. This provision does not impose any obligation on exporters to notify the national authority in cases where they are aware or have suspicions of such end uses.
- Article 10 enables member states to impose their own authorization requirement in cases where other member states have refused export authorizations under their own national controls under the grounds set out in Article 9.

An important point to note is that a license is only required where dual-use goods are exported. The term “export” is defined in Article 2(2) by reference to the EU customs rules. It follows that as movements between EU member states are internal movements within the EU (in the same way as movements between U.S. states are not “exports”) that a license is not generally required for such internal movements.

The exception to this provision concerns those dual-used goods that are more sensitive and are listed in Annex IV of the EUDUR (see Article

11(1)). For Annex IV goods, a license is also required for internal movements between EU member states.

The EUDUR also includes provisions that address the boundaries of EU controls, how to deal with items that although physically located in the EU have not entered into free circulation and therefore do not require an export procedure to be used for the goods to leave the EU. A classic example would therefore be where goods arriving on a vessel that docks at an EU port, for example, Antwerp, are not unloaded (or if they are they are transhipped onto another vessel) and then leave the port of Antwerp for delivery to a customer in another country outside the EU, for example, Russia.

The EUDUR provides that member states may take actions to deal with dual-use items that have not been imported into the EU, that is, are not in free circulation but are either under a transit procedure or are in a free zone or customs warehouse. In particular, member states may take actions to prohibit the transit of such items where they have "reasonable grounds for suspecting" that the items are intended for use in whole or in part for the proliferation of weapons of mass destruction or the means of their delivery. These provisions are then set out in Article 7 of the EUDUR as follows:

- Article 7(1) permits (but does not oblige) member states in which the transit occurs to prohibit transit of dual-use items listed in Annex I where they decide that the goods are to be used for a WMD program as defined in Article 4(1).
- Article 7(2) confirms that member states may decide to authorize their national authority to grant individual licenses to permit such transits.
- Article 7(3) confirms that member states can extend the scope of such licenses to cover non-Annex 1 listed items.

Finally, as the scope of the EUDUR is limited to the control of "exports" of dual-use items,[17] we can make two further clarifications on what EUDUR does *not* control, clarifications which will be of particular interest to those well versed in the provisions of U.S. export controls:

- First, the EUDUR does not contain an express control on re-exports, that is, a control on the further sale/export of the goods initially exported whether or not incorporated into other products.

- Second, the EUDUR contains no provision which would create a requirement to obtain a license to cover deemed exports, that is, where controlled goods are supplied to a foreign (non-EU) national.

In both cases there are certain caveats to be noted.

In relation to re-exports, national authorities can and do include conditions in the terms of the export licenses granted, in particular in the End Use Certificates, which require the end user to commit to obtaining a further authorization from the national authority in the EU in the event that the EU items are to be sold/exported. Second, in certain circumstances the involvement of an EU entity in the sale of items in third countries could be covered by the EUDUR rules on brokering.

In relation to the absence of any provisions in EUDUR on deemed exports, similar controls may be applied through EU sanctions, for example, where the supply of dual-use goods to a national of the country subject to measures is prohibited. Such measures are not incorporated into all EU sanctions measures but are reserved for those cases where the EU wishes to impose the strictest and most restrictive of sanctions regimes.

(g) Who Is Regulated?

As an export license is required for exports of controlled items, it follows that the person required to obtain the license is the exporter. The exporter is the party responsible for both physical and intangible exports. For physical items, the definition is more complex than the basic definition for customs purposes, and involves the person who or on behalf of whom an export declaration is made. Article 2(3)(a) goes on to clarify that the exporter is "the person who, at the time that the declaration is accepted, holds the contract with the consignee in the third country and has the power for determining the sending of the item outside the [EU]." This definition becomes critical when we come to consider which national authority is competent to grant a license in relation to a given export.

In relation to exports of technology, the export is the transmission of software or technology by any electronic means (fax, email, etc.) to a destination outside the EU. In addition, it covers making available in electronic form such software or technology to persons outside the EU. Finally, an export also includes the oral transmission of technology to someone outside the EU by telephone.

EU export control rules also apply to “brokers,” defined as being any natural or legal person or partnership resident or established in a member state of the community. This means that companies or individuals who are neither resident nor established in the EU cannot be considered to be an EU-based broker. These rules then only apply where the broker provides brokering services, which are defined as follows in Article 2(7):

> the negotiation or arrangement of transactions for the purchase, sale or supply of dual-use items from a third country to any other third country, or the selling or buying of dual-use items that are located in third countries for their transfer to another third country.

Ancillary services (in relation to such goods) are excluded. Such services include the provision of transportation, financial services, insurance or re-insurance, or general advertising or promotion.

(h) Licensing/Reasons for Control

Although the licensing procedures are national, the EUDUR does impose obligations on how member states take decisions on whether or not to grant an authorization. Article 15(1) describes the responsibility of the member states as being “to take into account all relevant considerations.” It then lists four specific considerations that must be included in the relevant considerations of the member states:

- Commitments and obligations agreed and accepted as part of international nonproliferation regimes and export control arrangements;
- Obligations imposed by OSCE or United Nations sanctions measures;
- Considerations of national foreign and security policy including the Common Position agreed on the control of exports of military technology and equipment; and
- Considerations of intended end use and the risk of diversion.

(i) Types of Export Control Licenses and Permits for Dual-Use Items

Article 12(1) provides that apart from the Union General Export Authorization, national authorizations may be individual, global, or general. By using the word “may” it is clear that there is no obligation on member states to use all three types of license.

Indeed only eight out of 27 member states have adopted national general export authorizations. In six of these eight countries—Austria, Greece, France, Netherlands, Germany, and Italy—these national general licenses are in current use. However, in the other two countries with national general export authorizations, Croatia and Finland, although national enabling measures have been adopted to create national authorizations, they have not been used in practice.

There are also automatic authorizations created by EUDUR, the Union General Export Authorizations (UGEAs). UGEAs establish as a matter of EU law, general authorizations to export items to specified third countries. They are an example of pure EU export control law because they derive their force of law from the EUDUR itself and do not require any national transposition measures. They are automatically valid across all 27 member states.[18] There are currently eight UGEAs, numbered EU001 to EU008. In formal terms, the UGEAs are set out in detail in Annex II of the EUDUR.

The UGEAs cover the following issues:

EU001: exports of most but not all Annex I items to eight "friendly" countries including the United States of America
EU002: export of a limited list of Dual-Use Items to certain destinations
EU003: export after repair/replacement
EU004: temporary export for exhibition or fair
EU005: telecommunications
EU006: chemicals
EU007: intra-group export of software and technology
EU008: encryption

Each UGEA sets out the detailed conditions that need to be met in order for the export to be covered. The most obvious conditions are those that identify which items can be exported under the UGEA and to which third countries. For example, UGEA EU001 provides a general authorization to export all dual-use items listed in Annex I to the United States.[19] All that is required in order to rely on EU001 is (1) for the exporter to notify the relevant national authority no later than 30 days after the date on which the first export took place;[20] (2) a reference to the use of EU001 must be included in the customs export document (SAD); (3) EU001 cannot be used

if the exporter has been informed that the items in whole or in part are intended for a WMD program; (4) the items are intended for a military end use or for export to a country subject to an arms embargo of the EU, OSCE, or United Nations; and (5) that the items are not exported to a customs zone or free warehouse in the third country, that is, that the goods are indeed intended for end use in, for example, the United States.

The conditions applicable to the various UGEAs differ and therefore there can be no mixing and matching of conditions from the various licenses. Each UGEA defines a set of circumstances in which a license is automatically available; if all these conditions are not met an automatic license will not be available and an application for an individual license will be needed.

Even though UGEAs are established as a matter of EU law, it is a requirement that an exporter intending to rely on a UGEA registers with the national authority in the member state where it is established.[21]

(j) Export Control Licensing Procedure

Licensing procedures are national and therefore national procedures apply. Although these procedures may be substantially similar, there will be differences between each of the member states.

The EUDUR includes specific provisions that must be followed by the member states where the place of export of the items is different from the place in which the application for the export authorisation is made. The provisions of Article 14 require prior notification and consultation between the member states involved, adding both complexity and time required to complete the export authorization application and review procedure.

Where goods are located in a member state other than member state to which an application for authorization is filed, notice to and consultation with the member state where the goods are located must take place immediately. The member state where the goods are located then has ten working days to confirm whether an authorization should be granted and their view is then binding on the national authority reviewing the application.[22]

In addition, member states may inform the national authority of another member state that is reviewing an application—irrespective of the location of the items—requesting that a license be refused or revoked where the

authorization could "prejudice its essential security interests."[23] While not binding, the member state receiving such a request must engage in consultations with the member state issuing the request. Where a member state receives a request to deny or revoke a license but nevertheless authorizes the export, notice of such authorization must be provided to the Commission and all member states.

Finally, in Chapter V, the EUDUR sets out details of the Customs Procedures applicable to exports of dual-use items. The first and primary responsibility for an exporter is to provide proof to the customs office dealing with the export that the export is covered by an export license. This may require the exporter to provide translations of documents into the language of the exporting member state.

Member states are then permitted to suspend the export process—beyond the time permitted under EU Customs rules—where the member state has grounds for suspicion that either relevant information was not taken into account when the authorization was granted or that circumstances have changed since the authorization was issued.

Where goods are so detained and the authorization to export was granted by another member state, the member state carrying out the detention must immediately consult with the member state that issued the authorization. If the issuing member state maintains its position and confirms the authorization, the items must be released for export. Where the issuing member state agrees with the grounds for blocking the export, it will then use powers to revoke or modify the original authorization.

(k) Penalties, Enforcement, and Voluntary Disclosures

The EUDUR contains no detailed provisions on penalties or enforcement procedures nor on voluntary disclosure procedures. Instead, Article 24 provides that it is an obligation for member states to take necessary and appropriate measures to "ensure the proper enforcement" of the EUDUR. In addition, Article 24 requires member states to provide for penalties that are "effective, proportionate and dissuasive" to be established.

Thus, the detailed mechanisms for enforcement, the nature of the penalties and the procedures (if any) for voluntary disclosures are all established at a national level. It should come as no surprise, therefore, that

there are material differences in approach and procedure between the member states.

Experience suggests that there are still significant differences between EU member states in terms of the effectiveness of the enforcement of controls on dual-use exports. These differences are then further accentuated by differences in procedures and penalties such that enforcement outcomes may differ substantially across the member states. The nature of the EU system and the reliance on national controls without any corresponding federal control at the EU level make it hard to see these differences being eliminated anytime soon.

7.5 EU Sanctions

(a) European Union Overview

The use of sanctions by the EU as a tool of foreign policy has grown significantly over the last 20 years. Generally, this has been viewed as a success by member states, such that the EU is actively looking at how to improve the rather tortuous route by which such measures are adopted.

The success of EU sanctions has been a surprise to some observers because of the degree of constitutional difficulty the EU has in adopting measures that straddle foreign policy and trade. As described earlier, CFSP is a late addition to the EU's competence, giving the EU a role of coordination of national policies.

The key elements of the current EU system are as follows:

- Sanctions measures are initially adopted by the EU through the provisions of the CFSP, which sets out political rather than legal obligations on member states.
- Where the measures involve imposing limits on trade and commerce with third countries in addition to the CFSP measure, a further regulation is adopted under the provisions of Article 215 TFEU, which authorizes "the interruption or reduction, in part or completely, of economic and financial relations with one or more third countries."
- Whereas a CFSP decision is only politically binding upon the member states, an Article 215 Regulation is binding upon companies and citizens. The CJEU has held that as both sets of measures affect

the legal interests of the listed persons, listed persons or entities can challenge both the CFSP decisions and the TFEU regulations before the CJEU.

- As the EU approach to sanctions is to coordinate joint action, member states retain their traditional national rights to impose sanctions—and may do so where their national interests (rather than the combined interests of all EU member states) are impacted.
- Implementation and enforcement of sanctions, and the issuance of licenses or authorizations, is a matter for each member state.
- As a matter of policy, all EU sanctions are targeted, that is, designed on a case-by-case basis to achieve the specific objective of EU CFSP without causing unnecessary collateral economic damage. They are limited in scope to situations involving the EU or its citizens and, therefore, seek to avoid any pure extraterritorial application.

(b) Defining the Term "Sanctions"

The terms "sanctions" or "economic sanctions" are not used in the relevant EU legislative measures. Instead, the EU uses the term "restrictive measures." The legal basis in the EU Treaties on which "sanctions" measures are adopted is particularly wide and all-encompassing. In the TEU, Article 21(2) states that "The Union shall define and pursue common policies and actions, and shall work for a high degree of cooperation in all fields of international relations." Similarly, Article 24(1) confirms that "The Union's competence in matters of common foreign and security policy shall cover all areas of foreign policy and all questions relations to the Union's security. . . ." Thus, EU sanctions may be used in a wide variety of situations beyond the scope of UN Security Council resolutions.

EU sanctions are used:

- To implement binding resolutions of the UN Security Council (measures that each member state as a member of the UN must implement);
- To adopt additional measures by which the EU develops and extends the scope of UN sanctions (sometimes called gold plating or UN Plus measures); and
- To adopt unilateral EU measures that are not based on UN sanctions, whether or not such measures have been adopted in concertation or

coordination with other UN members.

Although sanctions are generally considered to be measures targeted against a specific country, an interesting recent example of a non-country-specific measure concerns action against anyone who is involved in cyberattacks that threaten the EU. These measures were adopted by the EU in 2019 pursuant to Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796.[24]

(c) Where to Find the Legislation

EU sanctions measures must be published in the normal way that EU legislation and decisions are published, that is, in the EU Official Journal, which is available at https://eur-lex.europa.eu/oj/direct-access.html.

As explained earlier, most EU sanctions measures require two sets of legislation to be adopted: a CFSP Common Position and an EU single market regulation. Both such measures are published in the EU Official Journal.

In addition, the EU uses the C series of the Official Journal to publish and give formal notice to entities affected by the adoption of measures.

The EU Commission maintains a webpage with information and details of all current sanction activities of the EU: https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures_en. This page includes a link to a database listing all current EU sanctions measures in force. To access the database, it is necessary to create a user account with the EU Commission. In the alternative, the Commission offers the opportunity to download a pdf of the list.

(d) Who Is the Regulator?

In the EU, there is a distinction between the procedures needed to adopt sanctions measures, that is, the legislative role, from administration and enforcement of sanctions measures.

The legislative role rests with the EU Council of Ministers, that is, the representatives of the national governments before the EU.

The administrative and enforcement roles are played by the competent national authorities of the EU member states. However, both the EU Council and the EU Commission provide “guidance” to these national

authorities and to third parties on how EU sanctions should be interpreted and implemented.

Each sanctions measure needs to be read and interpreted in its own context. Although the EU has sought to standardize the use of language and concepts, these terms may be used in different contexts or with additional limitations in a given measure. What follows is, therefore, a brief overview of the standard forms of procedure needed to reach the adoption of EU sanctions measures.

Where the measure in question concerns a UN measure or the adoption of UN Plus provisions, the point of departure will be the decision adopted by the UN Security Council, to which a reference will be made in the preamble of the EU measure seeking to comply with the UN decision. Where measures are adopted only by EU, the grounds for adopting measures will be recited, for example, some form of EU policy statement regarding the objectionable conduct of the targeted state, entities, or persons.

From a legislative perspective, the point of departure will typically be a decision made by the Council of Ministers acting under Article 29 TEU, within the field of CFSP. That decision may have been adopted based on the conclusions reached in a meeting of the European Council, comprising heads of state and government of the member states. In such case, a reference will also be made to the conclusions concerned.

Based on the decision made under Article 29 TEU, the Council will then adopt a regulation under Article 215 TFEU to ensure application within the EU.

(e) Structure of the Laws and Regulations

As confirmed already, each EU sanctions measure needs to be considered individually.

By way of comparison with U.S. measures, the EU takes a fundamentally difference approach to implementing sanctions. A typical U.S. approach would be to impose a general embargo on trade with a third country. Having imposed the full embargo, the U.S. authorities will grant exceptions to the embargo thereby permitting trade in defined and limited areas. The EU approach is in fact the opposite. The EU will, in almost all cases, not impose a general global embargo on trade with a third country.

Instead its sanctions measures will define those specific areas and activities that are prohibited. Outside the scope of the prohibitions, trade and commerce with the targeted country are permitted.

An EU sanctions measure will typically include some or all of the following provisions:

- The document will start with a series of recitals, which provide the evidence to show why and how the legislative measure complies with the requirements of the legal base for its adoption. In addition, the recitals will define the nature of the targeting measures to be adopted.
- The measure will then include a set of definitions that are needed in order to define the scope of the measures adopted. Care is needed to verify the scope of each such definition—even if it appears that it follows a standard formulation previously used in other EU measures.
- The measure will then set out a statement of what actions are to be prohibited. The prohibitions are generally set out in a series of separate articles covering each aspect of the targeted measures. It is also quite normal for the measures to include specific annexes listing in detail which goods or services are concerned by any export or import bans.
- Where the measures also involve a requirement not to deal with or provide benefits, directly or indirectly, to certain listed persons, the details of these persons or entities will be set out in an annex to the measures. The lists will include as much information as is needed in order to identify the listed person (e.g., full names, dates of birth, aliases, and other identifying information for individuals and, for companies or other corporate entities, full names addresses and company registration details).
- The measure will then set out the details of any exceptions or exemptions from the prohibition. It will also state who is authorized to deal with such exemptions—which will invariably be the competent national authorities. A list of the competent national authorities is then normally set out in an annex to the measure.
- The measures may then also include detailed provisions on the circumstances in which the national authorities are required to refuse a requested license. In order to ensure greater transparency between member states and with the EU Commission, the measure will normally require any member state who refuses to grant a license (or

cancels or suspends an existing license) to immediately inform the Commission and all other member states of this fact and to provide all relevant information.

- The measure may then also require any member state that intends to grant a license that has previously been denied by another member state, to inform and consult with the member states concerned, and, if it does decide to grant the license, it must inform all member states and the Commission of this decision.
- The measure will then require the member states to impose penalties for infringements of the rules and these penalties will need to be seen as "effective, proportionate and dissuasive." Detailed information on the relevant penalties has to be notified to the Commission.
- Finally, the measure will conclude with a provision stating to whom the measure applies. Typically this will include anyone within the territory of the EU; all nationals of the EU whether or not inside or outside the EU; all companies or legal entities incorporated within the EU in relation to their actions inside and outside the EU; any person or entity on board any vessel (plane or ship) that is registered in the EU; and all companies and other legal persons in respect of business done in whole or in part in the EU.

EU sanctions are also typically imposed for a limited period of time, and normally for periods of one year only. This means that the EU Council needs to review periodically the reasons for the measures and in particular the detailed reasons for the listings of individuals and entities in order to be able to propose and adopt new legislative measures to continue the measures. This then also has the effect that at each such review the persons and entities listed must be given a further opportunity to contest the legality of the measures.

(f) Types of Sanctions

The EU will seek to define its response to any crisis which justifies the imposition of sanctions by making sure that the measures are targeted. EU smart sanctions typically involve the following types of measures: the first is a travel ban, which restricts the listed persons from entering and travelling within the EU member states; the second is an asset freeze, which applies to any assets held by the listed persons with the EU. And finally, the

third is a transaction freeze, which prohibits any EU citizens from participating in any economic transactions with the listed persons.

Typically, sanctions do contain exemptions for certain necessary transactions, such as the listed person engaging an EU lawyer to challenge the sanctions. For country sanctions, there is often an exemption for urgent medical supplies.

In more general terms, the types of measures that the EU will adopt include the following:

- Arms embargoes;
- Trade restrictions, such as import and export bans in particular in relation to sectors or types of goods;
- Financial restrictions in particular asset freezes where the assets are held in the EU or where EU entities are involved in providing services in relation to the assets of listed entities or individuals; and
- Restricting movement, by imposing EU visa or travel bans.

These measures will be imposed at either a government level, or in relation to listed state or non-state entities, and finally in relation to dealings with named and identified individuals—whether alleged terrorists or their supporters or indeed persons known to have dealt with and provided support to such persons.

(g) Reasons for Sanctions

The aim of economic sanctions is traditionally to achieve a foreign policy goal, but this must be understood in a broader sense than merely relations between sovereign states. Thus, foreign policy and the related sanctions may include issues that are internal to the third country.

Smart sanctions are generally directed against persons, and companies that are considered to be supporting the regime in a third country, or certain activities in that country that are targeted by the sanctions. This has been the case in relation to Iran, where economic sanctions have been directed against companies that were deemed either directly or financially to support the development of nuclear capabilities.

The CJEU has also accepted that foreign policy may include the re-establishment of law and order in a third country that has overthrown a corrupt regime. Effectively, this entails that smart sanctions can be directed against former members of government or other key players in the former

regime whom the new regime wishes to hold responsible for the transgressions of the former regime (such as serious violations of international human rights or international humanitarian law, or egregious acts of corruption).

(h) Sanctions Procedure

The process of adopting sanctions requires procedures and dialogues to be pursued between the EU Council, the member states, EEAS and the EU Commission, and EU Council Working Groups. The complexity is necessary in order to manage the Treaty requirements in terms of legal base and decision-making procedures. The EU decision-making process increasingly seeks to find a uniform procedure that can encompass two completely different legislative procedures and produce a seamless set of measures uniform in content and without any visible gap in time for their adoption and implementation.

The first and primary procedure is the procedure to adopt the CFSP decision. Without this, there is no need to engage the Article 215 procedure, which is needed where sanctions are to include economic and financial restrictions. Under the CFSP, the decision is adopted by unanimity of all EU member states. Under the Article 215 regulation, the decision of the Council is adopted on the basis of a qualified majority vote (QMV) following the presentation of a joint proposal from the High Representative and the EU Commission.

Behind the adoption of all sanctions measures, the EU institutions are required to follow appropriate procedures to ensure that all three major principles of EU law, which are set out in the Charter of Fundamental Rights (the Charter) forming part of the EU Treaties and imposing rights and obligations similar to those found in the European Convention on Human Rights (ECHR), are fully respected. The three Charter principles are: the right to be heard (Charter Article 41(2)(a)), the obligation for the administration to provide reasons (Charter Article 41(2)(c)), and the right to a fair trial (Charter Article 47(1)), which implies an access to a court of law.

Thus, the obligation to provide reasons also applies to legislators, as set out in Article 296 TFEU. In this connection, it is important to recall that in the language of the EU treaties, the decisions of the administration also

constitute legal acts, and thus legislative and administrative acts are in principle subject to the same requirements.

(i) Enforcement and Legal Challenge

One of the consequences of the structure of the EU is that while it has a strongly centralized legislative function, in the area of sanctions the EU has only limited and mostly indirect administrative functions, and virtually no enforcement functions.

Thus, all questions on enforcement of EU sanctions are addressed at the national level. This means of course that there are inevitably differences in both procedure and enforcement in each member state. Differences may be clear, such as differences in the type of sanctions imposed for breach of EU sanctions, or they may be opaque, where for example some member states are more active in terms of enforcement procedures than others. They may also be more contentious where, for example, a member state pursues a policy of implementation that effectively involves a different approach in terms of substance to that set out in the EU measures.

These national issues fall outside the scope of this chapter.

As a matter of EU law, in addition to the potential to challenge the implementation of EU sanctions measures before national courts, EU sanctions measures can and indeed are regularly challenged before the CJEU by those entities and persons who are affected by the measures. The time limit for bringing the challenge is two months from the adoption of the measure to which is added additional days (ten or sometimes 14 days depending on the procedure followed) as set out under the CJEU Rules of Procedure.

The CJEU will also not generally enter into the evaluation of foreign policy objectives or the substance of administrative decision-making but will oversee the administrative and legislative procedure and whether the Charter principles have been respected during that procedure. Thus, the practitioner will require intimate knowledge of the case law on administrative and legislative procedure in order to mount a challenge an EU listing.

(j) EU Sanctions and Russia

Although EU sanctions against Russia have been in place since the 2014 invasion of Crimea, it is the attack on the whole of Ukraine, which started on February 24, 2022, that has resulted in the EU Russia sanctions becoming the most complex and detailed set of measures ever adopted by the EU. All of the difficulties that have faced the EU when adopting any sanctions measure have been highlighted by the immediacy and proximity of the war in Ukraine. As confirmed earlier, these difficulties include the differences of foreign policy between the EU member states, different levels of exposure economically and strategically to the war in Ukraine, and finally different approaches to the interpretation of the sanctions themselves and the appropriate methods of enforcing the rules.

The complexity of the sanctions measures adopted was needed to take account of the economic dependence of the EU on certain imports from Russia (notably oil and gas). Even if the formal sanctions fell far short of imposing any de facto embargo on trade with Russia, the impact of the war on Ukraine had a greater impact on trade for two other reasons: first, the views of EU citizens was generally that trade with Russia should be stopped; and second, many EU banks and financial institutions withdrew their support for transactions involving Russia, which left EU-based companies unable to carry on permitted business in Russia even if they wanted to.

The regulatory position in the EU has and remains that with the exception of certain sectors of the economy and certain types of product, trade, in general, is still permitted with Russia.

The measures themselves are set out in two Regulations:

- Council Regulation (EU) No 269/2014 of 17 March 2014[25] concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty, and independence of Ukraine (as amended). This sets out the identity of the persons and entities who have been listed by the EU and the nature and consequences of the prohibitions related to dealings with such persons and entities.
- Council Regulation (EU) No 833/2014 of 31 July 2014[26] concerning restrictive measures in view of Russia’s actions destabilizing the situation in Ukraine (as amended) sets out the nature of the sectoral prohibitions on trading with or purchasing goods from Russia.

Both measures have been accompanied by a growing list of EU and national guidance documents, including guidance notes issued by the EU Commission and the EU Council on the Regulations together with the now regularly updated Frequently Asked Questions document of the EU Commission.[27]

Such guidance may be valuable, but it remains guidance only and at least in some respects is directed as much at the national authorities of the member states (to indicate how the provisions of the Regulations should be interpreted) than at the wider business community at large.

It is in the area of interpretation and enforcement that Putin's invasion of Ukraine may well come to have the most lasting impact in the EU. Just as the invasion has caused a seismic change in German foreign policy as well as causing traditionally neutral EU member states Sweden and Finland to change their stated policy of the last 50 years and seek membership of NATO, so the difficulties of imposing clear and consistent sanctions measures across the EU has led to new discussions on the potential for further reform to enable the EU to implement and apply consistent sanctions measures across all 27 member states, that is, to have a truly federal sanctions policy. It has been suggested that this could be achieved by creating an EU version of OFAC.

For the reasons set out earlier, creating an EU OFAC would require a wholesale change in the constitutional relationship between member states and the EU. It would require that, at least on sanctions, the EU would work on the basis of a single foreign policy rather than coordination of 27 domestic foreign policies. Such is the perceived threat from President Putin's Russia, that it may well be possible to move forward toward a much more federal approach. A more realistic version would see an intermediate solution—with some form of EU administrative function working alongside national authorities, that is, moving from information sharing to coordinating formal directions on policy.

In the short term however, in the absence of major treaty and constitutional reforms, the EU will be left with the existing difficulties of inconsistent application and enforcement.

7.6 Conclusion

The words apparently attributed to Otto von Bismark about sausages (but probably coined by John Godfrey Saxe) spring to mind: “Laws are like sausages. It is best not to see them being made.” And so it is with EU export control laws and sanctions. From a distance they may seem clear, built on solid constitutional grounds and reflecting a clear EU wide policy consensus. However, the closer we look the more the imperfections become clear—imperfections that can have very substantial consequences on a day-to-day basis in the commercial life of both EU and U.S. companies.

The practical focus of EU export control and sanctions is very much the national laws of the 27 member states that administer and enforce them. Given this, is it appropriate to look at all at the EU measures? The answer from these authors is a resounding yes. The EU rules set out not only the framework and some of the detailed obligations and procedures to be followed but the rules also define the limits of such member state action. Without an understanding of these provisions it is impossible to assess whether the member states are correctly administering and enforcing EU law.

A detailed knowledge of EU law is needed to understand whether the position taken by one member state in terms of scope of application of a given measure is a legitimate approach to the implementation of EU rules or an illegal application of powers that it has no right to enforce.

The differences may be substantive or may lie beneath the surface of national measures that are remarkably similar to all other national measures adopted in the EU but nevertheless are applied in such a way as to produce different outcomes. These differences sometimes arise out of a different but legitimate approach to technical assessments of products, differences in the sorts of national licenses available and the way in which a given member state evaluates the risks of the proposed transaction. Such differences may also, however, reflect a fundamental difference of opinion in terms of the substantive rules that are to be applied.

With this in mind, the reader can now consider and assess the implications of the EU export control and sanctions measures adopted by the 27 EU member states.

---

1. John Grayston is a Belgian Avocat, English Solicitor and founding member of Grayston & Company, a law firm specializing in all aspects of EU regulatory law but particularly customs, trade and export control, and sanctions. Peter Gjørtler is a Danish Advokat and founding Of Counsel at Grayston & Company, with many years of experience working as legal advisor to the President and

Advocate General at the Court of Justice of the European Union. John and Peter have represented clients in more than 15 sanctions cases before the General Court and Court of Justice of the European Union.

2. Updated version available at http://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/en/pdf (last visited Dec. 14, 2022).

3. *See* https://service.betterregulation.com/document/446371 (last visited Dec. 14, 2022).

4. A limited set of exceptions to this rule are set out in Annex IV of the DU Regulations.

5. *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008E0944 (last visited Dec. 14, 2022).

6. *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0043 (last visited Dec. 14, 2022).

7. *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003E0468 (last visited Dec. 14, 2022).

8. The most recent version (as of February 2022) is available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022XG0301(01)&from=EN (last visited Dec. 14, 2022).

9. The EU Council's press release is at https://www.consilium.europa.eu/en/press/press-releases/2019/09/16/control-of-arms-export-council-adopts-conclusions-new-decision-updating-the-eu-s-common-rules-and-an-updated-user-s-guide/ (last visited Dec. 14, 2022).

10. The text of the EUDUR can be found at https://trade.ec.europa.eu/doclib/docs/2021/june/tradoc_159639.pdf (last visited Dec. 14, 2022).

11. *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02021R0821-20220505 (last visited Dec. 14, 2022).

12. *See* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0001 (last visited Dec, 14, 2022).

13. *See* https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en (last visited Dec. 14, 2022).

14. The United Kingdom ceased to be a member state of the EU on December 31, 2020.

15. *See* https://trade.ec.europa.eu/doclib/docs/2016/august/tradoc_154880.pdf#page=27.

16. *See* Article 2(3)(i) EUDUR.

17. *See* per Article 3(1) EUDUR.

18. Not all member states follow this logic in practice, and it is not uncommon to find attempts to introduce national procedural or substantive variations to the application of the UGEAs.

19. Likewise, EU001 also authorizes exports to Australia, Canada, Japan, New Zealand, Norway, Switzerland, and Liechtenstein.

20. In practice, member states generally require notification in advance and in order to complete this an exporter must complete national registrations for customs and export control purposes.

21. This requirement and indeed the conditions of application of each of the UGEAs are set out in Annex II to the EUDUR.

22. *See* Article 11(1) EUDUR.

23. *See* Article 11(2) EUDUR.

24. *See* at L 129 of 17.05.2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0797 and https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2019%3A129I%3ATOC&uri=uriserv%3AOJ.LI.2019.129.01.0001.01.ENG (last visited Dec. 14, 2022).

25. *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0269 (last visited Dec. 14, 2022). Note that this link is to the original version of Regulation 269 although in the title section there is a hyperlink to the most recent consolidated version.

26. *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.229.01.0001.01.ENG (last visited Dec. 14, 2022). Note once again that

this link is to the original version of Regulation 833 although in the title section there is a hyperlink to the most recent consolidated version.

27. *See* https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine_en (last visited Dec. 14, 2022).

8

Export Controls and Economic Sanctions in Canada

John Boscariol and Oksana Migitko[1]

8.1 Overview

What Is Regulated: Export controls regulate the transfer of certain listed goods and technology from a place in Canada to a place outside of Canada. These controls apply not just to physical shipments but also to transfers by intangible means, including through the provision of services or training, server upload, downloads or access from abroad, other electronic file transfers, emails, faxes, telephone conversations, teleconferencing, and face-to-face meetings.

Canada also regulates brokering of certain controlled items, that is, the negotiation or arrangement of a transaction relating to the movement or disclosure of these goods or technology from one foreign country to another.[2]

Canadian economic sanctions regulate the activities of persons in Canada and Canadian companies and individuals outside Canada in connection with economic measures taken against other countries, entities, and individuals. In some cases, sanctions may overlap with export controls; however, they generally apply more broadly, including in circumstances where there is no export or transfer of items from Canada.

Where to Find the Regulations: As is further discussed later in the chapter, Canada's export controls are implemented pursuant to the Export

and Import Permits Act and its regulations, including the Export Control List, Area Control List (ACL), and Brokering Control List. Economic sanctions are set out under Canada's United Nations Act, Special Economic Measures Act, Freezing Assets of Corrupt Foreign Officials Act, Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law), Criminal Code, and their regulations. Canada's Defence Production Act and its Controlled Goods Regulations set out the requirements and prohibitions in respect of the possession, examination, and transfer within Canada of defense-related items.

Who Is the Regulator: Canadian export controls and economic sanctions are administered by Global Affairs Canada (GAC) and enforced by the Royal Canadian Mounted Police (RCMP) and the Canada Border Services Agency (CBSA). GAC's Export Controls Operations Division (ECOD) is responsible for processing permit applications for the export and brokering of controlled items. GAC's Sanctions Policy and Operations Coordination Division processes applications for certificates or permits under Canada's economic sanctions legislation.

Controls under the Defence Production Act (DPA) are administered by the Controlled Goods Directorate of Public Services and Procurement Canada and are enforced by the RCMP.

How to Get a Permit: Export and brokering permits can be obtained through an application to the ECOD. This includes applications to export or broker listed controlled items to other countries or any items to countries listed on the ACL. An application may be made to GAC's Sanctions Policy and Operations Coordination Division to carry out any activities or transactions that are restricted or prohibited under sanctions laws.

Key Websites: Current information on Canada's export and brokering controls can be found at GAC's website.[3] GAC also maintains a website on Canadian economic sanctions.[4]

Generally, all laws and regulations of Canada, including those pertaining to export controls and economic sanctions, are published on the Department of Justice website.[5]

8.2 Structure of the Laws and Regulations

(a) International Treaties

Canada is a participating state in the key multilateral export control regimes, including the Wassenaar Arrangement, Nuclear Suppliers Group, Missile Technology Control Regime, and Australia Group.

In September 2019, Canada became a State Party to the United Nations Arms Trade Treaty (ATT), a treaty establishing standards for international trade in a broad range of conventional arms that currently includes more than 100 State Parties. To meet its ATT obligations, Canada made significant amendments to its Export and Import Permits Act (EIPA)[6] and regulations in 2019, which included the adoption of a package of brokering regulations (which are described later in greater detail).

In addition to this, Canada participates in a number of international treaties relating to disarmament, including the Treaty on Non-Proliferation of Nuclear Weapons (NPT), the Convention on Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (1972), and the Convention on Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (1993).

(b) National Laws and Regulations on Export Controls

In Canada, the control of exports and cross-border technology transfers falls within the mandate of the federal government.

Exports of goods and technology are primarily controlled by means of the EIPA, and other sectoral regimes, such as for nuclear-related items.[7] Economic sanctions legislation, such as the United Nations Act (UNA)[8] and the Special Economic Measures Act (SEMA),[9] can also be used to restrict or prohibit exports to sanctioned countries, entities, and individuals.

Canada's DPA[10] and Controlled Goods Regulations[11] set out requirements and prohibitions in respect of the possession, examination, and transfer within Canada of certain "controlled goods and technology" listed on the DPA Schedule, which include U.S.-origin items subject to the U.S. International Traffic in Arms Regulations (ITAR)[12] as well as other defense and missile technology–related items.

(c) Export Control List

Established under the EIPA, the Export Control List (ECL)[13] identifies those goods and technology that may not be exported or otherwise transferred from Canada by tangible or intangible means without first obtaining an export permit, subject to exemptions for certain destination countries. The ECL is not product specific, but instead provides a set of technical specifications that are technology neutral for the most part and that are functional in their description. Listed goods and technology are categorized into groups as follows:

- Dual-use items (Group 1)
- Munitions (Group 2)
- Nuclear non-proliferation items (Group 3)
- Nuclear-related dual-use goods (Group 4)
- Miscellaneous goods, including all U.S.-origin goods and technology, forest items, agricultural and food products, apparel goods, certain vehicles, laser weapons, nuclear-related and strategic items (Group 5)
- Missile equipment and technology (Group 6)
- Chemical and biological weapons and related technology (Group 7)
- Arms trade treaty (Group 9)

The items within each group are further set out in A Guide to Canada's Export Controls[14] (Guide), published by GAC and incorporated by reference into the ECL. The Guide contains a detailed list of items subject to export restrictions under the EIPA and ECL as well as their technical specifications. The Guide is updated from time to time to reflect Canada's commitments under multilateral export control regimes, namely, the Wassenaar Arrangement, Nuclear Suppliers Group, Missile Technology Control Regime, and Australia Group. Historically, these updates are not made immediately to reflect changes agreed to under the export control regimes so that goods and technology that may be controlled or de-controlled by other countries under these international regimes may not be controlled or de-controlled under Canadian law at a given point in time.

The last changes to the ECL were implemented on December 21, 2022.[15]

(d) Brokering Control List

The Brokering Control List,[16] established under the EIPA, identifies the items for which a brokering permit is required. It encompasses all ECL Group 2 (Munitions List) and Group 9 items (eight ATT categories of full-system conventional arms), as well as other ECL items, including dual-use ones, that are likely to be used to produce or develop a weapon of mass destruction.

(e) Area Control List

Under the authority of the EIPA, Canada maintains the ACL,[17] on which prohibited destination countries are identified from time to time. No goods or technology may be exported or transferred to these countries without first obtaining an export permit. Currently, North Korea is the only country on the list. Such permits are only issued by the ECOD in rare circumstances, for example, when the transfer is for humanitarian purposes.

(f) Canada and United Nations Security Council Sanctions

As a United Nations member state, Canada is required to implement economic sanctions resolutions adopted by the United Nations Security Council. Such sanctions are imposed under Canada's domestic law through regulations issued under the UNA.

(g) National Laws on Economic Sanctions

There are five federal statutes through which Canada has enacted economic sanctions: the UNA, SEMA, the Freezing Assets of Corrupt Foreign Officials Act (FACFOA), Sergei Magnitsky Law, and the Criminal Code.

(i) United Nations Act

Canada's UNA enables the Canadian government to give effect to decisions passed by the United Nations Security Council. If the United Nations Security Council determines that an act of aggression or a breach of peace has occurred, it may decide what measures member states shall take to restore or maintain international peace and security. These measures are generally economic and trade sanctions. Such a decision imposes a legal obligation on Canada as a United Nations member to introduce the required

measures into domestic law. This is done by enacting regulations under the UNA.

(ii) Special Economic Measures Act

In order to maximize the effectiveness of a sanctions regime, Canadian policy seeks to ensure, whenever possible, that sanctions are applied multilaterally through the UNA. However, in the absence of a United Nations Security Council resolution or one that is sufficient in the view of the Canadian government, SEMA authorizes the imposition of sanctions in certain specifically defined circumstances—namely, where (1) an international organization or association of states, of which Canada is a member, has made a decision or a recommendation calling on its members to take economic measures against a foreign state, (2) a grave breach of international peace and security has occurred that has resulted in or is likely to result in a serious international crisis, (3) gross and systematic human rights violations have been committed in a foreign state, or (4) a national of a foreign state who is either a foreign public official or an associate of such an official is responsible for or complicit in ordering, controlling, or otherwise directing acts of significant corruption.

SEMA allows Canada to restrict the export, supply, or sourcing of goods and technology, as well as the movement of people and money and the provisions of services, to or from any country against which Canada has imposed economic sanctions. It also allows for the listing of individuals and entities who are subject to “asset freezes,” that is, persons in Canada and Canadians outside Canada are prohibited from engaging in a wide range of dealings involving such listed persons and their assets.

On June 23, 2022, amendments to SEMA as well as to the Sergei Magnitsky Law came into force that allow for the forfeiture of property that has been the subject of a seizure order under these sanctions statutes. The amendments allow the government to sell the seized property and use the proceeds for various enumerated purposes, including reconstruction of foreign states, and compensation to victims of grave breaches of international peace and security, human rights violations, and acts of significant corruption.

These new measures can be applied to any property situated in Canada that is owned, held, or controlled directly or indirectly by any foreign state or by any person in, or national of, any foreign state. The Minister of

Foreign Affairs can issue an order for the seizure or restraint of such property in certain specified circumstances. Once such a seizure order has been issued, the minister can now apply to the Superior Court of the province in which the seized or restrained property is located for an order to forfeit such property. The court must issue the forfeiture order if it is determined that (1) the property in question is the same property as described in the seizure order and (2) it is owned, held, or controlled directly or indirectly by the person referred to in the seizure order.

(iii) Freezing Assets of Corrupt Foreign Officials Act

Pursuant to FACFOA,[18] Canada has also implemented economic sanctions measures targeting activities involving certain "politically exposed foreign persons." If a foreign state in a state of internal turmoil or an uncertain political situation asserts in writing to the government of Canada that a person has misappropriated or inappropriately acquired property of the foreign state by virtue of their office or a personal or business relationship, the Governor in Council may freeze that person's property in Canada.

Under FACFOA, "politically exposed foreign persons" are defined as persons who hold or have held certain identified offices or positions in or on behalf of a foreign state, such as heads of state, members of legislatures, deputy ministers, ambassadors, military officers, presidents of state-owned companies or banks, heads of government agencies, judges, or political party leaders, and their family members.

FACFOA restrictions are intended to be a form of assistance that Canada provides to the requesting country as an initial step toward possible mutual legal assistance, consistent with Canada's Mutual Legal Assistance in Criminal Matters Act.[19] Canada has adopted regulations under FACFOA to provide for specific measures to be taken against former Tunisian and Ukrainian leaders and senior officials, and their associates and family members, suspected of misappropriating state funds or obtaining property inappropriately.

(iv) Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law)

Pursuant to the Sergei Magnitsky Law,[20] Canada can impose targeted measures against foreign nationals who are, in the opinion of the Governor

in Council, responsible for or complicit in gross violations of human rights or who are public officials or associates of such officials who are responsible for or complicit in acts of significant corruption. There are presently sanctions in place under the Sergei Magnitsky Law against Venezuelan, Russian, Sudanese, Myanmar, and Saudi Arabian nationals.

Persons in Canada and Canadians outside Canada are prohibited from engaging in a wide range of dealings involving persons listed under the Sergei Magnitsky Law, as well as their assets.

(v) Criminal Code

The listing of entities under the Criminal Code enables Canada to apply appropriate criminal measures to terrorist entities, including those not necessarily listed under the United Nations Al-Qaida and Taliban Regulations[21] or the United Nations Resolutions on the Suppression of Terrorism.[22]

(vi) Foreign Extraterritorial Measures Act

Canada's Foreign Extraterritorial Measures Act (FEMA)[23] purports to help protect Canadians and Canadian businesses from extraterritorial application of foreign laws. FEMA allows the Canadian government to respond to what it views as unacceptable extraterritorial assertions of foreign jurisdiction, including with "blocking orders" that prohibit compliance with foreign measures. Currently, there are two orders under FEMA, one regarding U.S. sanctions against Cuba[24] and the other relating to the application of U.S. "Buy America" rules to construction activities at the Prince Rupert ferry terminal in British Columbia.[25] FEMA is reviewed in greater detail later in this chapter.

(h) Sanctioned Parties Lists

The Sergei Magnitsky Law, as well as most regulations promulgated under the UNA, FACFOA, and SEMA identify designated or listed persons, which can include entities, associations, governments, and individuals that are subject to asset freezes and financial prohibitions. Persons in Canada and Canadians outside Canada are generally prohibited from engaging in

dealings with these designated persons regardless of whether such dealings involve a sanctioned country.

The measures prohibit dealing directly or indirectly in any property of such persons, entering into or facilitating related financial transactions, and providing financial services or other related services in respect of such property. They may also prohibit providing financial or related services or making goods available to or for the benefit of these designated persons.

There is no single official consolidation of Canada's economic sanctions lists. However, GAC maintains a Consolidated Canadian Autonomous Sanctions List and includes individuals and entities subject to specific sanctions regulations made under SEMA and the Sergei Magnitsky Law.[26] The list of sanctioned persons under FACFOA can be found in the respective regulations. The United Nations Security Council maintains the Consolidated Sanctions List that can be accessed on the United Nations' website.[27]

The Solicitor General of Canada maintains the Regulations Establishing a List of Entities[28] made under subsection 83.05(1) of the Criminal Code. This list is composed of entities determined to have carried out, attempted, participated in, or facilitated a terrorist activity. Public Safety Canada also maintains a list of entities associated with terrorism—Listed Terrorist Entities.[29] This list, which has been prepared for reference only and follows the List of Entities under the Criminal Code, provides brief background information on the listed entities.

All transactions should be screened to ensure that designated or listed persons are not involved in any way—including, for example, as purchasers, suppliers, creditors, agents, brokers, or freight forwarders—or otherwise benefiting from the transaction. Screening based on denied party lists under U.S. or other foreign laws is not sufficient for these purposes.

(i) Destinations of Concern

Currently, there are various Canadian sanctions as well as restrictive export control policies in respect to the following countries and territories or persons from these countries and territories: Afghanistan, Belarus, Central African Republic, China, Cuba, Democratic Republic of the Congo, Haiti, Hong Kong, Iran, Iraq, Lebanon, Libya, Mali, Myanmar, Nicaragua, North Korea, Pakistan, Russia, Saudi Arabia, Somalia, South Sudan, Sudan, Syria,

Tunisia, Turkey, Ukraine, Venezuela, Yemen, Zimbabwe. This section will cover the most frequently encountered destinations of concern.

(i) Afghanistan under the Taliban

The Taliban takeover of Afghanistan following the withdrawal of U.S. troops in the summer of 2021 created new challenges for organizations engaged in activities in that region. Although Canada has not imposed sanctions against Afghanistan, the Taliban is a listed terrorist group under the Regulations Establishing a List of Entities[30] adopted under the Criminal Code, while persons associated with the Taliban are listed under the Regulations Implementing the United Nations Resolutions on Taliban, ISIL (Da'esh) and Al-Qaida.[31] The Criminal Code prohibits directly or indirectly providing or making available property and financial or related services that will be used by or will benefit such terrorist groups either in whole or in part.[32] The government of Canada also announced it has no plans to recognize the Taliban as the legitimate government of Afghanistan.

(ii) Belarus

On September 29, 2020, the Canadian government announced the imposition of sanctions on various officials of the government of Belarus effective immediately. The sanctions are Canada's response to the Belarus government's violent and sustained crackdown on opposition leaders and civilians protesting the results of Belarus's fraudulent presidential election on August 9, 2020.

Initially, the measures targeted 11 high-ranking Belarussian civil and military figures alleged to be involved in gross and systemic human rights violations following the failed election. These include the purported winner of the election, Aleksandr Lukashenko, as well as his son and National Security Advisor, Viktor Lukashenko. Canada expanded these measures following the Belarusian government's diversion and forced landing of Ryanair Flight 4978 as well as the arrest of Belarusian journalist Roman Protasevich and his companion Sofia Sapega in May of 2021. Between June and August 2021, Canada adopted additional measures, which included significant sectoral and trade sanctions targeting important sectors of Belarus' economy. These measures apply to dealings in transferable securities and money market instruments; interactions with debt with more

than 90 days' maturity; the provision of insurance and reinsurance to certain individuals and entities; and dealings in petroleum and potassium chloride products.

The next wave of sanctions on Belarus was imposed by Canada from March to June 2022 as a response to Belarus's support of the Russian invasion of Ukraine. Canada listed Belarusian government and financial elites, their family members and associates, senior officials of the Belarusian Ministry of Defence, and entities involved in Belarus's financial, potash, energy, tobacco, and defense sectors. Canada also prohibited the provision of all insurance, reinsurance, and underwriting services for aircraft, aviation, and aerospace products owned, controlled, chartered, registered to, or operated by Belarusian individuals or entities. Further, there is a ban on export to Belarus of all items in the Restricted Goods and Technologies List,[33] certain luxury goods, and goods that could be used in the manufacturing of weapons. Import of certain luxury goods from Belarus such as fish, seafood items, liquor, and diamonds, is also prohibited.[34]

On November 9, 2020, Canada announced that it temporarily suspended the issuance of all new permits for the export and brokering of all controlled goods and technology to Belarus, including dual-use items (Group 1). Exporters who were issued permits for the export or brokering of items to Belarus prior to November 9 may continue to export against those permits during their period of validity.[35]

(iii) China

On March 22, 2021, Canada imposed economic sanctions against the People's Republic of China under SEMA. This is the first imposition of sanctions on China since the 1989 crackdown on student protestors in Beijing's Tiananmen Square. The measures target four Chinese government officials and one Chinese entity in response to what the Canadian government has deemed to be "gross and systematic human rights violations" against Uyghurs in China's northwest region of Xinjiang.

Although these latest Canadian measures are closely aligned with those of the EU, the United Kingdom, and the United States, they represent a historic step in Canadian sanctions policy that could reflect a new willingness on the part of the Canadian government to take further measures in responding to human rights violations in China.

Canada has also issued several guidance documents (measures[36] and an advisory[37]) to Canadian businesses designed to address human rights concerns in sourcing from and exporting to China.

(iv) Cuba

Canada does not restrict exports or transfers to Cuba unless the goods or technology are of U.S. origin or otherwise controlled on the ECL, in which case a permit must first be obtained. It is important to note that, pursuant to an order issued under FEMA (FEMA Order),[38] Canadian companies and their directors, officers, and employees in a position of authority are prohibited from complying with the U.S. trade embargo of Cuba and are required to advise the Canadian Attorney General forthwith of any communications related to the U.S. trade embargo received from a person in a position to direct or influence their policies in Canada. Failure to comply with the order is punishable with criminal penalties.

(v) Haiti

In November 2022, Canada imposed sanctions on Haiti under both the UNA and SEMA. The measures were adopted in response to the activities of criminal gangs and those who support them in fomenting violence and insecurity, which constitutes an ongoing grave breach to international peace and security that has resulted in a serious international crisis. The sanctions measures impose dealings prohibitions, asset freezes, and travel bans on listed persons, as well as an arms embargo.

(vi) Hong Kong

Following China's adoption of national security law giving the Chinese government new powers over Hong Kong, the government of Canada issued a statement on July 3, 2020, declaring that Canada will treat exports of sensitive goods to Hong Kong in the same way as those destined for China and, further, will not permit the export of sensitive military items to Hong Kong. On July 7, 2020, the ECOD issued a notice clarifying that in order to ensure that sensitive items are not exported to Hong Kong, GAC will closely scrutinize all export permit applications for items to Hong Kong, and will deny permits that are not in line with Canada's domestic and international legal obligations, foreign policy, or security interests.[39]

(vii)Iran

In response to Iran's nuclear and weapons of mass destruction programs, Canada has imposed sanctions against Iran for many years and has applied a comprehensive trade embargo for almost three years. Effective February 5, 2016, shortly after the coming into force of the Joint Comprehensive Plan of Action[40] (JCPOA), Canada repealed many of its sanctions against Iran under both the UNA and SEMA. Currently, the remaining measures are composed of more narrow economic sanctions and export control restrictions.

Even though the sanctions were substantially relaxed as a result of the JCPOA, Canada still maintains prohibitions under the UNA regulations[41] with respect to the supply to Iran of nuclear-related materials, equipment, goods and technology, arms, as well as provision to any person in Iran of related technical assistance or financial services. The SEMA regulations also prohibit the supply to Iran or to persons in Iran of a broad range of products, including certain precious metals, chemical compounds, stainless steel goods, and machinery and production equipment.

Canada maintains tight controls on exports and transfers of controlled goods and technology to Iran. All applications for export permits for any item listed on the ECL are considered on a case-by-case basis. In addition, there is a policy of denial of export permit applications relating to all items in Groups 2 to 4, as well as certain items in Groups 1, 5, 6, and 7, as these are considered to be the most sensitive from a national and international security perspective.[42] The Canadian government has not issued any formal guidance on how it will apply its new brokering control regime to transfers from foreign countries to Iran; however, one would expect it to follow a similar policy.

Further, no U.S.-origin goods or technology can be transferred to Iran from Canada without an export permit, and that can only be obtained in limited circumstances.[43] Exporters should be aware that CBSA is also closely scrutinizing exports to locations that are commonly used for transshipment to Iran, including the United Arab Emirates, Malaysia, and Hong Kong.

(viii)Myanmar

Sanctions against Myanmar were enacted by Canada under SEMA in December 2007 to respond to human rights violations and the deteriorating humanitarian situation in the country, which threatened peace and security in the region. At the time, they were among the most restrictive sanctions imposed against Myanmar by any country. In April 2012, the sanctions measures were significantly scaled back, but they still include prohibitions on exporting and importing arms and related material and technical data to and from Myanmar, related financial services prohibitions, and asset freezes. On February 18, 2021, in response to the coup d'état in Myanmar, nine senior military officers were added to the list of sanctioned individuals. These sanctions were repeatedly expanded throughout 2021 and the first half of 2022 by adding further key senior military and military-appointed officials and their family members, as well as military, defense-related, and affiliated commercial entities to the sanctions list.

(ix) Nicaragua

On June 21, 2019, Canada implemented sanctions against Nicaragua. The sanctions were imposed under SEMA to include a dealings prohibition, asset freezes, and travel bans on nine individuals. These listed individuals are key members of the government of Nicaragua. The sanctions were implemented in response to gross and systematic human rights violations and state-sponsored violence against anti-government protests, including the torture, extrajudicial killings, and mistreatment of protestors. Nicaragua sanctions do not impose general export restrictions. In November 2021, in response to ongoing human rights violations, Canada imposed additional sanctions on Nicaragua by listing 11 high-ranking officials as part of President Daniel Ortega's inner circle.

(x) North Korea

Sanctions against North Korea were implemented under the UNA in November 2006 in response to a North Korean claim that it conducted a test of a nuclear weapon. The initial set of sanctions measures was further expanded under SEMA in 2011, following a North Korean torpedo attack that sunk a South Korean naval ship. The measures against North Korea have since been progressively strengthened with the adoption of regulations under both the UNA and SEMA. The sanctions program against North

Korea is the most comprehensive one Canada has implemented to date. It encompasses such measures as complete export and import bans, prohibitions against certain dealings involving any person in North Korea or a national of North Korea who does not ordinarily reside in Canada, financial services prohibitions, asset freezes, and travel bans.

Further, as noted earlier, North Korea is the only country included on the ACL. This means that exports of any goods or technology from Canada to North Korea may only be made under a valid export permit obtained from the ECOD.

(xi) Pakistan

Canada has not imposed economic sanctions against Pakistan, however, it does maintain a restrictive policy with respect to controlled goods. Specifically, since May of 1998, military exports to Pakistan have been banned as a result of nuclear weapons tests by that country. Any application to export or transfer goods or technology controlled under Group 2 of the ECL to Pakistan will be denied.[44]

(xii)Russia and Ukraine

Canada imposed sanctions under SEMA against Russia in 2014 in response to Russian occupation of parts of eastern Ukraine and the annexation of the Crimea region of Ukraine.[45] In addition, in 2017 Canada imposed targeted measures against certain Russian individuals involved in human rights violations under the Sergei Magnitsky Law.

The list of sanctioned persons under the SEMA Russia Regulations[46] was gradually expanded throughout 2019–2021, including in response to human rights violations committed against Mr. Navalny, a prominent Russian opposition leader.

On February 21, 2022, Russia signed a decree recognizing the “independence” and “sovereignty” of the so-called Luhansk People’s Republic (LNR) and Donetsk People’s Republic (DNR) regions. Two days later, Russian forces initiated a comprehensive invasion of Ukraine. In response, Canada began rolling out of what has turned out to be one of its most comprehensive and complex sanctions programs ever. At the time of drafting this chapter, there have been 19 amendments to SEMA Russia Regulations since the invasion. Although Canada has indicated that these

sanctions measures have been implemented in coordination with the United States, the United Kingdom, and the European Union, many of the Canadian measures, including those with respect to designated or listed persons, sourcing and supply bans, and the services prohibitions, are more restrictive than those of its allies. With no end in sight to the conflict between Russia and Ukraine, further expansion of Canada's Russian sanctions program is expected to continue.

The SEMA Russia Regulations encompass a very broad set of measures, including asset freeze and dealings prohibitions with respect to persons listed under Schedule 1 thereto. At the time this chapter was drafted, over 850 individuals and over 230 entities were listed. The list of individuals encompasses president Putin, as well as members of his family, key government officials including ministers and members of the Russian Federal Assembly, oligarchs, close associates of the Russian regime, executives working in the energy sector, as well as members of their families. The list of entities encompasses state bodies, such as the Ministry of Finance and the National Wealth Fund, the Ministry of Defence and its communication center, defense sector entities, including research centers and institutes, over 25 Russian banks and financial institutions including the Central Bank, major Russian media outlets involved in disinformation activities, entities active in the oil and gas section, and many others. Notably, a number of the individuals and entities listed by Canada have not been listed or designated by the United States, the United Kingdom, or the European Union.

Canada has prohibited the import, purchase, or acquisition of petroleum products, wherever situated, from Russia or from any person in Russia, by persons in Canada or Canadians outside of Canada. A similar import ban has been introduced with respect to the import of certain gold products from Russia, including unwrought gold, semi-manufactured gold, gold powder, monetary gold and jewelry made of gold, as well as some luxury goods.

Canada has imposed a number of bans on goods that are to be exported, sold, supplied, or shipped to Russia or to any person in Russia. Since 2014, Canada has prohibited the supply of certain listed goods for use in offshore oil (depth greater than 500 m), shale oil, or Arctic oil exploration and production. This includes a ban on the provision of any financial, technical, or other services related to the goods subject to this prohibition. More recently, Canada prohibited the supply of luxury items as well as certain

advanced goods and technologies, including software, that could be used in the production and manufacturing of weapons.

There is also a broad supply ban on so-called restricted goods and technologies as set out in the Restricted Goods and Technologies List[47] prepared by Global Affairs Canada. This wide prohibition forbids any person in Canada and any Canadian outside Canada from exporting, selling, supplying, or shipping any good (or technology) on the list, wherever situated, to Russia or to any person in Russia. Generally speaking, the list includes a broad range of items in the areas of electronics, computers, telecommunications, sensors and lasers, navigation and avionics, marine, aerospace, and transportation.

In addition to the preceding, persons in Canada and Canadians outside Canada are now prohibited from providing to Russia or to any person in Russia a broad range of services referenced in Part 1 of Schedule 8 of the SEMA Russia Regulations in relation to certain industries referenced in Part 2 of Schedule 8 thereto. The affected industries include oil, gas, mining, the manufacture of chemicals and chemical products, transport and transport via pipelines, the manufacture of basic metals, fabricated metal products, machinery and equipment, computer, electronic and optical products, electrical equipment, motor vehicles, and transport equipment. Prohibited services include, among others, accounting, management consulting, engineering, scientific and technical consulting, services incidental to the manufacture of metal products, machinery and equipment, and advertising services.

There are restrictions in place relating to the provision of insurance and reinsurance to or for the benefit of Russia or any person in Russia for aircraft, aviation, and aerospace products described in Chapter 88 of the Harmonized Commodity Description and Coding System, and in relation to technology for a good described in that chapter.

It is also prohibited for ships registered in Russia or used, leased, or chartered (in whole or in part) by, on behalf of, or for the benefit of Russia, a designated person, or—most broadly—a person in Russia from docking in Canada or passing through Canada.

In addition to the preceding, the SEMA Ukraine Regulations[48] also impose broad embargoes on dealings in the Crimea region of Ukraine, DNR, and LNR.

(xiii)Saudi Arabia

In the fall of 2018, GAC was tasked with conducting a review of Canada's arms exports to Saudi Arabia. The issuance of new permits for exports to Saudi Arabia was put on hold, pending the completion of this review.

In November 2019, as set out in a departmental briefing note, GAC conducted its review under the new substantial risk assessment process and concluded that there was no "credible evidence linking Canadian exports of military equipment or other controlled items to any human rights or humanitarian law violations committed by the Saudi government." GAC also noted that there are no existing permits or pending applications that "would be of concern under the standard robust risk assessment framework."[49]

On April 9, 2020, GAC issued a statement noting that because the review did not result in a finding of a substantial risk under the EIPA procedure, it would resume approving exports of controlled items to Saudi Arabia. These permit applications are reviewed on a case-by-case basis.[50]

(xiv)Syria

Import of goods from Syria is generally prohibited for Canadians and persons in Canada, with the exception of food for human consumption. There is a ban on the supply to Syria of any goods or technology for use in the monitoring of telecommunications.[51] Canada has prohibited the supply to Syria of luxury goods as well as certain listed items that can be used for internal repression or chemical weapons. Canada has also imposed a financial services ban on Syria and persons in Syria.[52] As is the case with transfers to Iran, all U.S.-origin goods and technology are prohibited from being transferred to Syria without a permit, which can only be obtained in very limited circumstances.

(xv)Turkey

Turkey's intrusion into northern Syria in October of 2019 created a wave of responses from the international community. These events led to the imposition by the United States and some EU countries of sanctions of varying degrees on Turkey. However, the U.S. sanctions against Turkey were lifted by the United States shortly thereafter.

While Canada has not imposed formal economic sanctions against Turkey, it did suspend the issuance of new permits for exports of controlled items to its fellow NATO member on October 15, 2019. On April 16, 2020, the Canadian government announced that as of that date applications to export Group 2 items (i.e., military items) to Turkey will be presumptively denied. However, these applications will be reviewed on a case-by-case basis to determine whether exceptional circumstances exist to justify issuing the permit, including in relation to NATO cooperation programs.[53]

(xvi)Venezuela

Canada has imposed sanctions against Venezuela to respond to attacks on Venezuelans' democratic and human rights by the regime of Nicolás Maduro. During 2017 to 2019, Canada imposed several rounds of targeted sanctions under SEMA and the Sergei Magnitsky Law. The sanctions are composed of asset freezes and prohibitions on dealings with listed persons. In April 2019, the list of sanctioned individuals was significantly expanded as a result of Maduro's anti-democratic elections of May 2018 and subsequent repressions against his political opponents. These sanctions do not impose general export restrictions.

8.3 What Is Regulated: Scope of the Regulations

(a) Export and Brokering Controls

(i) Export and Import Permits Act

Canada maintains controls on exports and transfers of certain goods, services, and technology as well as on brokering activity pursuant to the EIPA. This includes controls based on the nature of the goods and technology as well as their destination. Permit applications for the transfer of such goods and technology are made to the ECOD. The RCMP and CBSA are responsible for the enforcement of these requirements.

Unlike the United States, Canada does not have a "deemed export" rule. The release of otherwise controlled software or technology within Canadian borders to a foreign national does not constitute an export. At the same time, as mentioned in Section 8.2 of this chapter, Canada regulates the

possession and transfer within Canada of certain goods under the DPA and Controlled Goods Regulations.

It is also important to note that, unlike the United States, Canada does not impose controls on the re-export of Canadian-sourced controlled items from other countries; although as discussed further later, Canada has recently implemented controls over the brokering of certain items between two foreign countries.[54]

(ii) Brokering Controls under the Export and Import Permits Act

To meet its ATT obligations, Canada amended the EIPA and adopted a package of brokering regulations, namely, the Brokering Control List,[55] Brokering Permit Regulations,[56] Regulations Specifying Activities that Do Not Constitute Brokering,[57] General Brokering Permit No 1,[58] and General Export Permit No 47 (the "ATT Package").[59]

The newly established legislative scheme imposes controls over brokering activities. This was a significant development for Canadian industry, as it was the first time such extraterritorial controls had been introduced in Canada. The amended EIPA prohibits unauthorized brokering by any Canadian company or individual, whether one is located in Canada or abroad, which essentially means that new Canadian brokering obligations apply on an extraterritorial basis. All companies and individuals in Canada as well as Canadians (including permanent residents) abroad require a Canadian permit to engage in brokering activities.

The EIPA defines brokering as arranging or negotiating a transaction that relates to the movement of goods or technology included on the BCL from one foreign country to another foreign country.[60] The import or export of goods or technology into or out of Canada or negotiations or arrangements solely in respect of such transfers are not covered by these brokering controls.

(iii) Defense Trade Controls

As was noted in Section 8.2 of this chapter, Canada's DPA and Controlled Goods Regulations regulate the possession, examination, and transfer in Canada of "controlled goods and technology," which include defense and other items covered by the ITAR. To export or transfer DPA-controlled

goods or technology from Canada, proof of registration with the CGD is required.

(b) Sanctions

As noted in Section 8.2 of this chapter, most regulations promulgated under the UNA, SEMA, FACFOA, the Sergei Magnitsky Law, and the Criminal Code identify designated or listed entities and individuals, that are subject to asset freezes and with whom persons in Canada and Canadians outside Canada are prohibited from engaging in dealings. Sanctions imposed on China, Mali, Nicaragua, Tunisia, Venezuela, and Yemen are list-based sanctions only.

In addition to the list-based only sanctions, Canada maintains broad trade embargoes, export/import controls, and technical assistance prohibitions that are imposed on targeted countries or specific sectors of the economy of such countries. These country-based sanctions under the UNA and/or SEMA allow Canada to restrict the supply of goods and technology from Canada or anywhere in the world, as well as the movement of people and money, or the provisions of services.

At the present time, trade embargoes and import/export controls of varying degrees are imposed on activities involving the following countries: Belarus, Central African Republic, the Democratic Republic of the Congo, Haiti, Iran, Iraq, Lebanon, Libya, Myanmar, North Korea, Russia, Somalia, Sudan, South Sudan, Syria, Ukraine (linked to Russia's ongoing violations of Ukraine's sovereignty and territorial integrity), and Zimbabwe. Any involvement of these countries or any designated or listed person in proposed transactions or other activities should raise a red flag for further investigation to ensure compliance with economic sanctions.

8.4 Who Is Regulated

(a) Export Controls

Canadian export and brokering controls apply to all residents of Canada, who are defined in the EIPA as either persons who ordinarily reside in Canada (in case of a natural person) or corporations that have their head office in Canada or operate a branch office in Canada.

(b) Sanctions

Economic sanctions generally apply to persons in Canada, which are defined as citizens or a corporation incorporated under the laws of Canada or of a Canadian province,[61] and Canadians outside Canada. This includes non-Canadian individuals and entities who are present in or conduct activities in Canada. It also includes Canadian nationals and companies who are operating outside Canada. Foreign entities owned or controlled by Canadians are not in and of themselves subject to Canadian economic sanctions, although the involvement of Canadians in their activities abroad could trigger Canadian jurisdiction.

8.5 Classification

Most items are listed on the ECL as a result of Canada's commitments under multilateral export control regimes, including the Wassenaar Arrangement, Nuclear Suppliers Group, Missile Technology Control Regime, and Australia Group, or Canada's international obligations as a signatory to multilateral or bilateral agreements. Participating governments negotiate common lists of goods and technology that are implemented by all, including Canada, according to national legislation. These lists evolve in response to changing international and technological circumstances.

The controlled goods are divided into groups and categories. Goods or technology controlled under one group or item of the ECL may also be controlled under other groups. When classifying goods, services, or technology, exporters should ensure that they have reviewed the ECL in sufficient detail to assure themselves that all relevant groups and items have been considered and identified.

(a) Classification of Dual-Use Items

Dual-use items comprise Group 1 of the ECL. This group contains goods and technologies that have dual purposes in that they could have both civilian and military applications. The dual-use list is organized under the following nine categories:

- Category 1: Special Materials and Related Equipment
- Category 2: Materials Processing

- Category 3: Electronics
- Category 4: Computers
- Category 5: Part 1: Telecommunications
- Category 5: Part 2: Information Security
- Category 6: Sensors and Lasers
- Category 7: Navigation and Avionics
- Category 8: Marine
- Category 9: Aerospace and Propulsion

(b) Classification of Military Items

Group 2 of the ECL is composed of items that are specially designed or modified for military purposes and those that present a strategic military concern. This group includes items that Canada has committed to controlling for export as a result of its participation in the Wassenaar Arrangement.

Group 2 includes smooth-bore weapons, ammunition, bombs, torpedoes, rockets, missiles, fire control items, surveillance and warning equipment, chemical agents, naval equipment, aircraft, electronic equipment, and high-velocity kinetic energy weapon systems as well as their associated technologies. Group 2 covers not only equipment but, in many cases, their parts and components as well.

8.6 General Prohibitions/Restrictions/Requirements

(a) Export Controls

Export of goods and technology included on the ECL or exports of any items to a country included on the ACL may only be made under a valid export permit. An export permit sets out, among other things, the quantity, technical description, and nature of the goods and technology to be exported, as well as the final destination country and consignee. As described earlier, brokering of certain controlled items also requires a valid permit.

Unless otherwise stated, an export permit may authorize multiple shipments up to the date of expiry of the permit and as long as the

cumulative total of the quantity or value of exported goods and technology does not exceed the quantity or value stated on the permit.

Factors such as the nature, characteristics, origin, or destination of the goods or technology being exported affect export permit requirements.

Section 7.3 of the EIPA sets out mandatory criteria that must be considered by the government when issuing permits. Permit applications for exports, transfers, or brokering will be denied if they could contribute to or facilitate the following:

- Undermining of peace and security;
- A serious violation of international humanitarian law or international human rights law;
- An offence under international conventions or protocols relating to terrorism or transnational organized crime to which Canada is a party; or
- Serious acts of gender-based violence or serious acts of violence against women and children.

(b) Sanctions

Sanctions laws and regulations prohibit persons in Canada and Canadians outside Canada from engaging in restricted activities or transactions with or involving certain countries, entities, or individuals. These measures are separate from, and apply in addition to, export controls. Sanctions differ by country and can encompass a variety of measures, including restricting or prohibiting trade, financial transactions, or other economic activity between Canada and the target state, and the seizure or freezing of property situated in Canada. Sanctions range from a full trade embargo to narrower list-based sanctions or sectoral measures.

Canadian sanctions regulations generally include mechanisms for the Minister of Foreign Affairs to allow activities or transactions that are otherwise prohibited. SEMA, FACFOA, and the Sergei Magnitsky Law set out procedures to obtain a permit (general permits can also be issued under SEMA and the Sergei Magnitsky Law), while the UNA prescribes a mechanism for obtaining a certificate to allow the proposed activities to proceed. Further, the Sergei Magnitsky Law and FACFOA allow a politically exposed or a listed person to apply for a certificate from the Minister of Foreign Affairs to exempt property from the application of the

respective order. They also allow a person claiming not to be a politically exposed foreign person or a listed person to apply for a certificate confirming such status. SEMA regulations provide for a mechanism for a designated person to have their name removed from the list or to obtain a certificate that they are not the person who has been designated.

All permits or certificates are granted on a discretionary and exceptional basis to persons in Canada or Canadians outside Canada.

8.7 Permits/Reasons for Control

(a) Export Controls

As a participating party to the Wassenaar Arrangement, Canada seeks to promote transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies and ensure that transfers of dual-use items do not contribute to the development or enhancement of military capabilities, or that these items are not diverted to support such capabilities. The Group 1 list, which is composed of dual-use items, pertains to goods and technology originally designed for civilian purposes, but that could have a military use or be used to produce military items. The Group 2 list, which is composed of items that are specially designed or modified for military purposes and those that present a strategic military concern, includes items that Canada has committed to controlling for export as a result of its participation in the Wassenaar Arrangement.

There are several distinct types of export permits under Canadian law:

- General export permits that are issued by order and available generally to all Canadians;
- Individual export permits that allow for shipments or transfers to specified consignees in a single country; and
- Multiple destination permits for dual-use items. Permits of this kind are granted on an individual basis and are subject to several conditions, but allow exporters to export items to consignees in certain group of countries.

The permit process for items of all groups is essentially the same. The permits for dual-use items and military items as well as the application process are described in detail later in the chapter.

(b) Brokering Controls

To meet its ATT obligations, Canada has recently introduced brokering controls under the EIPA. As described earlier, activity aimed to arrange or negotiate a transaction that relates to the movement of goods or technology included on the BCL from a foreign country to another foreign country constitutes brokering and requires a permit.

There are two types of brokering permits: an individual permit and a general brokering permit. General Brokering Permit No. 1 allows for the brokering of any good or technology referred to in Group 2 of the ECL if the good or technology is to be imported into an eligible country for end use in that country.[62]

(c) Types of Export Permits for Dual-Use Items

Essentially, all types of export permits are available for dual-use items. As general export permits will be discussed in the next section of this chapter, this section will cover multiple destination permits.

Multiple Destination Permits for Dual-Use Items (MDP-Dual-Use) are available to exporters of certain dual-use goods and technology identified in Group 1 or in item 5504 (strategic goods and technology) of the ECL to certain eligible destinations. MDP-Dual-Use permits are designed for use with countries that participate in all four multilateral export control regimes, namely the Wassenaar Arrangement, the Missile Technology Control Regime, the Australia Group, and the Nuclear Suppliers Group.

An MDP-Dual-Use permit can be an effective alternative to using a single export permit for each consignee and/or destination. It is intended for use by exporters that can demonstrate a record of and capacity for compliance with the EIPA. End-use information and the names of consignees do not have to be provided at the time of application but must be obtained prior to export.

There are reporting requirements under this type of permit. Certain information must be reported every six months and records must be retained for inspection upon request.

An MDP-Dual-Use may be valid for up to five years for both temporary and permanent exports.

In addition to MDP-Dual-Use permits, there are also two types of “multi-destination” export permits available for cryptographic items

controlled under Category 5, Part 2 of Group 1 of the ECL ("Information Security"): EU+5 cryptography permits and broad-based permits. These permits allow for exports to multiple countries without consignees being specified in the application.

The EU+5 permit authorizes exports of "information security" items to final consignees in all EU countries except Cyprus, as well as to Australia, Japan, New Zealand, Norway, and Switzerland. The permit specifically excludes any exports or transfers involving countries on the ACL, as well as countries that are subject to Canadian economic sanctions, including those implemented under the UNA and SEMA. There is an uncertainty about the post-Brexit status of the United Kingdom under this permit; currently the United Kingdom is mentioned on the EU+5's guidance document as a part of the EU.[63]

The broad-based permit typically can be obtained by those exporters to whom export permits have been issued in the past.

(d) Import and Export Permits for Military Items

The permits available for military items depend on the types of the equipment. Export permits issued for Group 2 items authorize the export of a maximum quantity and value of the goods and technology identified to specific customers in specific countries.

As a general rule, export permits for military items falling under Items 2-1 through 2-4 of the ECL, a group that encompass smooth-bore weapons, bombs, torpedoes, grenades, smoke canisters, rockets, mines, missiles, depth charges, and demolition devices specially designed for military use, will be issued only for a single shipment to a single consignee. In such cases, the export permit becomes invalid after the first shipment is made, even if the shipment is only a partial one.

For other Group 2 items, multiple shipment permits for up to two years may be issued, or up to five years upon request and with evidence of a long-term contract.

Permits for permanent exports of Group 2 military items may be subject to a quarterly reporting requirement.

(e) Export Permit Application Procedure

To apply for a permit, an applicant must submit an export permit application in electronic form via an online portal—NEXCOL. To apply for a permit, the applicant is required to submit information about the exporter, consignee, end user, description of goods and end use, their value, and the country of manufacture. The applicant is also required to provide supporting documentation: at least one technical document and an end-use assurance document.

The EIPA prescribes a residency requirement for export permit applications. Residents are defined as persons who ordinarily reside in Canada and corporations having their head office in Canada or operating a branch office in Canada.[64] There is no residency requirement for brokering permit applications. Any persons in Canada and Canadians operating abroad engaged in brokering activities can apply for a permit.

Processing time may vary, depending on the type of the permit, items, destinations, and end users. For export and brokering permits, the published time-frames under current service standards are normally within 10 to 40 business days. MDP-Dual-Use permits are normally issued within 40 business days. These time-frames are not mandatory and the actual processing times can exceed the specified timeline.

(f) Nuclear-Related Controls

In addition to export controls imposed under the EIPA and ECL Groups 3 (nuclear items) and 4 (nuclear-related items), transfer of nuclear goods and technology is also controlled under the Nuclear Safety and Control Act[65] and the Nuclear Nonproliferation Import and Export Control Regulations (NNPIECR),[66] which are administered by the Canadian Nuclear Safety Commission (CNSC). As a rule, the export of Group 3 and Group 4 items requires both an export permit under the EIPA and a license from the CNSC. Exporters should also be aware that some nuclear-specific and nuclear-related items that are not listed in the ECL are controlled under the Nuclear Safety and Control Act and the NNPIECR.

A CNSC export license authorizes a licensee to carry out the export activity defined in the license. The license is transaction-specific and identifies the item, quantity, end use, end user, and consignee. It may authorize shipments to single or multiple consignees in a given country. The license is normally issued within 15 to 30 business days (we note that the

actual timeframes could be longer) and is generally valid for one year. It is possible to request a longer license period to accommodate a commercial contract.

(g) Other Controls

In addition to the EIPA and the Nuclear Safety and Control Act, other Canadian legislation regulates import and export activity, including in respect of rough diamonds,[67] cultural property,[68] wildlife,[69] hazardous products,[70] and environmentally sensitive items.[71]

8.8 General Licenses/License Exceptions

(a) General Export Permits

General export permits are intended to facilitate trade in certain defined circumstances, and are issued generally to allow the export or transfer of specified goods and technology that are identified in the ECL to eligible destinations. Goods and technology listed on the ECL may not require an application for an individual export permit provided they meet certain terms and conditions set out in a General Export Permit (GEP).

If the particular exportation in issue satisfies the conditions set out in a GEP, there is no requirement to apply for an individual export permit, nor is it necessary to seek any authorization from the ECOD. However, the GEP number must be provided on the customs export declaration so that CBSA officials are in a position to verify and to satisfy themselves that the particular exportation meets the terms and conditions of the GEP. Some GEPs also contain specific requirements for pre-notification to the ECOD before use in each calendar year as well as reporting export volumes and specific final consignees.

At the present time, there are approximately a dozen GEPs in force. These include GEPs for the export of nuclear goods and nuclear-related dual-use items,[72] dual-use goods and technology,[73] personal computers and software,[74] and cryptography items.[75]

(b) License Exceptions

As each other's most important trading partner, the transfer of goods and technology between the United States and Canada proceeds with much less cumbersome trade controls. Export permits are not required for many of the goods and technologies listed in the ECL if they are destined to a consignee in the United States. There are, however, a number of key issues arising from the interaction of each country's trade control regime that U.S. and Canadian companies need to address.

(i) Export of U.S.-Origin Goods and Technology

Canada has implemented special rules for the transfer of U.S.-origin goods and technology. Item 5400 of the ECL controls transfers from Canada of all goods and technology that originate in the United States and that are not elsewhere identified on the ECL. The item specifically excludes goods that have been further processed or manufactured outside the United States so as to result in a substantial change in value, form or use of the goods or in the production of new goods.

In the distant past, there had been a practice that allowed exporters to make this determination simply on the basis of whether the U.S. content exceeded 50 percent of the value of the item to be transferred. In the authors' experience, this is not the only factor to be considered and exporters should be carefully considering whether U.S. inputs have gone through a sufficient transformation in form or use when incorporated into the new item to be exported from Canada, even if the value of the U.S. content is below 50 percent.

There are two types of export permits available for goods and technology controlled by Item 5400 of the ECL: General Export Permit No. 12 and an individual export permit.

(ii) General Export Permit No. 12

In most cases, exporters of U.S.-origin goods may rely on an exemption from this control that allows them to transfer U.S.-origin goods or technology without having to apply for and obtain a permit. GEP No. 12[76] allows for the export from Canada of any goods or technology of U.S. origin, other than those listed elsewhere on the ECL, to any destination other than an ACL country or certain U.S.-sanctioned countries.

At the present time, GEP No. 12 may not be used for transfers to Cuba, Iran, Syria, or North Korea. Canada strictly controls the export of U.S.-origin goods and technology to certain U.S.-sanctioned countries in order to ensure that Canada does not act as a conduit for avoiding the application of U.S. trade embargoes.

(iii) Individual Export Permit

If U.S.-origin items are to be transferred to Cuba, Iran, Syria, or North Korea, the exporter must apply to the ECOD for an individual export permit.

It is within the ECOD's discretion as to whether to grant a permit or not, and this may depend on many factors, including the nature of the goods or technology and the destination country. It is the experience of the authors that such permits are issued on relatively rare occasions, including where the transfer is for humanitarian purposes, the exporter has obtained a U.S. license or can show that it could benefit from a licensing exemption under U.S. law, the U.S.-origin part will be for repair or replacement of a U.S.-origin item that was previously permitted to be exported, the goods are "replacement parts" for non-U.S. origin items, the goods relate to a previously lawfully exported good of Canadian origin, the goods are part of a turnkey operation, or where the transfer is to support permissible Canadian operations in the destination country.

8.9 Penalties, Enforcement, and Voluntary Disclosures

Failure to comply with export controls or sanctions can result in the delay and detention of shipments, the imposition of administrative monetary penalties, seizure or ascertained forfeiture, and criminal prosecution.

(a) Enforcement

Implementation and enforcement of Canadian trade controls are the responsibility of the ECOD, the RCMP, and CBSA. CBSA continues to exercise its broad authority under the Customs Act and the EIPA to engage in searches, detentions, seizures, ascertained forfeitures, investigations, and other enforcement activities to ensure that exports from Canada are in full compliance with Canadian legislation. In addition to the EIPA, this includes

UNA and the SEMA regulations and the Customs Act export reporting obligations.[77]

(b) Voluntary Disclosures

Exporters and brokers that inadvertently fail to comply with the EIPA are encouraged by the government to disclose any incidents of noncompliance to the ECOD.[78] Even though there is no formalized policy that provides relief from liability under Canadian law in cases of voluntary disclosure, and the information about violations can be referred by the ECOD to CBSA or the RCMP for further investigation, it is the authors' experience that in most cases prosecution will not be pursued if the ECOD is satisfied that the disclosure was truly voluntary and complete and not reflective of an ongoing pattern of noncompliance.

8.10 Recent Export Enforcement Matters

Historically, Canada does not have an enforcement record as extensive as that of the United States regarding export controls and economic sanctions. However, in recent years Canadian enforcement agencies have conducted several seminal investigations and prosecutions under the EIPA, the UNA, and SEMA, signaling that enforcement is becoming more active.

On July 6, 2010, Canada had its first successful prosecution under the UNA Iran regulations.[79] In that case, Mahmoud Yadegari had attempted to ship from Canada to Iran dual-use pressure transducers that could be used in heating and cooling applications as well as in centrifuges for enriching uranium. An Ontario provincial court judge found that Yadegari knew or was willfully blind to the fact that the transducers had the characteristics that made them embargoed and was therefore guilty of violating the UNA Iran regulations and other federal legislation governing export transactions.[80] Yadegari was sentenced by the trial judge to 20 months of imprisonment. This sentence was further reduced by the Ontario Court of Appeal Ontario by three months.

In December 2011, Kenn Borek Air Ltd., a Calgary-based airline, was fined $25,000 under the EIPA and the Customs Act for export of one Havilland DHC-6 Twin Otter airplane and 149 aircraft parts to Myanmar in November 2007 without export permits.

On April 14, 2014, Canada witnessed its first prosecution under SEMA. In that case, Lee Specialties Ltd., a Canadian manufacturer of oil field equipment operating in Alberta, had attempted to ship to Iran Viton O-rings having a total value of $15. The Viton O-rings were intercepted by CBSA officers at Calgary International Airport. Despite their minor value, charges were laid against Lee Specialties Ltd., as the Viton O-rings could potentially be used in nuclear applications and were, therefore, prohibited under the SEMA regulations. Lee Specialties Ltd. pled guilty, was convicted, and paid a $90,000 fine as a result of this violation.

In December 2020, Canada had its first trial for SEMA sanctions violations. Nader Mohamad Kalai was charged with violating the SEMA Syria regulations by making a payment of 15 million Syrian pounds (equivalent of $140,000) to a company called Syrialink. The charges were laid by the CBSA in June 2018. Following an admissibility ruling that was unfavorable to the Crown, the Nova Scotia Supreme Court acquitted Mr. Kalai due to lack of evidence.

It is expected that enforcement will continue to intensify in the future. In a 2017 report on Canada's sanctions regime, the Standing Committee on Foreign Affairs and International Development noted there were very few prosecutions or convictions for SEMA or FACFOA, and concluded that it was not due to absence of criminal violations as such but due to them being uninvestigated.[81] The Standing Committee recommended prioritization of the enforcement of sanctions measures.

8.11 Special Topics

(a) Practical Issues Related to Export Control Clearance

(i) Screening Counterparties

Regardless of the destination country, exporters should be routinely screening all parties they deal with, and the entities that own or control them, against the lists of companies, organizations, and individuals established under the numerous SEMA and UNA regulations, the Sergei Magnitsky Law, FACFOA, as well as the Criminal Code provisions regarding dealings with terrorist entities. Canadian exporters are prohibited from engaging in dealings with these listed parties.

(ii) "Catch-all" controls

Pursuant to a "catch-all" provision in the ECL, exports of all goods and technology are prohibited without a permit if "their properties and any information made known to the exporter would lead a reasonable person to suspect that they will be used" in connection with chemical, biological, or nuclear weapons and their delivery systems or missiles (WMDs) or used in any WMD facility (even if not used in WMDs).[82] Accordingly, exporters must exercise due diligence to ensure that their uncontrolled goods and technology are not destined for a WMD end use or facility.

(iii) Mitigating Risks

Failure to comply with these requirements exposes Canadian exporters to significant financial and operational costs arising from penalty assessments as well as delayed, detained, or canceled export shipments. In many cases, there can also be disastrous reputational consequences for the company as a whole.

In order to mitigate risk, exporters should be in a position to demonstrate effective due diligence by designing and implementing a robust trade controls compliance strategy. A Canadian exporter's internal compliance program should include measures such as:

- A clearly articulated and readily accessible written manual that is regularly reviewed and updated;
- Appointing a senior officer(s) responsible for the implementation and enforcement of the policies and procedures;
- Education and training of frontline sales and other employees and executives;
- Procedures for reporting potential violations internally and externally (e.g., voluntary disclosure) and for providing protection against retaliation;
- Internal disciplinary procedures for violations;
- Destination and party screening, including the screening of customers, suppliers, freight forwarders, and other involved service providers or agents;
- End-use screening, including written certification from customers; and

- Regular auditing, testing, and enhancement of processes and procedures to ensure full compliance.

There is no one-size-fits-all compliance program, as these measures will differ depending on the size of the company; the nature of the goods, services, and technology; and its markets, customers, and end users, among other factors. Canadian companies should be conducting and updating comprehensive risk assessments of their operations when developing and maintaining their export control compliance programs. In addition, companies should be sure that their compliance policies explicitly reflect the requirements of Canadian law and not simply graft their U.S. parents' or affiliates' trade control program on to their Canadian operations.

As exporters face increasing CBSA scrutiny of their shipments, it is important to pay careful attention to trade control obligations in order to minimize noncompliance risk and avoid the financial and reputational costs associated with CBSA enforcement and delayed or canceled orders.

(b) Recordkeeping

The EIPA requires persons or organizations applying for a permit to keep all records that are necessary to determine whether they have complied with export control requirements and obligations for a period of six years after the end of the year to which they relate. Specific regulations may prescribe other durations for the retention period.

(c) How to Be Compliant When Exporting to the United States

(i) Exports of Controlled Items to the United States

While Canadian business has enjoyed permit-free export and transfer of most military items to the United States since World War II, compliance with the ATT required Canada to report on its export of full-system conventional arms, including those shipped to the United States.

To satisfy this ATT obligation, Canada has created nine ATT categories of full-system conventional arms that require a permit to be exported to the United States—these are set out in new Group 9 of the ECL. New General Export Permit No. 47 provides a streamlined permitting process that eliminates the need to file individual export permit applications for the

majority of ATT items to be exported to the United States.[83] The permit-free movement of other controlled military goods and technology to the United States remains intact.

(ii) Goods and Technology in Transit

Generally, controlled goods and technology originating outside of Canada and moving through Canada, whether in bond or cleared through customs, are subject to permit requirements.[84] There is an exception for goods or technology that moves in transit on a through journey on a billing that originates outside Canada if the billing indicates that the ultimate destination is a country other than Canada.

There is an additional requirement in order for goods or technology shipped from the United States to qualify for this exception. In such cases, the billing must also be accompanied by a certified true copy of the U.S. shipper's export declaration, and the declaration cannot contain terms that conflict with the billing.

8.12 Encryption Controls

(a) General Comments

Canada's export controls over goods, software, and technology designed or modified to perform encryption or to work with such items (as identified on the ECL) are more cumbersome than their U.S. counterparts. Often, exporters first discover that their products are subject to control when they are detained or seized by CBSA and the delays in responding to the enforcement action and obtaining a permit result in costly commercial disruption and lost sales.

Permits are not required to export cryptography and information security goods or technology from Canada to the United States.

(b) Encryption Permit Requirements

There are two GEPs relating to the export or transfer of cryptography: GEP 45—Cryptography for the Development or Production of a Product and GEP 46—Cryptography for Use by Certain Consignees.[85] These GEPs

contain annual pre-notification and reporting requirements. Prior to their first export or transfer in any calendar year, exporters are required to provide in writing to the ECOD their name, business number, and the description of the respective items. Before January 31 each year, exporters are required to file with the ECOD records on exports made during the previous calendar year.

In addition to the GEPs, in an effort to level the playing field for Canadian exporters, the ECOD has made available "multi-destination" broad based and EU+5 permits for cryptographic items that were discussed in Section 8.7. Although they still require exporters to apply to the ECOD and meet reporting and other conditions, depending on the applicable multi-destination permit, they may be obtained without having to specify consignees in the application. This avoids having to apply for individual export permits for different consignees.[86]

---

1. John Boscariol is a partner and head of the International Trade & Investment Law Group of at McCarthy Tétrault LLP. Oksana Migitko is an associate at International Trade & Investment Law Group at McCarthy Tétrault LLP.

2. Brokering controls are reviewed in greater detail in Sections 8.3 and 8.7 of this chapter.

3. *See* Global Affairs Canada, *Export and Import Controls*, https://www.international.gc.ca/controls-controles/index.aspx?lang=eng (last visited Dec. 18, 2022).

4. *See* Gov't of Canada, *Current Sanctions Imposed by Canada*, https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/current-actuelles.aspx?lang=eng (last visited Dec. 18, 2022).

5. *See* the Department of Justice, https://www.justice.gc.ca/eng/.

6. R.S.C. 1985, c. E-19, https://laws-lois.justice.gc.ca/eng/acts/e-19/index.html.

7. Nuclear Safety and Control Act, S.C. 1997, c. 9.

8. R.S.C. 1985, c. U-2.

9. S.C. 1992, c. 17.

10. R.S.C. 1985, c. D-1.

11. SOR/2001-32.

12. The Schedule to the DPA defines "controlled goods" for these purposes by reference to certain goods and technology on the Export Control List. Under the Schedule, the following are controlled goods: (1) goods of United States origin that are defense articles as defined in section 120.6 of the ITAR; (2) goods, other than goods of United States origin, that are manufactured using technical data of U.S. origin, as defined in section 120.10 of the ITAR, if the technical data is a defense article; and (3) a range of items, regardless of origin, included in the Export Control List Group 2 (munitions list), item 5504 (strategic goods and technology), and Group 6 (missile technology), the provisions of which have been modified for purposes of their listing in the Schedule.

13. SOR/89-202.

14. The current version of *A Guide to Canada's Export Controls* is dated December 2021.

15. Order Amending the Export Control List, SOR/2021-121.

16. SOR/2019-220.

17. SOR/81-543.

18. S.C. 2011, c. 10.

19. R.S.C. 1985, c. 30 (4th Supp.).
20. S.C. 2017, c. 21.
21. SOR/99-444.
22. SOR/2001-360.
23. R.S.C. 1985, c. F-29.
24. Foreign Extraterritorial Measures (United States) Order, 1992, SOR/92-584.
25. Certain Foreign Extraterritorial Measures (United States) Order, 2014, SOR/2015-12.
26. *See* Gov't of Canada, *Consolidated Canadian Autonomous Sanctions List*, https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng (last visited Dec. 18, 2022).
27. *See* United Nations Security Council Consolidated List, https://www.un.org/securitycouncil/content/un-sc-consolidated-list (last visited Dec.22, 2022).
28. SOR/2002-284.
29. *See* Pub. Safety Canada, *Currently Listed Entities*, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-en.aspx (last visited Dec. 18, 2022).
30. SOR/2002-284.
31. SOR/99-444.
32. R.S.C. 1985, c. C-46 §§ 83.02–83.04.
33. *See* Gov't of Canada, *Restricted Goods and Technologies List*, https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/goods_gechnologies-marchandises_technologies.aspx?lang=eng (last visited Dec. 18, 2022).
34. Regulations Amending the Special Economic Measures (Belarus), SOR/2022-167.
35. *See* Gov't of Canada, *Notice to Exporters and Brokers No. 1033 Exports and Brokering of Items Listed on the Export Control List and the Brokering Control List to Belarus*, https://www.international.gc.ca/trade-commerce/controls-controles/notices-avis/1033.aspx?lang=eng (last visited Dec. 18, 2022).
36. *See* Global Affairs Canada, *Measures Related to the Human Rights Situation in the Xinjiang Uyghur Autonomous Region*, https://www.canada.ca/en/global-affairs/news/2021/01/backgrounder---measures-related-to-the-human-rights-situation-in-the-xinjiang-uyghur-autonomous-region.html (last updated Jan. 18, 2021).
37. *See Global Affairs Canada Advisory on Doing Business with Xianjiang-Related Entities*, https://www.international.gc.ca/global-affairs-affaires-mondiales/news-nouvelles/2021/2021-01-12-xinjiang-advisory-avis.aspx?lang=eng (last visited Dec. 18, 2022).
38. Foreign Extraterritorial Measures (United States) Order, 1992, SOR/92-584.
39. *See* Gov't of Canada, *Export of Items Listed on the Export Control List to Hong Kong*, July 7, 2020, https://www.international.gc.ca/trade-commerce/controls-controles/notices-avis/1003.aspx?lang=eng.
40. *See* Joint Comprehensive Plan of Action, https://www.europarl.europa.eu/cmsdata/122460/full-text-of-the-iran-nuclear-deal.pdf.
41. Special Economic Measures (Iran) Regulations, SOR/2010-165, and Regulations Implementing United Nations Resolutions on Iran, SOR/2007-44.
42. *See* Global Affairs Canada, *Notice to Exporters No. 196, Exports of Items Listed on the Export Control List to Iran*, Feb. 5, 2016, https://www.international.gc.ca/controls-controles/systems-systemes/excol-ceed/notices-avis/196.aspx?lang=eng.
43. As discussed further later, ECL item 5400 controls all U.S.-origin goods and technology for export or transfer from Canada. General Export Permit No. 12 allows for the transfer of these goods and technology to any destination other than North Korea, Cuba, Syria, and Iran.

44. *See* Global Affairs Canada, *Guidance on Export Controls to Certain Destinations*, https://www.international.gc.ca/controls-controles/about-a_propos/expor/destination.aspx?lang=eng (last modified June 30, 2022).

45. The sanctions were enacted by two regulations under SEMA: Special Economic Measures (Ukraine) Regulations, SOR/2014-60 and Special Economic Measures (Russia) Regulations, SOR/2014-58.

46. Special Economic Measures (Russia) Regulations, SOR/2014-58.

47. *See* Restricted Goods and Technologies List, https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/goods_technologies-marchandises_technologies.aspx?lang=eng (last visited Dec. 22, 2022).

48. Special Economic Measures (Ukraine) Regulations, SOR/2014-60.

49. *See* Gov't of Canada, *Memorandum for Information: Update on Export Permits to Saudi Arabia*, https://www.international.gc.ca/trade-commerce/controls-controles/arms-export-saudi-arabia_exportations-armes-arabie-saoudite.aspx?lang=eng (last visited Dec. 18, 2022).

50. *See* Global Affairs Canada, *Canada Improves Terms of Light Armored Vehicles Contract, Putting in Place a New Robust Permits Review Process*, Apr. 9, 2020, https://www.canada.ca/en/global-affairs/news/2020/04/canada-improves-terms-of-light-armored-vehicles-contract-putting-in-place-a-new-robust-permits-review-process.html.

51. Special Economic Measures (Syria) Regulations, SOR/2011-114.

52. Effective Mar. 5, 2012.

53. Gov't of Canada, *Notice to Exporters No. 992—Export of Items Listed on the Export Control List to Türkiye*, Apr. 16, 2020, https://www.international.gc.ca/trade-commerce/controls-controles/notices-avis/992.aspx?lang=eng. Although the government's announcement did not discuss its policy with respect to the issuance of brokering permits for transfers of controlled items from a foreign country to Turkey, the ECOD has confirmed to the authors that a similar policy would be applied in such cases.

54. Canada also imposes certain limited prohibitions over diversion—see section 15 of the EIPA, which prohibits doing anything in Canada that causes or assists (1) the transfer of controlled goods or technology from anywhere to a country on the ACL or (2) the transfer of prohibited firearms, weapons, or their components to countries not included on the Automatic Firearms Country Control List.

55. SOR/2019-220.

56. SOR/2019-221.

57. SOR/2019-222.

58. SOR/2019-229.

59. See the text of the act to amend the EIPA and the Criminal Code, https://www.parl.ca/DocumentViewer/en/42-1/bill/C-47/royal-assent, and the ATT Package, http://gazette.gc.ca/rp-pr/p2/2019/2019-06-26/html/index-eng.html.

60. Section 2(1) of the EIPA.

61. Section 2 of SEMA, subsection 2(1) of FACFOA, section 2 of the Sergei Magnitsky Law.

62. General Brokering Permit No. 1, SOR/2019-229.

63. *See* Global Affairs Canada, *Export Permits for Cryptographic Items*, https://www.international.gc.ca/controls-controles/export-exportation/crypto/eu_5.aspx?lang=eng (last modified July 23, 2015).

64. Sections 2(1) and 7 of the EIPA.

65. S.C. 1997, c. 9.

66. SOR/2000-210.

67. Export and Import of Rough Diamonds Act, S.C. 2002, c. 25.

68. Cultural Property Export and Import Act, R.S.C., 1985, c. C-51.

69. Wild Animal and Plant Protection and Regulation of International and Interprovincial Trade Act, S.C. 1992, c. 52.

70. Export and Import of Hazardous Waste and Hazardous Recyclable Material Regulations, SOR/2005-149, under the Canadian Environmental Protection Act, 1999, S.C. 1999, c. 33.

71. Ozone-depleting Substances and Halocarbon Alternatives Regulations, SOR/2016-137, under the Canadian Environmental Protection Act, 1999, S.C. 1999, c. 33.

72. General Export Permit No. 43—Nuclear Goods and Technology to Certain Destinations, SOR/2012-89; General Export Permit No. 44—Nuclear-Related Dual-Use Goods and Technology to Certain Destinations, SOR/2012-90.

73. Dual-use Goods and Technology to Certain Destinations, SOR/2015-200.

74. General Export Permit No. Ex. 18—Portable Personal Computers and Associated Software, SI/89-121.

75. General Export Permit No. 45—Cryptography for the Development or Production of a Product, SOR/2012-160; General Export Permit No. 46—Cryptography for Use by Certain Consignees, SOR/2013-1.

76. General Export Permit No. 12—United States Origin Goods, SOR/97-107.

77. Reporting of Exported Goods Regulations, SOR/2005-23.

78. See section G.7 of the *Export and Brokering Controls Handbook* (2019).

79. Regulations Implementing the United Nations Resolutions on Iran, SOR/2007-44.

80. R. v. Yadegari, 2011 ONCA 287.

81. Report of the Standing Committee on Foreign Affairs and International Development, *A Coherent and Effective Approach to Canada's Sanctions Regimes: Sergei Magnitsky and Beyond*, Apr. 2017, https://www.ourcommons.ca/Content/Committee/421/FAAE/Reports/RP8852462/faaerp07/faaerp07-e.pdf.

82. ECL Item 5505. See Notice to Exporters No. 176: Export Controls over Goods and Technology for Certain Uses, http://www.international.gc.ca/controls-controles/systems-systemes/excol-ceed/notices-avis/176.aspx?lang=eng&view=d. This does not apply if the goods or technology are intended for end use in, and the final consignee (and any intermediate consignee) is located in, one of 29 listed allied countries.

83. General Export Permit No. 47—Export of Arms Trade Treaty Items to the United States, SOR/2019-230.

84. Item 5401, ECL.

85. General Export Permit No. 45—Cryptography for the Development or Production of a Product, SOR/2012-160; General Export Permit No. 45 Cryptography for Use by Certain Consignees, SOR/2013-1.

86. *See* Export Permits for Cryptographic Items, https://www.international.gc.ca/controls-controles/export-exportation/crypto/eu_5.aspx?lang=eng (last visited Dec. 22, 2022) and https://www.international.gc.ca/controls-controles/export-exportation/crypto/Broadbased-Elargie.aspx?lang=eng (last visited Dec. 22, 2022).

9

Extraterritoriality and Foreign Blocking Statutes

Paul M. Lalonde and Anca M. Sattler (Canada), Anahita Thoms (European Union), and Glen Kelley

9.1 Overview

The introduction of extraterritorial economic controls has led some countries to enact "foreign blocking" legislation designed to counter what they view to be the objectionable application of trade restrictions extraterritorially. These blocking measures help to protect the interests of these countries against the intrusion of foreign trade and commerce policies on their domestic actions and citizens.

However, the interaction of these measures poses compliance challenges, as these extraterritorial restrictions often directly conflict with penalties imposed through "foreign blocking" legislation. This chapter provides an overview of the "foreign blocking" legislation enacted by Canada and the European Union, as well as the legal implications for companies operating in these countries whose business operations may be subject to extraterritorial trade legislation.[1]

What is regulated: The blocking statutes seek to prohibit local compliance with certain foreign extraterritorial measures (in practice, U.S. extraterritorial sanctions on Cuba).

Where to find the regulations: The measures are contained in the Canadian Foreign Extraterritorial Measures Act (*FEMA*),[2] the EU Blocking Regulation,[3] and the Common Action 96/668 CFSP of the Council of the European Union.[4]

Who is the regulator: In Canada, the FEMA is enforced by the Attorney General of Canada and in the EU by the respective competent public prosecutor's office.

9.2 U.S. Extraterritorial Measures

The United States maintains several trade restrictions that apply outside its borders. The U.S. Cuban Assets Control Regulations (CACR),[5] administered by the U.S. Department of the Treasury's Office of Foreign Asset Controls (OFAC), imposes U.S. trade restrictions on Cuba, Cuban companies and citizens, and companies designated as "specially designated nationals."[6] The CACR provides that non-U.S. entities operating outside the United States are "persons subject to U.S. jurisdiction" who must comply with the CACR if they are owned or controlled by U.S. companies or individuals.

Similarly, the U.S. Iranian Transactions and Sanctions Regulations (ITSR)[7] administered by OFAC provide that non-U.S. entities that are owned or controlled by U.S. companies or individuals are generally prohibited from engaging in a transaction with the government of Iran, Iranian companies and individuals, if the transaction would be prohibited for a U.S. person. While the JCPOA (Iran nuclear agreement) was in effect, certain conduct by such non-U.S. entities was authorized by OFAC General License H, from January 2016 through June 2018.

The Helms-Burton Act of 1996[8] purports to apply to all companies carrying on business in or with Cuba, including Canadian and other non-U.S. companies. It prohibits trade between Cuba and foreign subsidiaries of U.S. corporations, and provides civil penalties for violations, including fines and the forfeiture of property. These provisions are implemented through the CACR.

Title III of the Helms-Burton Act gives U.S. citizens with claims to Cuban property confiscated by the Castro regime the right to sue any person or entity that traffics in confiscated property. Until recently, Title III of the Helms-Burton Act had been suspended by various U.S. Presidents since it was enacted. The suspension only applied to the right to sue and did not relieve a person of potential future liability. On May 2, 2019, U.S. Secretary of State Michael Pompeo announced that President Trump would not continue the historic suspensions, thus making it possible that persons dealing in confiscated property may be liable retroactively.[9] U.S. nationals are now able to file lawsuits in federal court against any individual or entity that "traffics" in property confiscated by the Cuban government on or after

January 1, 1959—a time span of more than 60 years.[10] While the volume of such lawsuits has been lower than many commentators had predicted, since May 2019, plaintiffs have brought Helms-Burton lawsuits against U.S. and international companies, such as cruise ships, hotels and related booking agencies, and airlines, among others. Many of these lawsuits center around the definition of "trafficking" in Title III, which is broad but also includes exceptions, including one that proved successful for defendants who had the burden to prove that transactions and uses of property were incident to lawful travel to Cuba.

Title IV of the Helms-Burton Act directs the U.S. government to deny entry to a non-U.S. citizen (and his or her spouse, minor child, or agent), if the non-U.S. citizen converts or traffics in confiscated property or is an officer or principal or controlling shareholder of an entity that converts or traffics in confiscated property.[11] These sanctions have been applied only very rarely, but since the law remains on the books and with the availability of Title III claims, it could be used in future.[12]

The Export Administration Regulations (EAR),[13] a broad set of export control regulations administered by the Bureau of Industry and Security in the U.S. Department of Commerce, has significant extraterritorial reach. The EAR generally regulates exports and transfers occurring entirely outside the United States of goods, software, or technology (items) that are of U.S. origin, that contain more than 25 percent U.S.-origin export-controlled content (or 10 percent for embargoed countries like Cuba), or that are the "foreign direct product" of certain U.S.-origin software or technology. In this way, the U.S. extends its trade laws to the conduct of non-U.S. parties outside the United States involving items that originated in the United States, or involving items that contain or are based on items that originated in the United States.

In addition, since 1996, the U.S. government has maintained "secondary sanctions" under which the U.S. Departments of State or of the Treasury (State or Treasury) may impose blocking (asset freezing) or other sanctions on any non-U.S. party determined to have engaged in specific types of transactions. Secondary sanctions were first imposed in 1996 as part of the Iran Sanctions Act, originally named the Iran and Libya Sanctions Act.[14] U.S. secondary sanctions relating to Iran have been greatly expanded over

the years since 2010, when the Comprehensive Iran Sanctions, Accountability and Divestment Act of 2010 (CISADA)[15] was enacted.

Since 2017, U.S. Congress and successive U.S. Presidents have created new secondary sanctions measures, in statutes and in Presidential Executive Orders, relating to Russia, North Korea, and Syria. Currently, State or Treasury can enforce secondary sanctions against a non-U.S. party carrying out a transaction outside the United States, with no connection or contact to the United States, if State or Treasury determine that the party has:

(a) Provided "material support" or engaged in a "significant transaction" for Iranian, Russian, North Korean, or Syrian designated parties (meaning parties on U.S. sanctions lists);
(b) Engaged in specified activities relating to the Iranian petroleum, mining, financial, construction, industrial, automotive or other manufacturing, metals, or textiles sectors; or
(c) Engaged in specified activities relating to the Russian oil and gas, military, or intelligence sectors.

9.3 Canada—The Foreign Extraterritorial Measures Act

(a) Overview of the FEMA

Canada has implemented blocking legislation specifically aimed at reducing the impact of the U.S. extraterritorial measures. Introduced in 1985, Canada's FEMA was originally designed to blunt the impact of U.S. antitrust legislation. However, it has only ever been used to protect Canadian interests against the U.S. Cuban embargo laws.[16]

(b) The Principal FEMA Countermeasures

FEMA contains four principal countermeasures against the extraterritorial application of U.S. Cuban embargo laws.

(i) Restriction of Production of Records to a Foreign Tribunal

The first countermeasure allows Canada's attorney general to order Canadian records and/or information not to be produced or disclosed to a

foreign tribunal, as well as prohibit or restrict the giving of evidence by a Canadian citizen or resident in foreign proceedings.[17]

(ii) Blocking the Judgment of Specific Foreign Trade Laws

The second countermeasure empowers the attorney general to maintain a schedule of foreign trade laws deemed contrary to international law or international comity and to block any judgment made pursuant to legislation listed in that schedule.[18] Currently, the only foreign trade law included in the schedule is the Helms-Burton Act. The Canadian government has taken the additional precautionary measure of specifying that no judgment given under the Helms-Burton Act shall be recognized and enforceable in Canada.[19] As such, no additional order is required to block the enforcement of a Helms-Burton Act judgment.

(iii) Clawback Provisions to Recover Damages

The third countermeasure is a "clawback" provision that allows a Canadian defendant in foreign proceedings brought under an instrument listed in the FEMA schedule to sue in a Canadian court to recover the judgment sum, expenses, and consequential loss or damage suffered by reason of the enforcement of the foreign judgment.[20]

A defendant also has the right, at any point during a proceeding instituted pursuant to an instrument listed under the FEMA schedule, to sue for the recovery of costs incurred in defending that proceeding even before a final judgment is made.[21] Moreover, where a Canadian court makes an order in favor of the Canadian defendant, the court is authorized, in addition to any other means of enforcing judgment, to order the seizure and sale of any property in which the foreign plaintiff has a direct or indirect beneficial interest, notwithstanding that such property may be located outside Canada.[22]

(iv) Notification Obligations and Noncompliance Orders

The fourth countermeasure is the notification obligations and noncompliance orders. Where a foreign state or tribunal takes measures affecting Canadian interests in international trade or infringing on Canadian sovereignty, the attorney general may issue orders requiring a person in

Canada to notify the attorney general of "any directives, instructions, intimations of policy or other communications relating to such measures from a person who is in a position to direct or influence the policies of the person in Canada."[23] In addition, the attorney general may also prohibit any person from complying with any such directive or communication from a person who is in a position to direct or influence the policies of the person in Canada.[24]

(c) The FEMA Order

To specifically address notification and noncompliance obligations in respect of the U.S.–Cuban legislative embargo measures and under its authority granted by FEMA under section 5, the attorney general issued the Foreign Extraterritorial Measures (United States) Order (1996) (the "1996 FEMA Order").[25]

The 1996 FEMA Order requires every Canadian corporation and every director and officer of a Canadian corporation to "forthwith give notice" to Canada's attorney general of any directive or communication relating to an "extraterritorial measure" of the United States in respect of any trade or commerce between Canada and Cuba received by the Canadian corporation from a person who is in a position to direct or influence the policies of the Canadian corporation in Canada.[26] The term "extraterritorial measure" is very broadly defined so as to cover the Helms-Burton Act plus any other instruments designed to enforce the U.S. embargo against Cuba.[27]

The 1996 FEMA Order also contains specific obligations prohibiting compliance with an extraterritorial measure of the United States by a Canadian corporation, including its directors, managers, and employees in a position of authority.[28] These noncompliance obligations apply in "respect of any act or omission constituting compliance" irrespective of whether or not "compliance with the extraterritorial measure or communication is the only purpose of the act or omission."[29]

This broad application of the noncompliance order places corporations with a number of legitimate reasons for not trading with Cuba in a precarious situation.[30] Canadian companies who refuse to trade with Cuba for legitimate business reasons might still be viewed as acting in compliance with the U.S. measure if one of the reasons for the company's

act or omission was the existence of a U.S. measure. The actual degree of reliance placed on the existence of the U.S. embargo (as opposed to another legitimate business reason) in the decision-making process seems to be irrelevant and the existence of legitimate business reasons does not shield the company from criminal prosecution under FEMA.

While the notification obligation under the 1996 FEMA Order applies only to the Canadian corporation and its directors and officers, the noncompliance obligation also includes managers and employees in a position of authority. Accordingly, managers and employees in positions of authority are not obliged to notify the attorney general of communications from their superiors but they are subject to the noncompliance obligation with respect to the content of those communications.[31]

(d) Enforcement of and Penalties under FEMA

(i) Enforcement of FEMA

It is challenging to assess risk under FEMA as there are very few enforcement statistics under the legislation. No prosecutions under the legislation have been brought in front of the Canadian courts. Investigations by Canadian authorities into allegations of Canadian companies following directives from U.S. parent corporations to cease engaging in business relationships with Cuba are not generally publicized, and their results are not reported.[32]

Soon after Title III of Helms-Burton Act came into force in the United States, the Honorable Chrystia Freeland, then Minister of Foreign Affairs and Honorable David Lametti, Minister of Justice and Attorney General of Canada, issued a joint statement to reaffirm the government of Canada's commitment to defend Canadians and Canadian businesses conducting legitimate trade and investment in Cuba, and reassure Canadians that the government is reviewing all options in response to the U.S. decision to fully implement Title III of the Helms-Burton Act to stand up for Canadian businesses.[33] The Department of Justice (DoJ), which oversees the administration and enforcement of FEMA, has also published a fact sheet containing an outline of the process to recover damages and/or expenses related to a final U.S. judgment through the application of FEMA.[34]

(ii) Penalties under FEMA

FEMA authorizes the Canadian government to prosecute violations of FEMA orders made under sections 3 and 5 either by indictment or summary conviction. Under indictment, the maximum fines are CAN$1.5 million for a corporation and CAN$150,000 for an individual. An individual may also face up to five years imprisonment.[35] In the case of a summary conviction, the maximum fines are CAN$150,000 for a corporation and CAN$15,000 for an individual. Moreover, an individual may be liable to imprisonment for a term not exceeding two years.[36] The penalties under section 7 apply irrespective of whether the violation of the notice or noncompliance order occurred in Canada or outside of Canada.[37]

In considering the actual sentence to be imposed for an offence contrary to FEMA, a court may take into account a number of factors, including (1) the degree of premeditation in the commission of the offense; (2) the size, scale, and nature of the offender's operations; and (3) whether any economic benefits have, directly or indirectly, accrued to the offender as a result of having committed the offence.[38]

The term "premeditation" relates to the mental element of the offence, such as the planning and deliberation. Although the prosecutor does not have to establish premeditation to obtain a conviction, the court is directed to impose a higher penalty if premeditation can be established.[39]

Although FEMA does not clarify the "size, scale and nature of the offender's operations" criterion, there is a strong chance that companies with relatively large-scale dealings or operations in Cuba will be subjected to more severe penalties than those companies whose operations are on a smaller scale. This is predicated on the view that the larger the size and scale of the Canadian offender's operations, the greater the profile and impact of its conduct on public awareness, and correspondingly the greater the effect the U.S. extraterritorial measures would have had in violating Canadian sovereignty.[40]

It is unclear how the courts might quantify the economic benefit obtained by the offender in complying with the U.S. extraterritorial measure. Ostensibly, the larger the net economic benefit accruing to a company by virtue of compliance with the U.S. measure, the larger the sentence and fine to be imposed on the offender,[41] but it is difficult to imagine a scenario where compliance with U.S. sanctions would generate a measurable net benefit. Rather, compliance with U.S. sanctions is more

likely to lead to lost business opportunities, rather than to any revenue-generating transactions.

(e) The Interaction of FEMA and the Extraterritorial Measures

(i) The Conflict between FEMA and the Extraterritorial Measures

Although independent Canadian-owned businesses are unlikely to be caught by the overlap between the application of FEMA and the U.S. extraterritorial trade restrictions with respect to the CACRs, Canadian entities with U.S. affiliates are at risk of being in scenarios that expose them to liability under either the U.S. trade embargo regime or the Canadian measures.

In the event a Canadian subsidiary places the U.S. parent in breach of the Cuba embargo regulations, the U.S. parent is likely to issue a communication or directive to the Canadian subsidiary to halt all business activities pertaining to Cuba. Pursuant to the 1996 FEMA Order, the existence and content of such communications would have to be reported to Canada's attorney general, and the Canadian subsidiary would be obliged not to comply with such directive. Where the Canadian subsidiary elects not to comply with the directive, the U.S. parent will be subjected to the sanctions applicable under the U.S. regime.

Walmart Canada (a wholly owned subsidiary of a U.S. corporation) faced this dilemma when, after it became aware that some of the pajamas being sold in its Canadian stores were manufactured in Cuba, it took the merchandise off its shelves to avoid legal action against its U.S. parent. The Department of Foreign Affairs and International Trade Canada (DFAIT, now GAC) referred the matter for investigation by the Canadian DoJ. However, two weeks after pulling the merchandise off the shelf, Walmart Canada recommenced distributing the pajamas in its Canadian stores, after concluding, following legal consultation, that it did not contravene U.S. law, since the pajamas were purchased from a Canadian distributor.[42] While OFAC announced that it was launching an investigation into this matter and that it was intent on enforcing the Cuban embargo, no criminal prosecution materialized initially.[43] Later, OFAC levied a $50,000 fine against Walmart Canada. After consultations with government lawyers, Walmart paid the

fine voluntarily without any determination that a violation had been committed.[44]

(ii) FEMA and Helms-Burton

Companies and individuals may also face challenges in relation to the application of the Helms-Burton Act to any Canadian individual and company trafficking in confiscated property. When Sherritt Inc., the largest Canadian private investor refused to divest itself of Cuban property after receiving exclusion notices related to Title IV of Helms-Burton, a ban from entering the United States was enacted on nine of its executives.[45] Since then, as Sherritt continued its expansions into Cuba, the ban was expanded to include some of Sherritt's new officers.[46] Until recently, apart from the Sherritt case, however, the U.S. government has rarely even threatened to apply the entry ban, thereby leaving it as a real, but low, risk for non-U.S. companies doing business in Cuba.[47] In February 2020, the chief executive officer of the Spanish hotel chain Melia was banned from entering the United States over the company's operations in Cuba. According to Melia, American officials cited two hotels affiliated with the company in the Cuban region of Holguin, claiming they are on a plot of land expropriated by the state in the 1950s.[48]

Now that Title III of Helms-Burton (allowing companies to be sued for trafficking in expropriated property) is no longer suspended, Canadian entities carrying on business in Cuba (especially where such entities have U.S. assets) may face substantial risk. Such entities have to consider whether to cease dealing in confiscated property and face sanctions under FEMA or open themselves to civil lawsuits.

(iii) Complying with Export Administration Regulations

Compliance with US export controls set out in the EAR may also attract liability under FEMA. The EAR is administered by the U.S. Department of Commerce's Bureau of Export Administration and regulate the export and re-export from third countries to Cuba of goods originating from the United States through licensing requirements, such as where the goods are of U.S. origin, where the goods are of foreign origin but the U.S. content exceeds 10 percent of the total value of the goods exported, and where the goods are of foreign origin but are the direct product of certain U.S. technology.[49] In

fact, the EAR requires a license even for the export to Cuba of goods subject to the EAR that are *not* on the commerce list—that is, EAR99 goods—in all but a very few circumstances where license exceptions are available.

Canada's export licensing authority, the Export Controls Divisions (ECD) of GAC, acknowledges to a limited extent the application of U.S. regulations to the re-export of U.S.-origin products to Cuba by requiring Canadian exporters of U.S.-origin items to apply for an export permit to Cuba.[50] However, no export permit is required where U.S.-origin goods have undergone transformation resulting in a substantial change in value.[51]

Canada's GAC has taken the view that, to the extent the EAR hinders trade relations between Canada and Cuba, it is an extraterritorial measure that falls under the scope of FEMA.[52] As such, compliance with the licensing permit requirements may place a Canadian company in contravention of FEMA. The mere act of complying with an American regulation that imposes obligations on Canadian entities with no direct connection to the United States is a violation of Canadian sovereignty and may be targeted for sanction under FEMA.

Where U.S.-origin content exceeds the substantial transformation threshold, a Canadian company will need to apply for a permit to export the goods to Cuba. Only where the permit is denied by Canadian authorities can the Canadian company safely refuse to export such goods to Cuba.[53]

The reality, however, is that there are instances where Canadian export authorities actually *do* grant permits for Canadian companies to export U.S. origin goods to Cuba, thereby placing Canadian companies in violation of their obligations under the EAR, a set of regulations that was not the target of the 1996 FEMA Order. Although there exists no formal government of Canada policy on the matter, it appears from experience that permits to export U.S. origin goods to Cuba may be granted (even where no U.S. re-export authorization is granted) in the following circumstances:

- If the goods are "replacement parts" for non-U.S. origin items;
- If the goods relate to a previously lawfully exported good of Canadian origin;
- If the goods are part of a turn-key operation (e.g., if a Cuban hotel is ordering a complete kitchen and it contains an appliance made in the

United States on the grounds that the "majority" of the shipment is not U.S. made); and

- If there is a humanitarian reason for the export.[54]

(iv) Consideration of FEMA in the U.S. Courts

While FEMA has received no judicial consideration in Canada, a U.S. decision has discussed the application of FEMA in the context of the obligations imposed on foreign corporations by the Trading with the Enemy Act of 1917 (TWEA)[55] and the CACRs.

In *United States of America v. Brodie*,[56] the Pennsylvania District Court convicted James Sabzali, a Canadian citizen, on 21 counts of conspiracy to violate the TWEA and the CACRs.[57] From 1992 through 1996, Sabzali worked as a sales representative in Canada selling U.S.-made water purification supplies to Cuba. He operated out of the Hamilton office of Purolite Canada, the Canadian subsidiary to Bro-Tech (a U.S. chemical company). During that time, he made more than 20 trips from Canada to Cuba on behalf of U.S. and Canadian chemical companies.[58]

The *Brodie* case is significant in a Canadian context for two reasons: (1) it is the first time that a Canadian citizen was convicted for violating the CACRs; and (2) it clarifies the U.S. position with respect to the availability of the defense of foreign sovereign compulsion in relation to liability under the U.S.-Cuba trade embargo regulations.

In *Brodie*, the court rejected the argument that a blocking statute such as FEMA could form the basis of a foreign sovereign compulsion defense. The court read FEMA as prohibiting persons from "not trading with Cuba" if the decision to do so was exclusively because of the CACRs. For the defendant to mount a successful foreign sovereign compulsion defense, it would have to prove that its motivation for trading with Cuba was based on fear of prosecution under Canadian law and that it could not have legally refused to accede to the Canadian government's wishes.

While this view is consistent with previous U.S. court decisions denying a conflict where it is possible to comply with both foreign and U.S. law,[59] it appears to be at odds with the broad scope of the noncompliance obligation imposed by the 1996 FEMA Order, which provides that as long as U.S. law is one of the reasons for ceasing to engage in business with or in Cuba, a Canadian company is in breach of this obligation.

Sabzali was also unable to establish that compliance with the Canadian laws was basic and fundamental to the alleged behavior because the alleged offences to which FEMA may have applied occurred prior to the introduction of the 1996 FEMA Order. Prior to the time, the noncompliance obligation was only imposed on corporations, and did not include directors, officers, managers, and employees in positions of authority as under the 1996 FEMA Order.

While *Brodie* gave cross-border companies a better understanding of the interaction between FEMA and the U.S. anti-Cuba measures, the Pennsylvania District Court later overturned the guilty verdict citing grievous prosecutorial misconduct.[60] While a new trial was ordered for Sabzali, a plea bargain was reached before the new trial took place.[61] As a result, the state of the law remains unclear. Furthermore, even if *Brodie* had not been overturned, it could be argued that due to the coming into force of the 1996 FEMA Order, the *Brodie* case is distinguishable from any new case dealing with post-1996 acts.[62]

(f) Shielding Companies from Liability

There are a variety of measures and practices that, depending on the circumstances, may help cross-border companies manage risk sensibly. Canadian experts have suggested the following best practices to help avoid a conflict between the application of the 1996 FEMA Order and the CACRs:

1. Brief the U.S. parent corporation managers about the Canadian legal implications of foreign directives before they are sent;
2. Maintain Canadian-specific export control manuals, policies, and training programs at the Canadian subsidiary's registered office;
3. Employ careful wording of all written and verbal communications from persons in authority at U.S. parent corporations to ensure that they cannot be characterized as foreign directives;
4. Limit or eliminate embargo communications between U.S. parents and Canadian subsidiaries;
5. Where appropriate given the nature of the communications, have all relevant communications from U.S. parent corporations sent through lawyers to shield them with solicitor–client privilege;

6. When withdrawing from Cuba or declining to pursue a trade or investment opportunity in Cuba for legitimate business reasons, ensure that those reasons are well documented;
7. Employ various corporate restructuring methods to spin off Cuban investments into separate entities;
8. Review for FEMA exposure any intercompany agreements and the Canadian subsidiary's contracts, purchase orders, and so on with unrelated parties; and
9. Consider whether any provincial business practices legislation is applicable.[63]

With respect to potential liability under the Helms-Burton Act, the advice is much simpler. Before investing in Cuban property, it is essential to carefully investigate whether such Cuban property may be confiscated property under Title III.[64]

(i) Actions to Take Following a Potential Contravention

If a Canadian company is caught in the crossfire of conflicting obligations under FEMA and a U.S. extraterritorial measure, the first step is to ascertain whether the U.S. measure falls within the ambit of the 1996 FEMA Order. If so, the company needs to determine whether the measure operates to reduce or impede trade or commerce between Canada and Cuba.[65] It is also essential to establish whether the Canadian subsidiary is in fact a "Canadian corporation" under the 1996 FEMA Order.[66]

With respect to communications between U.S. parents and Canadian subsidiaries, the Canadian subsidiary should determine (1) whether the communication is in the nature of a "directive" or "intimation of policy"; and (2) whether the source of the communication is in "a position to direct or influence the policies of the Canadian corporation in Canada."

As for the noncompliance obligation, the next step is to establish whether the Canadian company's act or omission constitutes "compliance" under the 1996 FEMA Order. This analysis involves establishing the principal reason for the Canadian company's act or omission. Is the act or omission carried out to comply with Canadian law, or are there other business reasons?[67]

Last but not least, if goods are to be supplied to Cuba, the Canadian company needs to ascertain the U.S.-origin content of the merchandise to

determine whether such goods have been sufficiently transformed outside the United States.

9.4 European Union: The EU Blocking Regulation

(a) Overview

In 1996, the EU held the view that the extraterritorial aspects of the aforementioned U.S. sanctions laws infringed public international law.[68] Therefore, as a reaction, the EU passed two legal acts, the EU Blocking Regulation, and Common Action 96/668CFSP of the Council of the European Union.

Following the U.S. withdrawal from the Joint Comprehensive Plan of Action (the so-called Iran Nuclear Deal) and the reintroduction of U.S. sanctions against Iran, on August 7, 2018, and November 5, 2018, the EU Commission amended the Annex to the EU Blocking Regulation.

(b) Rationale of the EU Blocking Regulation

The rationale of the EU Blocking Regulation, as outlined in its preamble, is based on the objectives of the EU, which include "contributing to the harmonious development of free trade and to the progressive abolition of restrictions on international trade" and "the objective of free movement of capital between Member States and third countries." In the European Council's view, these objectives are impeded by the extraterritorial application of laws, regulations, and other legislative instruments enacted by third countries and purporting to regulate activities of natural and legal persons under the jurisdiction of the EU member states.[69]

Although the EU Blocking Regulation was a direct reaction to specific U.S. sanctions laws, it was designed in a manner that allows its application to any other laws with extraterritorial effects, once these laws are added to the Annex of the EU Blocking Regulation.

(c) Scope of Application

The scope of application of the EU Blocking Regulation mirrors the principles of territorial and personal jurisdiction recognized under

international law.[70] Pursuant to Article 11, the EU Blocking Regulation applies to:

- Any natural person who is resident in the EU *and* is a national of a member state;
- Any legal person incorporated within the EU;
- Any national of a member state established outside the Union and any shipping company established outside the Union and controlled by nationals of a member state, if their vessels are registered in that member state in accordance with its legislation;
- Any other natural person being a resident in the EU, unless that person is in the country of which he is a national; and
- Any other natural person within the Union, including its territorial waters and air space and in any aircraft or on any vessel under the jurisdiction or control of a member state, acting in a professional capacity.

However, the EU Blocking Regulation only applies when these persons are engaged in international trade and/or the movement of capital and related commercial activities between the EU and third countries.[71]

The material scope of the EU Blocking Regulation is set forth in its Article 1. According to this provision, the EU Blocking Regulation applies only to the effects of the extraterritorial application of the laws specified in its Annex, including regulations and other legislative instruments and of actions based thereon or resulting therefrom. The following statutes and regulations are listed in the Annex:

- The National Defense Authorization Act for the Fiscal Year 1993, Title XVII; Cuban Democracy Act 1992, sections 1704 and 1706
- The Cuban Liberty and Democratic Solidarity Act of 1996
- The Iran Sanctions Act of 1996
- Iran Freedom and Counter-Proliferation Act of 2012
- National Defense Authorization Act for Fiscal Year 2012
- Iran Threat Reduction and Syria Human Rights Act of 2012
- Iranian Transactions and Sanctions Regulations

The European Commission can add or delete, where it deems appropriate, references to regulations or other legislative instruments deriving from the laws specified in the Annex. Regardless of the recent

amendment to the Annex, legal uncertainty, as discussed later, remains as to whether the EU Blocking Regulation automatically takes into account changes in foreign law that are not explicitly referred to in the Annex to the EU Blocking Regulation.

(d) The Principal Countermeasures

The EU Blocking Regulation contains four principal countermeasures against the extraterritorial application of the listed U.S. sanctions laws.

(i) Obligation to Inform the Commission

According to Article 2 of the EU Blocking Regulation, EU persons and companies are obliged to inform the European Commission within 30 days if their economic and/or financial interests are affected, directly or indirectly, by the listed U.S. sanction laws. Insofar as the interests of a legal person are affected, the obligation applies to its directors, managers, and other persons with management responsibilities.[72] The information can also be submitted to the European Commission through the competent authorities of a member state.[73]

(ii) Prohibition of Enforcement and Recognition

Article 4 of the EU Blocking Regulation stipulates that no judgment of a court or tribunal or decision of an administrative authority located outside the EU giving effect directly or indirectly to the listed U.S. sanctions laws shall be recognized or be enforceable in any manner. With this provision, the EU and its member states insist on their territorial sovereignty.[74] The broad language of the provision explicitly includes decisions of administrative authorities such as administrative sanctions available under the ILSA.[75]

(iii) Prohibition of Compliance

While Article 4 aims at blocking the enforcement of decisions that have already been taken by the relevant authorities outside the EU, Article 5 of the EU Blocking Regulation is directed at the addressees of the listed U.S. sanctions laws.

It expressively prohibits affected persons to comply directly or indirectly, and through a subsidiary or other intermediary persons, with any requirement or prohibition based on or resulting from the listed laws. Additionally, the ban covers not only compliance with legislative measures but also judicial decisions. The European Commission may authorize exceptions to the extent that noncompliance would seriously damage their interests or those of the EU.[76]

On that account, the Commission adopted the Implementing Regulation[77] on August 3, 2018, providing guidance on the interpretation of the EU Blocking Regulation with respect to the authorization requirement. Pursuant to Article 4 of the Implementing Regulation, the Commission must take the established criteria into consideration when assessing whether there would be serious damage to the protected interests within the meaning of Article 5 of the *EU Blocking Regulation*. The precise criteria laid down in Article 4 of Implementing Regulation, among others, include adverse effects on the conduct of economic activity; consequences for the internal market in terms of free movement of goods, persons, services and capital; as well as financial and economic stability of key Union infrastructures; and systemic implications of the damage. However, the criteria are themselves open to interpretation.

The authorization is only granted in exceptional cases. On that basis, the preceding requirements will be interpreted narrowly. Applicants must prove exceptional circumstances justifying compliance with the acts listed in the Annex, where the Commission will accordingly issue its decision following consultation with the Committee on Extra-Territorial Legislation.

Pursuant to number 20 of the Guidance Note,[78] a request for a compliance authorization does not have suspensive effect. Unless the relevant applicant receives such compliance authorization, there is no entitlement to comply with the U.S. acts listed in the Annex to the EU Blocking Regulation.

With this provision, the EU imposes a legal obligation upon the protected persons, which is diametrically opposed to the listed U.S. sanction laws. It *prohibits what is prescribed* by the listed U.S. laws and *prescribes what is prohibited* by the listed U.S. laws. Thereby it intends to allow for the invocation of the foreign state compulsion doctrine[79] before U.S. courts.[80]

(iv) “Clawback” Clause

Finally, Article 6 of the EU Blocking Regulation, titled as the “cornerstone” of the EU Blocking Regulation, goes a step further and provides for a clawback of damages. According to Article 6, persons affected by the listed U.S. sanctions laws shall be entitled to recover any damages, including legal costs, caused by the application of the listed laws or actions based thereon. The recovery may be obtained from the person that caused the damages.[81]

This provision aims at a complete neutralization of the effects of the U.S. sanctions imposed by Title III of the Helms-Burton Act, by creating a tort claim that is based on the U.S. administrative and judicial decisions as the event constituting the claim.[82] It is more extensive than typical clawback clauses, as it is not only directed against judgments but designed as a general damage claim that encompasses not only punitive damages but also compensatory damages including ancillary claims and legal costs. Thus, the claimant may retrieve anything that he has lost in previous U.S. proceedings.[83]

In order to facilitate the enforcement of the damages claims, Article 6 even allows for initiating judicial proceedings in the courts of any member state where the person causing damages holds assets.[84] Finally, Article 6 paragraph 4 of the EU Blocking Regulation highlights how extensively the provision is drawn. In order to give greater effect to the clawback, the recovery can take the form of seizure and sale of assets held by the persons and entities causing the damages and persons acting on their behalf or intermediaries in the EU, including shares held by a legal person incorporated within the EU.

(e) Penalties and Enforcement

Since provisions relating to criminal and administrative penalties can only be adopted by the member states of the EU, the penalties available in the event of a breach of an obligation under the EU Blocking Regulation depend on the national legislation of the respective member state. While, for example, Austrian law also explicitly provides for a penalty for the breach of the obligation to inform the European Commission as stipulated in Article 2 of the EU Blocking Regulation,[85] the German statutory law

only provides a penalty for the breach of Article 5. In Germany, the infringement of Article 5 is punishable by a fine of up to 500,000 euro.[86]

As publicly available information is limited, it is difficult to assess the actual enforcement of the EU Blocking Regulation. So far, there has not been any report on judicial decisions in criminal matters. However, member states have proven themselves to be willing to take action and pursue investigations of EU-based companies complying with U.S. sanctions law. The following cases have been discussed in publicly available sources. In November 2018, as a response to the U.S. sanctions, the German telecommunications provider Deutsche Telekom cut off the telephone and internet access of its customer, the Iranian Bank Melli. Bank Melli went on to file law suits against Deutsche Telekom, and in the proceedings before German District Courts and Higher Regional Courts, Deutsche Telekom was ordered to reactivate its services for the bank. The court based its decision on the view that a termination of business relations solely based on the motive of not being exposed to U.S. sanctions is a violation of the EU Blocking Regulation. Otherwise, the Regulation would lose its purpose. Deutsche Telekom inter alia argued that its U.S. subsidiary T-Mobile U.S. would have to fear a loss of revenue and potentially sanctions by the U.S. authorities that could lead up to an exclusion from the U.S. market if its parent company did not comply with U.S. regulations.[87] In view of the challenging situation for European companies, the Higher Regional Court subsequently made a request to the European Court of Justice (ECJ) for a preliminary ruling on Article 5 of the EU Blocking Regulation, which is still pending.

In the most high-profile case, the Austrian government initiated a legal enforcement procedure against one of its largest banks, BAWAG P.S.K., which in 2007 had reportedly closed accounts held by around 100 Cuban clients in order to comply with U.S. laws and thereby not to put at risk the expected takeover by an American private equity firm. When BAWAG applied for and was apparently granted a specific license from OFAC to reinstate the accounts of the Cuban nationals, the Austrian government dropped the charges against BAWAG.[88]

In the UK in 2010, Lloyds TSB reportedly refused to cash checks that were issued by Cuba-based banks. Lloyd had blocked a bank transfer from Cuba to a UK business that supplies agricultural consultancy services, despite the free flow of trade between the Caribbean country and the EU.

This came after Lloyds had already felt the full weight of the U.S. regulatory authorities, being forced to pay $350 million in January 2009 after being accused of helping clients in Iran, Libya, and Sudan to avoid U.S. sanctions. The sanctions power exercised by the United States was also on display when Barclays was fined in August for allegedly infringing U.S. sanctions through business dealings with persons linked to Cuba, Iran, Libya, Myanmar, and Sudan. The British bank agreed to pay a $298 million fine covering business transactions worth $500 million. The upshot was that Barclays has told customers it no longer handles any business with links with Iran, North Korea, Myanmar, or the sanctioned areas of Sudan. According to press reports, Lloyds modified its practice after the UK government's Department for Business, Innovation and Skills became informally involved.[89]

In 2011, a German online seller initiated civil proceedings before a German civil court, after the internet payment company PayPal closed his account, reportedly because the German online seller had been selling Cuban rum among other types of alcohol and alcohol-related products.

The embargo on goods from Cuba had existed in the United States since 1962. It was not expected that this almost 50-year-old ban could also affect private sellers of rum. After all, the company did not deliver to the United States. Neither the seller nor his customers are subject to American laws. Payment transactions always ran to full satisfaction through the American payment service provider with a European banking license. PayPal noted that as long as Cuban goods are sold, PayPal would no longer accept him as a customer. However, in this case, the court did not render a judgment, as the parties reportedly reached a settlement under which PayPal reopened the account of the German online seller who in turn refrained from using PayPal with respect to payments for Cuban goods.[90]

(f) The Blocking Regulation and CISADA

After global political pressure on Iran increased in 2010, the U.S. passed CISADA and the ITR Act, each of which significantly expanded the ISA and other U.S. sanctions measures targeting Iran. As the Annex to the EU Blocking Regulation had not been amended back then, since its enactment in 1996, it did not specifically refer to CISADA or the ITR Act. Therefore, the question arose whether CISADA and the ITR Act were encompassed by

the EU Blocking Regulation. The principal issue behind this question is whether the references in the Annex to the EU Blocking Regulation are static and thus relate only to the version of the legislation at the time of the drafting or whether the references need to be interpreted as dynamic and thus automatically taking into account the changes of the law and referring to its latest version.

This question has not yet been answered by the European authorities. However, the wording of the EU Blocking Regulation suggests that the Annex is static, because it refers only to the specific legal texts in the Annex. Although the object and purpose of the EU Blocking Regulation to counter the extraterritorial effects of foreign legislation might argue for another conclusion, it appears unlikely that the drafters intended to create such a dynamic reference. Being fully aware that sanction laws are subject to periodical renewals and often adapted to political changes, the drafters could have easily added a clause to the effect that the Blocking Regulation applies to the latest version of each listed law.

Against this background, the references in the Annex cannot be interpreted as being dynamic. Any other interpretation would set the European principle of sufficient clarity at risk—especially in the light of the possible criminal and administrative consequences for persons subject to the EU Blocking Regulation—because the Annex explicitly specifies U.S. sanctions laws in place at the time the EU Blocking Regulation was enacted. If the Annex was dynamic in its scope, persons subject to the EU Blocking Regulation would not be certain whether the regulation protects them if they do not comply with newer U.S. sanctions against Iran not expressly listed in the Annex.

Another argument in favor of this approach is certainly that the European Commission has felt compelled to change the Annex in 2019. If the Annex was dynamic, which already referred to the ILSA, such a change would hardly have been necessary. For quite some time, the EU Blocking Regulation did not receive a lot of attention, and its existence was barely taken notice of since its implementation in 1996. However, this has changed in the light of current events, especially in the context of the unilateral withdrawal by the United States from the Iran Nuclear Deal. The revision of the Regulation’s Annex, the Implementing Regulation, the Guidance Notes, and the *Telekom v. Bank Melli* case make it clear that a case-by-case assessment is always necessary to see whether and which anti-boycott risks

exist. In this regard, new jurisdiction by the ECJ is eagerly anticipated as multinational corporations are facing significant challenges of how to comply with colliding sanctions and blocking regulations.

---

1. Mexico's blocking statute is the *Law of Protection of Commerce and Investments from Foreign Policies that Contravene International Law* (often referred to as the "Antidote Law"). It is not examined in detail in the present Handbook but is briefly described in Chapter 1.

2. Foreign Extraterritorial Measures Act, R.S.C. 1985, c. F-29.

3. Council Regulation (EC) No. 2271/96 of Nov. 22, 1996, protecting against the effects of the extraterritorial application of legislation adopted by a third country, and actions based thereon and resulting therefrom, OJ L 309, 29.11.1996, p. 1, as amended by Commission Delegated Regulation (EU) 2018/1100 of June 6, 2018, OJ LI 199/1 7.8.2018.

4. Joint Action of Nov. 22, 1996, adopted by the Council on the basis of Articles J.3 and K.3 of the Treaty on European Union concerning measures protecting against the effects of the extraterritorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom (96/668/CFSP), OJ L 309, 29.11.1996, p. 7–7. Pursuant to Article 1, each member state shall take the measures it deems necessary to protect the interests of any person protected by the EU Blocking Regulation.

5. Cuban Assets Control Regulations, 31 C.F.R, Part 515.

6. John W. Boscariol, *An Anatomy of a Cuban Pyjama Crisis: Reconsidering Blocking Legislation in Response to Extraterritorial Trade Measures of the United States*, 30 LAW & POL'Y INT'L BUS. 439, 446 (1999) citing CACRs, § 305.

7. Iranian Transactions and Sanctions Regulations, 31 C.F.R, pt. 560

8. Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996, commonly referred to as the "Helms-Burton Act," 22 U.S.C. §§ 6021–6091 (Supp. III 1998).

9. U.S. Department of State, *Remarks to the Press by US Secretary of State Michael R. Pompeo* (Apr. 17, 2019), https://2017-2021.state.gov/remarks-to-the-press-11/index.html.

10. Dentons, *US Courts Open to Lawsuits for "Trafficking" in Confiscated Cuba Property*, Apr. 25, 2019, https://www.dentons.com/en/insights/alerts/2019/april/25/us-courts-open-to-lawsuits-for-trafficking-in-confiscated-cuba-property#_ftn3.

11. Helms-Burton Act, § 6091.

12. Notably, these sanctions have been used against a Canadian company and its directors and senior officers, Sherritt International, a mining company with operations in Cuba. The public securities filings of Sherritt International describe in detail the U.S. Cuba-related sanctions that apply to it. For further discussion on these extraterritorial measures, see Chapter 1.

13. Export Administration Regulations, 15 C.F.R. ch. VII, § 742.1.

14. Pub. L. 104-172 (1996), codified at 50 U.S.C.. § 1701 Note.

15. Pub. L. 111-195, 124 Stat. 1337 (2010), codified at 50 U.S.C. § 1701 Note.

16. Peter Glossop, *Recent US Trade Restrictions Affecting Cuba, Iran and Libya—A View from Outside the US*, 15 J. ENERGY & NAT. RES. 212, 227(1997).

17. FEMA, s. 3.

18. *Id.* ss. 2.1, 8.

19. *Id.* s. 7.1.

20. *Id.* s. 9(1)(a).

21. *Id.* s. 9(1.1).

22. *Id.* s. 9(2).

23. *Id.* s. 5(1)(a).

24. *Id.* s. 5(1)(b).

25. Order Requiring Persons in Canada to Give Notice of Communications Relating to, and Prohibiting Such Persons from Complying with, an Extraterritorial Measure of the United States that Adversely Affects Trade or Commerce between Canada and Cuba, SOR/96-84.

26. 1996 FEMA Order, s. 3(1).

27. *See* s. 2 of the *1996 FEMA Order* where "extraterritorial measure" is defined as including the CACRs and any law, statute, regulation, by-law, ordinance, order, judgment, ruling, resolution, denial of authorization, directive, guideline or other enactment, instrument, decision, or communication having a purpose similar to that of the CACRs, to the extent that they operate or are likely to operate so as to prevent, impede, or reduce trade or commerce between Canada and Cuba. "Trade or commerce between Canada and Cuba" includes the free exchange of goods and services between broadly defined private and public institutions in Canada and Cuba.

28. 1996 FEMA Order, s. 5.

29. *Id.* s. 6.

30. Deborah Senz & Hilary Charlesworth, *Building Blocks: Australia's Response to Foreign Extraterritorial Legislation*, 2 MELB. J. INT'L L. 69, 113 (2001). *Id.* citing Glossop, *supra* note 16, at 232, 237.

31. Boscariol, *supra* note 6, at 457.

32. Such investigations purportedly targeted large conglomerates such as Pepsi, American Express, Heinz, Eli Lilly, and Red Lobster. Boscariol, *supra* note 6, at 461, citing the *Special Session of the Commission on Foreign Affairs*, House of Commons (Sept. 26, 1996) (statement of Professor John Kirk). It is noteworthy that no official enforcement statistics exist with respect to investigations launched after 1996.

33. Global Affairs Canada, *Statement from Government of Canada for Canadians Doing Business in Cuba*, May 3, 2019, https://www.canada.ca/en/global-affairs/news/2019/05/statement-from-government-of-canada-for-canadians-doing-business-in-cuba.html.

34. Department of Justice, *Foreign Extraterritorial Measures Act (FEMA)*, Fact Sheet, https://www.justice.gc.ca/eng/rp-pr/csj-sjc/fema.html (last modified Aug. 16, 2022).

35. FEMA, s. 7(1)(a).

36. *Id.* s. 7(1)(b).

37. *Id.* s. 7(2).

38. *Id.* s. 7(4).

39. Andrew C. Dekany, *Canada's Foreign Extraterritorial Measures Act: Using Canadian Criminal Sanctions to Block U.S. Anti-Cuban Legislation*, 28 CAN. BUS. L.J. 210, 213 (1997).

40. *Id*. at 214.

41. For additional discussion, please see *id*. at 214–15.

42. Neil Campbell & Edward Akkawi, *Canada and U.S. "Cuba" Laws: The Risks of Getting Caught in the Crossfire* (Paper presented to the AIJA Winter Seminar or Extraterritorial Application of U.S. Laws, Vail, Colorado, Mar. 10, 1998) [unpublished] at 5.

43. Boscariol, *supra* note 6, at 463. For more discussion on this event, see David E. Sanger, *Wal-Mart Canada Is Putting Cuban Pajamas Back on Shelf*, N.Y. TIMES, Mar. 14, 1997, at D4.

44. *U.S. Fines Sanctions-busting Firms*, BBC News (Apr. 15, 2003), http://news.bbc.co.uk/2/hi/business/2948553.stm; Philippe Cicchini, U*.S.-Cuban Relations and the Helms-Burton Act*, 18(1) MICH. INT'L LAW. 14, 19 (2006).

45. Shoshana Perl, *Whither Helms-Burton: A Retrospective on the 10th Year Anniversary*, 6(5) Jean Monnet/Robert Schuman Paper Series, at 8 (Feb. 2006).

46. *Id*. at 11.

47. *Id*. at 8, lists three examples where the ban was threatened (STET, Grupo Domos) or applied (Sherritt).

48. *Spain's Melia Says CEO Banned from U.S. over Hotels in Cuba*, REUTERS (Feb. 5, 2020), https://www.reuters.com/article/us-melia-cuba-usa/spains-melia-says-ceo-banned-from-u-s-over-

hotels-in-cuba-idUSKBN1ZZ2G0.

49. EAR § 746.2(a).

50. Section 5400 of the Export Control List requires a permit for the export from Canada of "all goods that originate in the United States . . . other than goods that have been further processed or manufactured outside the United so as to result in a substantial change in value, form or use of the goods or in the production of new goods." While under general Export Permit No. 12, Canada generally permits the re-export of U.S.-origin goods; re-exports to certain countries such as Cuba, North Korea, Iran, and Syria require a permit.

51. In the past, it was generally understood that exporters could make this determination simply on the basis of whether the U.S. content exceeded 50 percent of the value of the item to be transferred. Recent experience shows that a simple value calculation is not sufficient and that U.S. value content is not the only factor to be considered. Exporters should also be carefully considering whether U.S. inputs have gone through a sufficient transformation in form or use when incorporated into the new item to be exported from Canada permit-free, even if the U.S. content is below 50 percent.

52. Boscariol, *supra* note 6, at 458.

53. Boscariol, *supra* note 6, at 459, citing an interview with an unnamed Department of Foreign Affairs and International Trade (DFAIT) official (June 30, 1998).

54. For a more detailed review of the application of U.S. re-export controls in Canada, see Chapters 1 and 8.

55. 50 U.S.C. apps. 144 (1994 & Supp. III 1998).

56. United States of America v. Stefan E. Brodie, Donald B. Brodie, James E. Sabzali, Bro-Tech Corporation d/b/a "The Purolite Company", 2001 U.S. Dist. Lexis 10533 (E.D. Pa. June 19, 2001) [*Brodie Main Decision*].

57. It is noteworthy that only 13 of these 21 convictions stemmed from activities that occurred while Sabzali was a resident of the United States. The other eight convictions pertained to Sabzali's dealings with Cuba while he was a Canadian resident. *See* John Boscariol, "Exposure of Canadians under the U.S. Trade Embargo of Cuba: The Case of James E. Sabzali (2002), 37 CAN. BUS. L.J. 419, 424 [Boscariol, 2002 Sabzali Article].

58. Sabzali was promoted to marketing director of Bro-Tech and in 1996 moved with his family to Philadelphia. Although he did not travel to Cuba after becoming a U.S. resident, Sabzali continued to be involved in Bro-Tech's sales to Cuba, which were made through the company's foreign subsidiaries.

59. *See* Timberlane Lumber Co. v. Bank of America, 549 F.2d 597 (9th Cir. 1977), Hartford Fire Ins., 509 U.S. 764 (1993).

60. United States v. Brodie, 268 F. Supp. 2d 420, 423–24 (E.D. Pa. 2003) [*Brodie 2002 Motion*].

61. Sabzali pleaded guilty to a superseding information charging a violation of 18 U.S.C. § 2 (aiding and abetting) and § 545 (smuggling goods into the U.S.), and was sentenced to one year probation and fined $10,000.

62. A final point of interest is that the goods being shipped by Sabzali to Cuba were of U.S. origin. As discussed earlier, under section 5400 of the Canadian Export Control List it is illegal to export U.S. origin goods from Canada without first applying for and obtaining an export permit. It is generally understood that such export permits are granted only if an applicant provides evidence to the Canadian authorities that permission has been obtained from U.S. authorities to export U.S. origin goods, although, as explained earlier, beginning on page 12, in practice we have seen otherwise. A breach of these rules could lead to fines of up to $25,000 and/or imprisonment for a term of up to ten years. In Sabzali's case, it is unclear whether an application for an export permit was ever made or whether a permit was ever issued by the Export Control Division of DFAIT; however, no charges have ever been brought by Canadian authorities against Sabzali for an alleged breach of these export regulations. For a more detailed discussion, *see* Boscariol, *supra* note 57, at 433–34.

63. *See* John W. Boscariol, *Managing Conflicting Obligations: Compliance with Canadian Law and Policy on Trade with U.S.-Sanctioned Countries* (Presentation presented to the American Conference Institute's 10th National Forum on Export Controls and Global Compliance Strategies, May 15-17, 2007) [unpublished] at 30–31 [Boscariol Presentation], and Campbell & Akkawi, *supra* note 42, at 6.

64. Boscariol, *supra* note 63.

65. *Id*. at 19–20.

66. *Id*.

67. *Id*.

68. For a detailed discussion of the extraterritoriality of the U.S. measures and the public international law aspects, see Werner Meng, *Wirtschaftssanktionen und staatliche Jurisdiktion—Grauzonen im Völkerrecht* (1997) Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 1997, 270–327.

69. See paras. 4 to 7 of the preamble of the EU Blocking Regulation.

70. Werner Meng, *supra* note 68, at 315.

71. Article 1 para. 1 EU Blocking Regulation; *see* August Reinisch, *Blockiermaßnahmen der EU gegen extraterritoriale Rechtsakte*, ecolex 900, 901–02 (1997).

72. Article 2 para. 1 sentence 2 EU Blocking Regulation.

73. Article 2 para. 3 EU Blocking Regulation.

74. Christoph Vedder & Stefan Lorenzmeier, *in* DAS RECHT der EUROPÄISCHEN UNION, 35th ed., Art. 133 EGV, para. 248 (Eberhard Grabitz/Meinhard Hilf eds., 2008).

75. JOACHIM KAYSER, GEGENMASSNAHMEN im AUSSENWIRTSCHAFTSRECHT und das SYSTEM des EUROPÄISCHEN KOLLISIONSRECHTS 124 (2000); Jürgen Huber, *The Helms Burton Blocking Statute of the European Union*, 20 FORDHAM INT'L L.J. 699, 704 (1996).

76. Article 5 para. 2 of the EU Blocking Regulation.

77. Regulation (EC) No. 2018/1101 of Aug. 3, 2018, laying down the criteria for the application of Article 5 para. 2 of Council Regulation (EC) No. 2271/96 protecting against the effects of the extraterritorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, OFFICIAL J. EUROPEAN UNION, L 199 I/8.

78. Guidance Note, *Questions and Answers: Adoption of Update of the Blocking Statute* (2018/C 277 I/03), OFFICIAL J. EUROPEAN UNION, C 277 I/4.

79. *See* RESTATEMENT (THIRD) of the FOREIGN RELATIONS LAW of the UNITED STATES (1987), § 441 (1): "In general, a state may not require a person (a) to do an act in another state that is prohibited by the law of that state or by the act in another state of which he is a national; or (b) to refrain from doing an act in another state that is required by the law of that state or by the law of the state of which he is a national."

80. Martin Gebauer, *Kollisionsrechtliche Auswirkungen der U.S.-amerikanischen Helms-Burton Gesetzgebung*, IPRAX, 145, 153 (1998); Werner Meng, *supra* note 68, at 315–16; Vedder & Lorenzmeier *supra* note 74, Art. 133 EGV, para. 248; Reinisch doubts whether the foreign state compulsion doctrine may indeed be invoked, *see* Reinisch, *supra* note 72, at 902–03.

81. Art. 6 para. 2 of the EU Blocking Regulation.

82. Werner Meng, *supra* note 68, at 315–16; Reinisch, *supra* note 71, at 903; Gebauer, *supra* note 80.

83. KAYSER, *supra* note 75, at 126.

84. Article 6, para. 3, EU Blocking Regulation. This additional basis for jurisdiction exceeds the jurisdiction allowed for by the Brussels Convention of September 27, 1968, on jurisdiction and the enforcement of judgements in civil and commercial matters; *see* Jacques H.J. Bourgois, *in* KOMMENtar zum EU-/EG-VERTRAG 6th ed., Art. 133 para. 146 (Hans von der Groeben/Jürgen Schwarze eds, 2003); KAYSER, *supra* note 75, at 127; Huber, *supra* note 75, at 706.

85. Bundesgesetzblatt zur Festlegung von Sanktionen bei Zuwiderhandlungen gegen die Verordnung (EG) Nr. 2271/96.

86. §§ 33, para. 4, sentence 1, German Foreign Trade and Payments Act (AWG), 70 para. 5 lit. f German Regulation Implementing the Foreign Trade and Payments Act Foreign (AWV).

87. *See EuGH will Firmen zwingen, sich im Iran-Konflikt den US-Sanktionen zu widersetzen*, HANDELSBLATT, Mar. 9, 2020.

88. *Plassnik: Strafverfahren gegen BAWAG eingeleitet*, KRONE, Apr. 27, 2007; HARRY L. CLARK & LISA W. WANG, FOREIGN SANCTIONS COUNTERMEASURES and OTHER RESPONSES to U.S. EXTRATERritorial SANCTIONS 23 (2007).

89. Roland Gribben, *Banks Action on Cuban Sanctions Hits UK Companies*, THE TELEGRAPH, Oct. 18, 2010; Roland Gribben, *UK Banks Warm to Cuba but Are Wary of U.S. Reproach*, THE TELEgraph, Nov. 8, 2010.

90. *See Ebay setzt Kuba-Embargo auch in Deutschland durch*, WELT ONLINE, July 28, 2011; *Vergleich im Kuba-Streit mit PayPal erzielt*, N-TV, Nov. 1, 2011.

10

Export Controls and Sanctions Compliance in the M&A Context (Including the CFIUS Notification and Review Process)

Meredith Rathbone, Peter Jeydel, and Evan Abrams

10.1 Introduction

Acquiring or merging with another company can present attractive business opportunities, but M&A activity also can present significant risks to the acquirer or surviving company. Among those risks are potentially severe penalties for noncompliance with export controls and economic sanctions laws and regulations. Assessing and addressing international regulatory compliance risks in an M&A context requires the upfront investment of time and resources, but typically pays dividends by allowing the acquiring/merging companies to take proactive steps to minimize the likelihood of an undesirable—and potentially costly—outcome. This chapter is intended to provide the reader with an overview of some of the proactive compliance steps companies can take when seeking to acquire (or be acquired by), merge with, or even make a significant investment in another company. Some of these same considerations may apply when companies acquire significant assets short of a full merger or entity acquisition.

When acquiring or merging with a company engaged in international business transactions, or with a company that utilizes or manufactures

sensitive goods, software, or technology, it is wise to conduct careful and targeted due diligence regarding international trade compliance. Discovering a potential problem and identifying compliance shortcomings before a deal closes gives a company the opportunity to decide whether and under what terms the deal should move forward. In addition, regardless of whether significant regulatory concerns arise during the due diligence process, there may be a requirement for companies engaged in certain types of manufacturing or exporting to provide notification to the U.S. government prior to (and/or after) closing a transaction, and to seek novation or transfer of relevant licenses and other authorizations. In some cases, it is legally required or prudent to seek prior approval from the U.S. government through the Committee on Foreign Investment in the United States (CFIUS) process, such as when a non-U.S. company intends to acquire a company with U.S. operations that is involved in the manufacture or export of sensitive goods, software, or technology; has a role with important infrastructure and/or government contracts;[1] or deals in sensitive personal information. Where notification to CFIUS is required, failure to notify CFIUS could result in substantial monetary penalties.

A company involved in M&A activity should take steps to ensure that its international regulatory compliance policy and procedures are applied throughout the corporate family, consistent with local laws and in light of particular risk areas in certain business units. Companies often experience growing pains (and sometimes resistance) throughout this process, which requires a clear tone from the top along with dedicated effort on the part of compliance personnel, managers, and others. Even with robust compliance efforts, the failure of a newly acquired company to adhere to corporate procedures or applicable U.S. laws can lead to enforcement actions and liability for the acquirer, the newly acquired entity, and/or responsible individuals at any level. Therefore, companies should consider sanctions and export controls risk carefully prior to closing, as certain risks that cannot be adequately mitigated may lead to a reconsideration of the transaction or its terms if fully understood.

In short, companies that take proactive steps to address export controls and sanctions compliance issues early on in a potential transaction typically fare better than those that ignore such issues, address them superficially, or treat them as problems to be solved after closing. Buyer’s remorse due to

unanticipated export controls and sanctions risk is becoming increasingly common—don't let it happen to you.

10.2 Enforcement

(a) Overview

The agencies responsible for export controls and sanctions enforcement have made clear that they are willing to hold an acquiring company liable for a target company's export controls and sanctions violations, even when those violations occurred prior to the transaction and wholly without the acquiring company's knowledge or involvement. In addition, these agencies have not hesitated to impose penalties for post-closing violations of U.S. law by a newly acquired subsidiary, even when the parent company makes fairly robust efforts to prevent such violations. Civil enforcement of export controls and sanctions violations is often based on the rule of "strict liability," meaning no negligence, knowledge, or intent is required to establish a violation. Criminal enforcement can also be a risk, but generally requires some level of willful misconduct. The Department of Commerce's Bureau of Industry and Security (BIS), the Department of State's Directorate of Defense Trade Controls (DDTC), and the Treasury Department's Office of Foreign Assets Control (OFAC) have all made these principles clear to varying extents through their enforcement practice in recent years. Accordingly, the importance of determining whether the target company/subsidiary is in compliance with export controls and sanctions laws both before and after closing cannot be overstated.

As discussed in more detail in the next section, the best strategy for the acquiring company is to engage in thorough due diligence early on, to require that the target company address any export controls and sanctions issues prior to closing, and to maintain robust oversight post-closing. Companies may be able to negotiate indemnity provisions, obligations for another party to (re)purchase the acquired interest if certain triggering events occur, or other protections that may reduce the financial and operational risks of the acquiring company due to unknown export controls or sanctions issues of the target company, or potential changes in law or other "unknowable" factors. However, such provisions would not shield the acquiring company from all risks (e.g., a requirement for the acquiring

company to retain a compliance monitor, subjecting the acquiring company to a policy of license denial, or denying the acquiring company export privileges altogether). Moreover, the enforcement process itself can be costly and disruptive, and it can be difficult to sell entities or assets after they become "tainted" with U.S. legal issues. While contractual protections can be critical, they are not a substitute for conducting adequate pre-closing due diligence and taking adequate steps post-closing to ensure a robust, risk-based compliance program.

(b) Department of Commerce

The case that serves as the foundation for the broad imposition of successor liability by BIS is *Sigma-Aldrich*.[2] In April 1997, three Sigma-Aldrich entities acquired certain assets of, and partnership shares in, Research Biochemicals Limited Partnership (RBLP).[3] Specifically, Sigma-Aldrich Research Biochemicals, Inc. acquired RBLP's assets, property, and liabilities, while two other Sigma-Aldrich entities acquired RBLP's partnership interests.[4] BIS alleged that RBLP had been making unauthorized exports of controlled biological toxins to Europe and Asia since 1995 (prior to the acquisition by Sigma-Aldrich), and that these unlicensed exports had continued for more than a year after the acquisition.[5] Sigma-Aldrich presumably failed to discover the prior unlicensed exports during its pre-acquisition due diligence review, and then failed to correct the export violations for a year after the acquisition was complete. Thus, BIS sought to impose liability against Sigma-Aldrich, both as a successor for violations occurring prior to the acquisition and as the actual wrongdoer by attribution for violations that occurred after the acquisition.[6] Although only one of the Sigma-Aldrich entities actually acquired RBLP's assets and liabilities, BIS maintained that all three Sigma-Aldrich entities were liable for the pre-acquisition violations, underscoring the potential breadth of successor liability in this area and the principle that contractual protections and other structures can often be pierced in the enforcement process.[7]

Sigma-Aldrich raised three primary defenses to the imposition of successor liability in its motion for summary judgment. First, the company argued that there was no statutory provision for successor liability underlying the Export Administration Regulations (EAR).[8] Second, Sigma-Aldrich maintained that liability could not be imposed because RBLP

remained a viable target for the enforcement action.[9] Third, Sigma-Aldrich argued that liability could not be imposed on the two entities that acquired only partnership shares in RBLP, without any assets or liabilities.[10]

> Among the factors to be considered under the "substantial continuity" approach are whether the successor (1) retains the same employees, supervisory personnel, and the same production facilities in the same location; (2) continues production of the same products; (3) retains the same business name; (4) maintains the same assets and general business operations; and (5) holds itself out to the public as a continuation of the previous corporation.

The administrative law judge (ALJ) hearing the case rejected all three of Sigma-Aldrich's arguments. First, the ALJ found that the underlying statute does permit the imposition of successor liability under the EAR even in an asset acquisition context.[11] The ALJ established a "substantial continuity" test for when such liability is conveyed.[12]

Second, the ALJ determined that successor liability could be imposed on the acquiring company even where the predecessor entity was not charged.[13] (However, the ALJ also found that, because RBLP had transferred all of its assets, contracts, and liabilities to Sigma-Aldrich, it was no longer a viable target for an enforcement action.[14])

Third, while the ALJ indicated that entities that acquire only partnership interests in a company may not generally be subject to successor liability, in this case, the ALJ was not convinced that all that was transferred to the two relevant Sigma-Aldrich entities was partnership units.[15] Accordingly, the ALJ denied Sigma-Aldrich's motion for summary judgment. Following the ALJ's decision, Sigma-Aldrich agreed to pay BIS $1.76 million to settle the case.[16]

(c) Department of State

DDTC, too, has not hesitated to impose liability on a successor company for alleged violations by the acquired company that took place prior to the acquisition. Shortly after the *Sigma-Aldrich* settlement, DDTC issued a

charging letter to the Boeing Company alleging violations of the International Traffic in Arms Regulations (ITAR) by Hughes Space and Communications (Hughes).[17] Boeing had purchased Hughes in 2000, and the charging letter alleged violations with respect Hughes' launch of satellites from the People's Republic of China in the mid-1990s.[18] In March 2003, Boeing and Hughes settled these charges for $32 million.[19]

In the General Motors (GM)/General Dynamics (GD) settlement the following year, the State Department indicated that a company may be able to lessen the penalties levied against it under the successor liability theory if it discovers export control violations during its due diligence investigation in connection with a proposed acquisition, and if those violations are voluntarily disclosed to the government in a timely and fulsome manner. While there was divided liability between GM and GD for export violations involving GM units that were purchased by GD after the violations occurred, GD was still required to pay $5 million of the $20 million fine.[20] As is common with ITAR settlements, GD was allowed to spend that $5 million over a five-year period on export compliance enhancements specifically directed at the acquired GM units rather than having to pay it as a civil penalty to the government.[21] This lesser penalty applied to GD may well have been the result of GD's discovery of GM's export control violations, and the actions it took in response to that discovery.

The State Department's settlement with AAR International likewise suggests that cooperation may have significant mitigating effects in successor liability cases. AAR International purchased Presidential Airways (Presidential), which was subsequently charged with 13 violations of the ITAR and the Arms Export Control Act.[22] In its Charging Letter, the State Department acknowledged that AAR International met with the Department prior to the purchase of Presidential to assist in resolving the export control violations.[23] The Consent Agreement resolving the dispute contained no monetary penalties.[24]

(d) Office of Foreign Assets Control

In recent years, OFAC has also used the doctrines of successor liability and post-acquisition strict liability to impose penalties on acquiring companies for export control violations committed by acquired companies prior to or

immediately after an acquisition. OFAC has also taken a more nuanced approach when acquiring/parent companies implement robust compliance measures by sometimes targeting the subsidiary and/or responsible individuals at the subsidiary, although the acquiring/parent company typically faces costs as well.

A good example of successor liability came in 2008, when Zimmer Dental Inc., successor to Centerpulse Dental Inc., paid $82,850 to settle allegations that Center-pulse had been exporting goods and services to Iran without an OFAC license. The alleged violations occurred prior to the acquisition of Centerpulse by Zimmer's parent company, and Zimmer voluntarily disclosed the apparent violations to OFAC.[25]

Similarly, in 2007, GE Security agreed to pay $1,900 to settle alleged violations of the Cuban Assets Control Regulations by a wholly owned foreign subsidiary of InVision Technologies, Inc. OFAC alleged that InVision's foreign subsidiary acted without an OFAC license by exporting goods and services to Cuba, and these alleged violations occurred prior to the acquisition of InVision by GE Security. InVision had voluntarily disclosed the matter to OFAC.[26]

Since October 2012, non-U.S. entities owned or controlled by U.S. persons have been directly subject to OFAC's Iran embargo, which has significantly increased the risk to U.S. companies with non-U.S. subsidiaries or acquisition targets that may do business with Iran.[27] Non-U.S. subsidiaries of U.S. companies have been directly subject to OFAC's enforcement jurisdiction under the Cuba embargo for decades. Two recent OFAC enforcement actions show that U.S. companies with subsidiaries doing business in Iran or Cuba still face significant legal risk even when they implement robust sanctions compliance measures that are ultimately not effective at preventing violations by their subsidiaries. Potential acquirers should be mindful of OFAC's "strict liability" approach to civil enforcement when considering the real-world risks of purchasing foreign businesses with exposure to sanctioned countries.

First, in February 2019, U.S.-based Kollmorgen Corporation paid OFAC a civil penalty of $13,381 to settle alleged violations of the Iran embargo by its Turkish subsidiary, Elsim, that took place immediately after Kollmorgen acquired it and continued for two years post-acquisition.[28] What is most noteworthy about this case is that OFAC fined the acquiring U.S. parent even after determining that it discovered these sanctions issues

during pre-acquisition due diligence, made “extensive efforts” to ensure the Turkish entity complied with U.S. law, and “implemented a wide range of pre- and post-acquisition compliance measures designed to ensure Elsim’s compliance with U.S. sanctions, which included but were not limited to the following:

> (i) conducting a comprehensive review of Elsim’s customer database in order to identify any sales or customers located in, or with connections to, countries or regions subject to U.S. economic and trade sanctions;
>
> (ii) identifying Elsim’s Iran-related customers and applying controls to block those customers from making future orders;
>
> (iii) drafting and circulating a memorandum to all Elsim employees notifying them of U.S. sanctions against Iran, the legal requirement for Elsim to comply with the Iranian Transactions and Sanctions Regulations (ITSR), and Elsim’s obligation to not sell products or services to Iran;
>
> (iv) conducting in-person trainings for Elsim’s employees regarding Kollmorgen’s trade compliance policies (specifically including Iran), which included a requirement that employees promptly report any and all violations of the law;
>
> (v) on a proactive and continuing basis, performing additional manual reviews of Elsim’s customer database to identify any sanctions-related customers;
>
> (vi) requiring Elsim customers to agree to modified terms and conditions of sale prohibiting the resale of any Elsim products, directly or indirectly, to Iran;
>
> (vii) requiring Elsim’s senior management to certify, on a quarterly basis, that no Elsim products or services were being sent or provided to Iran;
>
> (viii) ordering Elsim’s senior management to immediately cease transactions with Iran, including any technical support; and
>
> (ix) implementing an ethics hotline for reporting violations of law.”[29]

The Turkish subsidiary is alleged to have actively concealed its business with Iran from Kollmorgen, which ultimately was able to discover the issues and disclose them to OFAC:

> After the Apparent Violations were uncovered, Kollmorgen took a series of remedial actions designed to rectify the situation and discourage ongoing violative conduct, which included:
>
> > (i) terminating the Elsim managers responsible for, and involved in, the Apparent Violations;
> >
> > (ii) implementing new procedures to educate Elsim employees on compliance with U.S. economic and trade sanctions;

(iii) requiring Elsim to seek pre-approval from an officer based outside of Turkey for all foreign after-sales service trips; and

(iv) requiring Elsim to inform its major Turkish customers that Elsim cannot provide goods or services to Iran.[30]

OFAC appears to have gone out of its way to make these statements in the public settlement documents in order to (1) demonstrate the nature and extent of actions it expects acquirers to take in response to sanctions risks, and (2) make clear that even robust compliance is not a "safe haven," under OFAC's principle of strict liability. Of course, the low amount of the penalty reflects OFAC's view of Kollmorgen's compliance efforts.[31] It is also noteworthy that, in conjunction with the settlement with the U.S. parent company, OFAC added an individual affiliated with the Turkish subsidiary to the Foreign Sanctions Evaders (FSE) list, which is similar to the Specially Designated Nationals (SDN) list.[32]

In another February 2019 case, OFAC assessed a civil monetary penalty of $5,512,564 against Germany-based AppliChem GmbH for selling products to Cuba for nearly four years following its acquisition by U.S.-based Illinois Tool Works, Inc. (ITW).[33] ITW had discovered AppliChem's Cuba business during due diligence and warned AppliChem to cease it both before closing and again on two separate occasions after closing, one of which was in response to a discovery of continuing violations. ITW then submitted a voluntary disclosure to OFAC in which it represented that AppliChem had terminated its Cuba business, and received a warning letter in response. But ITW subsequently discovered continuing violations that AppliChem management had taken elaborate steps to try to conceal from ITW. In penalizing AppliChem rather than ITW, OFAC provided the following warnings/advice to U.S. parent acquirors and parent companies.[34]

> This case demonstrates the importance of (1) implementing risk-based controls, such as regular audits, to ensure subsidiaries are complying with their obligations under OFAC's sanctions regulations; (2) performing follow-up due diligence on acquisitions of foreign persons known to engage in historical transactions with sanctioned persons and jurisdictions; and (3) appropriately responding to derogatory

information regarding the sanctions compliance efforts of foreign persons subject to the jurisdiction of the United States.

Again, ITW's proactive measures including timely voluntary disclosures appear to have been what spared it any direct civil penalties in this case. Nonetheless, this process was surely costly and disruptive to ITW.

(e) Conclusions on Enforcement

The preceding cases suggest that the penalties imposed on the basis of successor liability or for violations immediately following closing of a transaction—in some cases, but not all—potentially could have been mitigated if the acquiring company had discovered and fully addressed the risks associated with export controls and sanctions violations in the context of its due diligence review. In most cases, a timely and complete voluntary disclosure of any violations to the government is the key differentiating factor for companies that obtain leniency in the enforcement process. The risk of imposition of a monetary penalty on a successor company may increase when an acquiring company fails to undertake a thorough international regulatory compliance review, and only discovers after the fact that the company it acquired was in violation of export controls or sanctions laws. This is particularly true when the violations continued to occur after the acquisition. Moreover, the agencies now expect active diligence post-acquisition in terms of auditing or checking transactions to ensure there is no ongoing prohibited business, as well as the provision of training and other compliance procedures and checks. The following section offers suggestions for conducting a thorough export controls and economic sanctions due diligence review.

10.3 Due Diligence

(a) Overview

M&A due diligence focused on the financial condition of the target company often fails to provide the attention and resources required to gain a full picture of the export controls and sanctions risks presented by the

target. As previously discussed, this cannot simply be a “check-the-box” exercise. Moreover, even robust compliance-focused due diligence and remedial measures may not eliminate the risks to the acquirer based on OFAC’s “strict liability” civil enforcement. At the end of the day, there is no substitute in higher-risk cases for conducting a thorough review of a target’s export controls and sanctions risks on a timeline that allows for the findings to be factored into the terms of the deal or allows the acquiring company an opportunity to reconsider the transaction altogether. Achieving this, of course, requires companies to begin to consider these risks—together with key stakeholders—at a relatively early stage in the transaction. The exact nature and extent of the compliance review that should be undertaken by an acquiring company will necessarily depend on the industry involved, the type of transaction, and the nature of the target company’s business. For example, companies in certain industries, such as technology, telecommunications, energy, defense, sophisticated software or electronics, and government contracts, are likely to be subject to more stringent regulatory regimes and/or enforcement focus. As discussed in more detail later, CFIUS notification may be required, for example, if a foreign company acquires a target that deals in “critical technologies.” If a target company is involved in one of these industries and does business overseas, or if it is a “critical technology” business and is subject to the mandatory CFIUS notification requirement, the necessary export compliance review will be more in-depth than if the target company operates in a less-regulated industry with little international activity.

The information collected during export compliance due diligence should allow the acquiring company to accurately assess the following: (1) the nature and footprint of the target company’s business, workforce, and third-party relationships; (2) the nature of the target company’s compliance program and the manner in which that program is implemented, along with some assessment of the target’s “culture of compliance” and the tone set by management; (3) the government agencies that have jurisdiction over the target company’s business (or that would have jurisdiction following the acquisition) and the target company’s licensing and enforcement history; (4) the existence of any past or present export controls or sanctions violations; (5) the policy or enforcement focus on the target company’s industry sector or geographical footprint; and, (6) the target company’s recordkeeping procedures and practices. Collecting this information in sufficient detail and

far enough in advance to allow for a real assessment of the findings and action in response will help to prevent delay caused by regulatory uncertainty or required government filings, and also to ensure that the transaction is properly valued, the terms are commensurate to the risks identified, and the future liability to the acquiring company is minimized.

(b) Conducting the Review

(i) Collecting Documents

Due diligence in the context of export controls and sanctions compliance is like due diligence in any other area of the target company's business in that the first step of the review is to begin collecting the relevant documents. The failure of an acquiring company to conduct sufficient export controls and sanctions due diligence frequently stems from not asking the right questions at the outset. As discussed previously, the exact nature of the export controls and sanctions review will necessarily depend on the industry involved and the specifics of the transaction. Generally speaking, documents should be collected that allow the acquiring company to answer the following types of questions:

- **Structure of the company's business.** Does the company's business involve products/technologies that are controlled under U.S. export laws? What percentage of the company's sales are to international markets? To which countries has the company exported over the past five years? How is the company structured? Does the company have international operations, and of what type and with which partners? How does the company sell? Through international distributors or with the assistance of agents? Does the company outsource aspects of its product development? Does the company employ foreign persons?
- **Compliance policy and procedures.**[35] Does the company have a written compliance policy that is sufficiently clear and appropriately tailored to the company's risk profile? Does the compliance policy establish a clear chain of command with respect to export controls and sanctions compliance decisions? Does the policy provide for adequate training for the employees involved in the company's export controls and sanctions operations? Does the policy establish an adequate procedure for screening potential overseas customers,

suppliers, distributors, and agents, and are third parties bound by the compliance policy through contract? Does the policy establish a procedure for screening employees? What does the policy provide with respect to document retention? To what extent has the company taken export controls risks into account in structuring its IT systems, including use of cloud service providers? Do the company's travel policies account for export controls and sanctions risks?

- **Export documentation.** What is the company's procedure for determining whether a particular transaction is subject to export controls or sanctions restrictions? How does the company determine the jurisdiction and classification of its products and technology? Does the company maintain a database with the classification of its products and technology? What export licenses does the company have from the relevant government agencies? If the company exports defense articles or defense services, is the company registered with DDTC under the ITAR? Which ITAR authorizations would need to be modified after the transaction, and what are the considerations for the required 60-day pre-acquisition notice to DDTC?
- **Past violations.** Has the company ever submitted a voluntary disclosure or been subject to an investigation (whether internal or government-led) regarding export controls or sanctions violations? If so, has the company ever been subject to any penalties or received any findings as a result of such an investigation? What was the cause of the violations? What changes were made within the company to ensure that similar violations did not occur?
- **Recordkeeping.** Has the company maintained copies of its export documents for at least five years (where "export documents" is defined broadly to include all relevant records including correspondence)?

These questions are examples: Appendix A to this chapter provides a sample preliminary export control compliance document request list.

As the acquiring company is conducting its initial document collection, a target company that does a substantial amount of business overseas, but lacks a comprehensive compliance policy or maintains inadequate records, is a clear red flag. Other red flags include when the target company does not know the export control classification of its products, does not screen customers or vendors against restricted party lists such as the Specially

Designated Nationals (SDN) list, or has sold to sanctioned or otherwise high-risk countries over the past five years. However, in many instances, potential export controls and sanctions compliance problems will be far less obvious, and it is only when the target company's documents are reviewed by persons with expertise in the area that deficiencies and risks become clear.

(ii) Going Beyond "Check-the-box" Diligence and Managing Regulatory Risk

Reviewing documents as part of the export controls and sanctions compliance due diligence effort may be complicated by the fact that the documents themselves may be regulated by export controls, data privacy, or other laws. Furthermore, there are sanctions prohibitions that may apply to conducting due diligence in sanctioned countries or involving sanctioned parties. In light of these and other complexities, this process should always be guided by experienced personnel.

One of the first steps that must be undertaken by the parties to the transaction is to ensure that adequate authorization exists for the acquiring company to review the documents that it has identified. Incorrectly limiting non-U.S. person participation in this process can itself constitute a violation of U.S. law, and even large international law firms do not always get this right.[36] Moreover, documents may be restricted for export under local/non-U.S. laws or may need to be reviewed locally for other reasons, such as data privacy or "national security" laws. These considerations may impact, for example, whether documents can be uploaded into a data room, the scope of appropriate permissions, where servers may be located, and so on.

Once a review plan has been crafted and vetted and any appropriate authorizations are in place, an export controls and sanctions compliance due diligence review must involve a substantive review and analysis of the documents and their implications by well-trained and experienced reviewers and compliance personnel, not just a confirmation that a certain set of documents has been provided in response to a request or the absence of any glaring red flags. Decision-makers need a full picture of the regulatory risks in order to take them into account as the deal progresses. For example, in order to determine whether the target company has adequate procedures for screening employees and overseas customers, suppliers, distributors, and agents, the acquiring company may need to

actually review the target company's screening process in order to ensure that it effectively flags any person or entity located in or linked to a restricted or sanctioned country or any person or entity on a U.S. restricted parties list such as OFAC's SDN list, including affiliated parties such as owners, officers, directors, or key employees. An acquiring company can only take limited comfort from knowing that there are screening procedures in place; ideally it would have the ability to examine (and test) the efficacy of those procedures. Indeed, one method sometimes employed in export compliance due diligence is to obtain a complete list of all customers of the target company for the preceding five years and screen those customers against all of the restricted party lists. Some acquirers take the additional step of independently looking into the ownership and control of some or all of those parties.

Again, screening is just one focus area, but this is meant to illustrate how to go beyond "check-the-box" due diligence. More examples are provided in the checklist found at the end of this chapter. In many instances, the responses to these questions lead to follow-up questions. For example, "deemed exports/re-exports" constitute a compliance area that is frequently overlooked, particularly by companies that only sell their products domestically. If a company employs non-U.S. persons (or dual/third-country nationals overseas), the acquiring company will want to ensure that those foreign persons are appropriately authorized to have access to source code, technology, defense articles, or anything else that would require an export license if it were being exported to that foreign national's home country, or that internal walls are sufficient to prevent such access.

Follow-up questions may also be appropriate even when the initial response would seem to suggest that there is no more information to be obtained. For example, the target company may say in response to an initial questionnaire that it has had no export controls or sanctions violations. If the target company does not employ many foreign persons and has limited export business, this may be reasonable. But if the target company produces controlled products or has a significant number of overseas customers, particularly in higher risk jurisdictions, this response should raise a red flag. While it is theoretically possible that a company operating in a controlled sector or with a large international footprint would have a perfect record of export controls and sanctions compliance, it may be more likely that the

response indicates that the target has simply not been sufficiently careful in assessing or documenting potential past violations.

Gathering and reviewing all of the relevant documents is not the end of the export controls and sanctions compliance due diligence process. It can be invaluable—particularly in higher-risk situations—for the reviewing team from the acquiring company to actually meet with some or all of the following personnel at the target company, depending on the particular risks associated with the transaction: compliance managers and personnel, sales and marketing representatives, the contracts management team, shipping department personnel, the information technology management team, and human resources personnel. Such interactions can help the acquiring company to feel comfortable that the compliance policies that exist on paper are both fully understood and actually implemented on the ground, and in some cases may alert the acquiring company to potential ongoing compliance problems that may not be evident on paper. This can also provide compliance personnel with a "head start" in integrating the acquirer's own compliance program with that of the target post-closing.

Finally, the acquiring company and its counsel should be mindful of sanctions risks in the due diligence process itself. For example, retaining due diligence services in sanctioned countries may be treated as a prohibited "importation of services."[37] While compliance-related advice and services in general are not prohibited,[38] this is a minefield that should be walked with care, guided by competent legal advice.

(iii) Addressing the Target Company's Failure to Turn Over Relevant Documents or Provide Adequate Responses to Questions, and Compliance Problems Identified during Due Diligence

Even if the acquiring company is diligent about requesting the relevant documents and asking the right questions for its export controls and sanctions compliance review, the acquiring company must ultimately rely on the target company to comply with its requests for production and information. To the extent that the target company is unwilling to produce the relevant documents or provide satisfactory responses to questions, or in acquisition contexts where complete due diligence is impossible for other reasons, the acquiring company will have to determine the degree of risk it is willing to take on in order to complete the transaction.

In the event that full due diligence or a satisfactory risk assessment is not possible, the acquiring company has a number of options. The acquiring company could insist on an adjustment to the purchase price or require the target to put funds in escrow in an attempt to account for unknown future liability, but arriving at an appropriate valuation of such potential future liability may prove difficult. The acquiring company could require that the target company provide warranty or indemnity language in the contract designed to make the acquiring company whole based on certain types of financial liability in the event that export compliance violations are discovered after the deal is finalized, but requiring such language will likely complicate negotiations. Moreover, it is simply not possible to "contract away" the full scope of legal risk in this area. If the nature of the target company's business makes it unlikely that significant export controls or sanctions violations have occurred in the past, the acquiring company may determine that it feels comfortable taking on the risk of proceeding with the transaction even with incomplete information. Alternatively, the acquiring company may decide to walk away from the deal altogether if the risks seem too high.

In some cases, a target may try to take the position that it cannot comply with certain requests or restrictions due to local "blocking" laws. Many jurisdictions around the world have had blocking laws in place for decades that restrict compliance by local companies with the "extraterritorial" aspects of the U.S. embargo of Cuba. In 2018, this issue gained even more attention with the EU's enactment of a broader blocking regulation relating to U.S. sanctions on Iran. These potential conflicts of laws situations may not always be fully resolvable, and may simply require risk-based decision-making. Companies should not assume that U.S. enforcement agencies will be swayed by conflicts of laws arguments or grant any leniency in these situations.[39]

In addition to determining how it will deal with incomplete information or unsatisfactory responses, the acquiring company will also need to be prepared to address export controls and sanctions violations that are actually uncovered during the course of its review. If the acquiring company discovers ongoing export controls or sanctions violations, the problematic activity should be stopped as quickly as possible (again, keeping in mind local laws such as blocking statutes), and an internal investigation should be undertaken in order to understand the nature and extent of the violation. A

decision must then be made regarding whether to disclose the violation to the relevant government agency and, if so, who makes the disclosure and at what time.

While, in most cases, disclosure of past violations of export controls and sanctions laws is not mandatory,[40] it will frequently be in the best interest of the acquiring company that any significant violations that are uncovered be disclosed. First, it may be that taking the necessary corrective measures is likely to alert the government to the violation anyway (e.g., obtaining new licenses, correcting false statements, etc.), thus essentially necessitating a disclosure, even if not technically mandatory. More importantly, as discussed earlier, a timely, thorough, and accurate voluntary disclosure will generally be considered a significant mitigating factor when an agency is determining whether to take enforcement action or of what type, whether to assess penalties, as well as the nature and magnitude of those penalties. However, the benefits of a voluntary disclosure are only available if the company comes forward in a timely manner and before the relevant government agency becomes aware of the problem through other means.

Furthermore, in the event that export controls or sanctions violations are discovered during the due diligence review, the acquiring company may decide that it wants to make closing the transaction contingent on the resolution of those violations or on obtaining related authorizations or responses to other agency requests such as advisory opinions. Disclosing a violation to the relevant government agency during the pre-closing period allows the parties to resolve the issue of liability, understand the exact nature of any penalties that may be assessed, and resolve any going-forward questions about the permissible scope of the target's business operations. Accordingly, the parties will have the necessary information to make decisions such as whether the purchase price or other terms need to be renegotiated, whether an escrow arrangement should be established to handle any penalties, and whether the transaction should proceed at all or should be scoped differently.

One question that we are frequently asked is, "who should make the voluntary disclosure?" In fact, it may be possible to require the target company to file an initial notice of voluntary disclosure prior to the close, noting in the initial notice that the violations were discovered during the due diligence process, and that the acquiring company will complete the investigation and submit the full voluntary disclosure report. This

underlines to the relevant agencies that these errors were made by the target company and not the acquiring company, and that the acquiring company is in “clean up” mode. It is also acceptable for the acquiring company to file the initial notice as soon as possible post-close. In any case, the acquiring company should ideally be responsible for the complete investigation and final voluntary disclosure to ensure that it has full access to all documents and personnel, and the decision-making powers necessary to investigate, disclose, and remediate the violations to its satisfaction. When possible, as discussed earlier, it may be preferable to make closing contingent on the full resolution of this process (though that is not always feasible due to the potentially lengthy and uncertain timelines for resolution) or to require that the target place funds in escrow to cover at least the financial aspect of the potential liability stemming from any violations.

(c) Conclusions on Due Diligence

Adequate export controls and sanctions compliance due diligence is a crucial part of many mergers or acquisitions given that the relevant government agencies have made clear that they will not hesitate to hold an acquiring company liable for past or ongoing violations committed by a target company without the acquiring company’s knowledge. In addition to ensuring that it is aware of a target company’s international regulatory compliance posture, an acquiring company must also work with the target company to ensure that the parties comply with any notification obligations that may arise from the merger or acquisition, as discussed in the following section.

10.4 Notification Requirements

(a) Department of State

Pursuant to section 122.4 of the International Traffic in Arms Regulations (ITAR), a registrant must, “within 5 days of the event” (i.e., closing in the case of an M&A transaction), notify the Office of Defense Trade Controls Compliance if there is a change in the following types of information contained in its Registration Statement:

> (i) Registrant's name; (ii) Registrant's address; (iii) Registrant's legal organization structure; (iv) Ownership or control; (v) The establishment, acquisition, or divestment of a U.S. or foreign subsidiary or other affiliate who is engaged in manufacturing defense articles, exporting defense articles or defense services; or (vi) Board of directors, senior officers, partners, or owners.[41]

In addition, "the new entity formed when a registrant merges with another company or acquires, or is acquired by, another company or a subsidiary or division of another company shall advise the Directorate of Defense Trade Controls of the following: (1) The new firm name and all previous firm names being disclosed; (2) The registration number that will survive and those that are to be discontinued (if any); (3) The license numbers of all [relevant] approvals" post-closing; and "(4) Amendments to agreements" as necessary, with a copy of such amendments to be provided to DDTC, signed by the relevant parties, within 60 days of the notification.[42] The parties should also provide the effective date of the closing of the transaction, and a point of contact at each of the U.S. subsidiaries. Pursuant to section 122.4(c), any licenses not identified in the notification and any amendments not properly executed within 60 days of the notification will be considered invalid.[43]

In light of this notification requirement, in preparation for a merger or acquisition, the parties should confer about any ITAR licenses or agreements that may need to be transferred to the buyer or otherwise amended after closing, recognizing that not all preexisting authorizations may be needed after the deal is finalized.

In addition to these general requirements, section 122.4(b) of the ITAR requires that the registrant notify DDTC at least 60 days in advance of any intended sale or transfer that will result in a foreign person acquiring ownership or control of a U.S. registrant "or any entity thereof."[44] Upon receipt of such a 60-day pre-closing notification, DDTC will assign a transaction number and will provide that number to the parties. These DDTC notifications are often, but not always, done in conjunction with CFIUS notifications, discussed in the next section.

Along with the five-day post-closing notification, a revised DS-2032 Statement of Registration should be simultaneously provided to DDTC for the surviving registration number.[45] The updated information—including changes to the name and location of the company, ITAR categories for defense articles/services produced or provided, changes in senior officers,

and so on—should be highlighted in the form.[46] Upon receipt of the five-day notification letter and the updated DS-2032 form, DDTC will notify the company of any deficiencies in the application or authorize it to proceed with amending the licenses and agreements listed in the five-day notification letter. If a transaction number was not previously provided (because a 60-day advance notification was not required), it will be included in this letter from DDTC. A general correspondence letter can now be used to accomplish the change, along with any agreement amendments that may be required.[47]

(b) Department of Commerce

The Bureau of Industry and Security also requires that a commerce licensee seek written approval from BIS in order to transfer any export licenses or other export authorizations to another party as the result of a merger or acquisition. Pursuant to section 750.10 of the EAR, such approval must be requested via a letter to BIS from the licensee, and that letter must describe the reason for the requested transfer, indicate which license numbers are to be transferred, list all pending license applications that are to be transferred, and state the entity to which they will be transferred. The letter should also describe why the transfer is necessary (including transaction details) and whether any consideration has been or will be paid for the transfer.[48] The transferee must submit a similar letter, accompanied by various certifications.[49] BIS will only authorize a transfer "to a transferee who is subject to the jurisdiction of the United States, is a principal party in interest, and will assume all powers and responsibilities under the license."[50] Unlike the ITAR, the EAR do not provide specific deadlines for the submission of such a letter to BIS. Also unlike the ITAR, the EAR do not require any notification if the preexisting licenses will continue to be held in the same form by the same legal entity, and, for example, if it is only the legal entity's parent company that has changed.

10.5 CFIUS Review

If the acquiring company is based outside the United States or is foreign owned or controlled, the transaction may be subject to review by the

Committee on Foreign Investment in the United States (CFIUS). CFIUS is chaired by the Department of Treasury, and includes as its members representatives from over a dozen other U.S. government departments, agencies, and offices. The Committee is responsible for reviewing certain forms of inbound foreign investment that might implicate U.S. national security. In most cases, parties are not required to make a filing with CFIUS, but may elect to do so if the parties believe the transaction is likely to raise national security concerns or questions for the Committee. Transactions voluntarily filed and approved by CFIUS receive a statutory safe harbor from future retroactive and unilateral review by the Committee. However, due to recent changes to the statutory regime underpinning CFIUS, certain transactions are now subject to mandatory filing requirements, described next in further detail.

(a) Jurisdiction

Historically, CFIUS review has been limited only to transactions that may result in control of a U.S. business by a foreign person. With respect to investments that may result in a foreign person obtaining control of a U.S. business, CFIUS may review the following categories of transactions:

(a) A transaction[51] which, irrespective of the actual arrangements for control provided for in the terms of the transaction, results or could result in control of a U.S. business by a foreign person.
(b) A transaction in which a foreign person conveys its control of a U.S. business to another foreign person.
(c) A transaction that results or could result in control by a foreign person of any part of an entity or of assets, if such part of an entity or assets constitutes a U.S. business.
(d) A joint venture in which the parties enter into a contractual or other similar arrangement, including an agreement on the establishment of a new entity, but only if one or more of the parties contributes a U.S. business and a foreign person could control that U.S. business by means of the joint venture.
(e) A change in the rights that a foreign person has with respect to a U.S. business in which the foreign person has an investment, if that change could result in foreign control of the U.S. business.

(f) A transaction the structure of which is designed to evade or circumvent the application of Section 721 of the Defense Production Act of 1950, as amended.[52]

More recently, the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) has expanded CFIUS's authority to review certain types of noncontrolling investments, called "covered investments," in U.S. businesses engaged in specified activities involving critical technology, critical infrastructure, or sensitive personal data. Such businesses are referred to as "TID" (technology, infrastructure, and data) U.S. businesses in CFIUS's regulations.

The term "covered investment," defined at section 800.211, includes noncontrolling investments that afford the foreign person:

(a) "Access to any material nonpublic technical information in the possession of the TID U.S. business,"[53]
(b) "Membership or observer rights on the board of directors or equivalent governing body of the TID U.S. business or the right to nominate an individual to a position on the board of directors or equivalent governing body of the TID U.S. business," or
(c) involvement, other than through voting of shares, in "substantive decision-making of the TID U.S. business" with regard to certain actions related to sensitive personal data, critical technologies, or critical infrastructure.

The term "critical technologies" is defined at 31 C.F.R. § 800.215 and includes items listed on the ITAR's U.S. Munitions List (USML); items listed on the EAR's Commerce Control List (CCL) pursuant to a multilateral control regime or for reasons relating to regional stability or surreptitious listening; certain nuclear-related items; Select Agents and Toxins controlled by the Department of Health and Human Services and the Department of Agriculture; and emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018. In addition, covered investments and transactions resulting in control of a U.S. business by a foreign person involving U.S. critical technology may trigger CFIUS's new mandatory filing requirements, discussed later.

With respect to critical infrastructure, Appendix A to Part 800 identifies 28 different categories of critical infrastructure covered by the rules, including, among others, telecommunications and satellite networks; U.S.

defense industrial resource providers; power utilities; specialty metals and materials manufacturers; oil and gas pipelines, refineries, and storage facilities; air and maritime ports; rail lines; and public water systems. Appendix A also identifies specific "functions" in each industry that would trigger CFIUS's jurisdiction. For example, category (vi) of Appendix A relates to "any satellite or satellite system providing services directly to the Department of Defense or any component thereof" and lists the applicable functions as owning or operating such satellite or satellite system.

CFIUS regulations defining sensitive personal data, at section 800.241, identify 11 categories of covered personal data (for example, financial data "that could be used to analyze or determine an individual's financial distress or hardship" or data "relating to the physical, mental, or psychological health condition of an individual," among other categories). The regulations give CFIUS the authority to review noncontrolling investments in a U.S. business that maintains or collects such data and that:

A. "Targets or tailors" products or services to U.S. federal government entities with "intelligence, national security, or homeland security responsibilities" or to their personnel or contractors;
B. Maintains or collects data on over one million individuals at any time during the preceding 12 months;[54] or
C. Has a business objective to collect such data on over one million individuals and such data is "an integrated part of" the company's "primary products or services."

U.S. businesses that maintain or collect genetic test results[55] are covered regardless of whether the preceding three criteria are met. The regulations exclude U.S. businesses that maintain or collect data regarding their own employees (with the exception of government contractors holding personnel security clearances) and data that is a matter of public record.

FIRRMA also extended CFIUS's jurisdiction over real estate transactions, which applies to "covered real estate transactions," defined as "the purchase or lease by, or a concession to," a foreign person of real estate within certain proximities of U.S. airports, maritime ports, and military facilities, that provides the foreign person with certain enumerated property rights.[56]

(b) Excepted Investors

The CFIUS regulations limit the agency's expanded jurisdiction over covered non-controlling investments by excluding from these requirements transactions by so-called excepted investors. In order to qualify as an excepted investor, a foreign person must meet one or more of the criteria laid out in section 800.219, which includes (1) individuals who are nationals only of one or more "excepted foreign states"; (2) foreign governments of an "excepted foreign state"; and (3) foreign entities meeting a variety of requirements with respect to place of incorporation, principal place of business, and nationality of directors and owners demonstrating the entities' closeness to an "excepted foreign state."[57] Currently, the regulations give excepted foreign state status to Canada, Australia, the United Kingdom, and New Zealand.

In addition, investments by investment funds with foreign person limited partners would not be considered "covered investments" if the fund meets the criteria of section 800.307, for example, that the fund is managed exclusively by a general partner (or equivalent) who is a U.S. person.

Investments from all foreign persons (including "excepted investors") remain subject to CFIUS's jurisdiction over transactions that could result in foreign control of a U.S. business.

(c) Voluntary and Mandatory Filings

The CFIUS process is voluntary in most cases, and unless there are national security issues potentially implicated by the transaction, a CFIUS filing is often unnecessary. However, CFIUS's jurisdiction—and its practice in construing the scope of reviewable national security issues—has expanded in recent years, so it is important that parties and their counsel consider the current state of CFIUS law and practice in deciding whether to file.

Even when not required, failing to file for CFIUS review in the event that there are potential national security issues is a risk that a company should be cautious in taking. While many CFIUS cases involve mergers and acquisitions within the defense and technology industries, CFIUS has reviewed transactions in many different industries, including many that people might view as normal commercial/civilian sectors, as the scope of technology or assets that are considered relevant to national security has expanded considerably. CFIUS can initiate a review of a transaction on its own initiative at any time, and can recommend that the President force the

parties to "unwind" a deal after the fact.[58] Thus, filing for CFIUS review prior to closing is the wiser course of action if the parties believe that there may be national security concerns with the merger or acquisition, as CFIUS clearance of a deal provides the parties with a safe harbor against subsequent unilateral action by the Committee.

While CFIUS remains a mostly voluntary process after FIRRMA, mandatory filings are now required in two scenarios. First, mandatory filings are required for transactions constituting a "covered investment" in, or that could result in foreign control of, a U.S. business that "produces, designs, tests, manufactures, fabricates, or develops one or more critical technologies" for which a "U.S. regulatory authorization" would be required for the export, re-export, transfer (in-country), or retransfer of such critical technology to certain foreign persons involved in the transaction. The term U.S. regulatory authorization is defined at section 800.254 and refers to licenses or other approvals issued by the Department of State pursuant to the ITAR or the Department of Commerce pursuant to the EAR, as well as those issued by the Department of Energy and Nuclear Regulatory Commission for nuclear-related activities. Notably, such analysis should be conducted without giving effect to any license exemptions under the ITAR or license exceptions under the EAR, with limited exceptions.[59] Second, mandatory filings are required for covered investments and transactions resulting in foreign control of a U.S. business where a foreign person obtains a "substantial interest" in a U.S. TID business and a foreign government holds a "substantial interest" in the foreign person. The term "substantial interest" is defined at section 800.244 to mean "a voting interest, direct or indirect, of 25 percent or more, and, in the context of a foreign person in which the national or subnational governments of a single foreign state have an interest . . . a voting interest, direct or indirect, of 49 percent or more."[60]

(d) Filing Process

Under the typical voluntary filing process, CFIUS encourages parties to engage in informal consultations with the Committee prior to filing a voluntary notice, in order to ensure that the process is efficient once it is actually underway. The official review process begins when the voluntary notice is filed with and accepted by the Department of the Treasury.[61] If the

filing is complete, it is then circulated to the other CFIUS members, and a lead agency is assigned to the case.[62] After an initial 45-day review period, all CFIUS agencies must approve the transaction, or else determine that a further 45-day investigation is warranted, except in certain cases in which a further 45-day investigation period is the default.[63] CFIUS can extend the investigation period by 15 days "in extraordinary circumstances."[64] If national security concerns remain at the end of that investigation period, CFIUS may elect to enter into an agreement with the parties in which it imposes conditions on the transaction in order to mitigate perceived risks.[65] Alternatively, CFIUS may send a report to the President, who then must decide whether to permit or block the transaction.[66] In some rare cases, the parties may withdraw and refile a notice in order to restart these clocks. This typically happens when CFIUS and the parties believe the transaction can be cleared but require additional time to negotiate the conditions necessary for clearance.

Under CFIUS's new regulations implementing FIRRMA, the Committee permits the use of a short-form declaration, instead of a full-length notice, for any transaction.[67] CFIUS must review such declarations within 30 days after acceptance, upon which the Committee may clear the transaction, require the parties to submit a full written notice, initiate a unilateral review of the transaction, or inform the parties it is "not able to complete action" on the basis of a declaration.[68]

CFIUS has traditionally not imposed fees for any filings. However, pursuant to authority given to CFIUS in FIRRMA, CFIUS now imposes filing fees on certain transactions. The fees, which apply to the submission of a written notice (but not a declaration) vary depending on the transaction value, with a maximum fee of $300,000 for transactions valued at $750 million or more.[69]

One cautionary note for parties that elect to undergo CFIUS review is that CFIUS filings are circulated to BIS, DDTC, and OFAC. In other words, if any information in the CFIUS filings describes activities that are regulated under the export controls or sanctions laws, these agencies will be put on notice of such activities. For example, if the CFIUS filing describes business activities that require a license from DDTC and DDTC knows that the company is not licensed for such activities—or, even worse, not registered under the ITAR—the information could trigger DDTC to initiate

a separate investigation or enforcement action. In fact, DDTC has been known to contact counsel when merely the nature of the products themselves suggests they might be subject to the ITAR. Therefore, parties that elect to undergo CFIUS review should seriously consider filing a voluntary disclosure with the relevant agency prior to, or concurrent with, their CFIUS filing if they are aware of any past unauthorized activity relating to export controls or sanctions.

10.6 Applying Export Controls and Economic Sanctions Policies to Newly Acquired Companies

As discussed earlier, the risk of international regulatory compliance violations does not come to an end after a deal has closed. The acquiring company remains responsible for any ongoing and future violations of export controls and economic sanctions laws committed by the acquired company. Therefore, the acquiring company should carefully consider how best to integrate the newly formed or acquired entity into its compliance framework. Steps that can be undertaken to accomplish this objective are outlined next.

(a) Identifying and/or Appointing Transition Point Persons

An effort to integrate a newly acquired company into an acquiring company's existing export and sanctions compliance framework, or to integrate the export and sanctions compliance policies and procedures of two companies that have merged, will not succeed unless appropriate personnel are identified to spearhead the transition, provide feedback, and implement the procedures that are chosen. Often, both the acquiring and the acquired company are large enough to have one or more personnel dedicated to supporting export controls and sanctions compliance full time. Any such people should be made part of the transition team, as they are likely to be highly familiar not only with the compliance policy and procedures but may also understand how they evolved and why they are written as they are.

Of course, in some cases, one of the companies involved in the M&A activity may not have dedicated compliance personnel in place. In such cases, it is critical to identify promptly one or more people who can

spearhead the integration process within that company. Every effort should be made to utilize existing employees, if at all possible, as this role requires knowledge of previously existing company personnel and procedures. However, if the person(s) selected is not highly knowledgeable about export controls and sanctions compliance, they will need either outside or in-house training early in the process, and also will need support from international regulatory compliance personnel with the compliance structure of the other party to the merger or acquisition.

Employees outside of export and sanctions compliance personnel also should be heavily involved in the transition. For example, it is very helpful —some would say essential—to have somebody in upper management on the business side of the company (rather than legal or compliance) involved. The right business person can help both to legitimize the process and drive employees to participate in providing feedback and implement the new procedures. Also, if the compliance function is not housed in the legal department, it can be helpful to involve an attorney with knowledge of export controls and sanctions compliance. Finally, it is critical to engage the employees who actually implement the policies and procedures on a daily basis. They are the ones who are the most likely to spot omissions or incongruities that can prevent newly implemented procedures from being fully effective, and their cooperation and dedication are needed to ensure that the new procedures are followed.

(b) Identifying Policies and Procedures That Will Be Applied to the Acquired Company

Once a transition team is in place (or at least after the primary stakeholders have been selected), the parties must identify which compliance policies and procedures will be applied to the acquired or newly merged company. While it is certainly possible for different members of a corporate family to maintain different compliance policies and procedures, especially during a transitional period, it is generally viewed as good corporate practice, if possible, to have one policy that applies to all parts of the corporation, even if it is tweaked or supplemented by some members of the corporate family to address their specific risk profile. By contrast, specific procedures may need to be tailored to the target’s risk profile, particularly when the target is

in a different line of business, has to apply for licenses where the acquirer does not, or has a different risk profile than its acquirer.

Whether to adopt one company's policy and procedures outright, or to pick and choose amongst the previously existing policies and procedures of two companies, very much depends on the companies, their similarities, their lines of business, how they will be functioning as part of the corporate family, and so on. Normally, large corporations that acquire a small company allow for a transition period to implement the corporation's policies within the newly acquired company, but the acquiring corporation's policies and procedures are eventually implemented in their entirety. However, in different situations, the decision is often made based on a variety of factors, including which company has a stronger compliance program, whose Enterprise Resource Planning software will be adopted, and so on. In short, there is no "right" answer, and each merger or acquisition will present unique facts and circumstances that should be evaluated in arriving at a determination.

Once policies and procedures are selected, many companies provide drafts for employee review and comment prior to finalizing. As noted earlier, employee review can help to identify any inadvertent shortcomings or oversights, help create business buy-in to the compliance plan, and ultimately will lead to a stronger compliance program.

(c) Providing Compliance Training

Providing thorough export controls and sanctions compliance training is critical to ensuring that the policies and procedures that have been selected are fully understood and implemented by the key stakeholders. Conducting a basic export and sanctions compliance training for all employees is generally a good place to start, though whether this is the best approach can depend on the size and nature of the company. There is almost always a need for additional training beyond a basic overview. Those responsible for implementing procedures on a daily basis should receive targeted training. For example, logistics personnel should be trained in the procedures for ensuring that an export has the appropriate authorization, completion of AES entries, recordkeeping, and so on. Human resources personnel should be trained in procedures relating to hiring and identification of foreign national employees. Business development personnel should be trained in

limitations on the release of controlled technical data to prospective customers, foreign national visitor policies, and so on. Depending on the topic, training can be either formal or hands on, or both. Training provided by U.S. government agencies (e.g., BIS seminars)[70] or outside vendors also can be informative.

Conducting such training has numerous benefits. It increases understanding of relevant policies and procedures and therefore reduces the risk of future violations. Training can lead to the uncovering—and stopping—of shortcomings in existing practices. Training can also create a link between export compliance personnel and employees, which often makes it more likely that the employees will reach out to the compliance personnel should they have questions or concerns, minimizing the likelihood of future violations.

The effectiveness of training can be assessed by including quizzes or tests to measure comprehension of the subject material. It is important to keep records of who has been trained, when, and on what subjects. Moreover, there should be a process for ensuring that all employees and management personnel designated for training are, in fact, trained.

(d) Performing Baseline and Periodic Compliance Audits

Acquiring companies should strongly consider conducting a baseline audit within a certain period of time (usually a few months, at most) after an acquisition closes. Even if the acquiring company conducted thorough export controls and sanctions due diligence on the target company, there is almost always much greater access to documents and personnel after a deal closes. Conducting an audit with full access to relevant information can yield additional insights beyond those gleaned in the due diligence process. The sooner a baseline audit can be undertaken, the better, as it is advantageous to identify and stop early on any problematic activity (or inaction) that could lead to a violation. If problematic activity or infractions are uncovered soon after the acquisition, the acquiring company can explain to the government that it affirmatively performed an audit intended to identify and discontinue problematic activity, which can be viewed as a mitigating factor (though, as discussed earlier, it will not necessarily preclude the imposition of penalties). Conversely, if problematic activity remains undiscovered for many months or even years, the likelihood that

the acquiring company would be granted mitigating credit for violations that took place after the acquisition is slim (though it may receive mitigating credit based on other factors).

10.7 Conclusion

Merger and acquisition activity presents unique export controls and sanctions compliance risks. Those risks can be mitigated with thorough due diligence, careful integration into the export controls and sanctions compliance framework, identification of appropriate personnel to assist with the transition process, and implementation of a tailored training and audit program. With proper planning and execution, export controls and sanctions compliance efforts need not be viewed as a cost or distraction. When properly performed, they help to ensure strong compliance going forward and can serve as a vehicle to ensure that the acquiring company adequately takes into account risk factors that could significantly affect the value of its investment.

---

1. Companies that deal with classified information (e.g., through facility security clearances) may also need to engage with the Department of Defense to address any concerns regarding foreign ownership, control, or influence (FOCI).

2. Order Denying Respondents' Motions for Summary Decision, *In the Matter of Sigma-Aldrich Business Holdings, Inc., et al.*, Case No. 01-BXA-06, 01-BXA-07, 01-BXA-11, Aug. 29, 2002.

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. *Id.*

8. *Id.*

9. *Id.*

10. *Id.*

11. *Id.*

12. *Id.* (citing Allied Corp. v. Acme Solvents Reclaiming, Inc., 812 F. Supp. 124 (N.D. Ill. 1993); Atlantic Richfield Co. v. Blosenski, 847 F. Supp. 1261 (E.D. Pa. 1994); Gould, Inc. v. A&M Battery & Tire Serv., 950 F. Supp. 653 (M.D. Pa. 1997)).

13. *Id.*

14. *Id.*

15. *Id.*

16. Two years later, BIS used the doctrine of successor liability to extract a $1.54 million civil settlement from Prochem Proprietary Ltd. (Prochem) for 220 violations of the EAR committed *not* by the company that Prochem actually acquired, but rather by a company, Protea, which had been sold to the company that Prochem acquired two years before Prochem's acquisition.

17. Investigation of Hughes Electronics Corporation and Boeing Satellite Systems (formerly Hughes Space and Communications) Concerning the Long March 2E and Long March 3B failure

investigations, and other satellite-related matters involving the People's Republic of China, December 26, 2002, https://www.pmddtc.state.gov/sys_attachment.do?view=true&sys_id=a99d3605db15df00d0a370131f96195f.

18. *Id*.

19. Consent Agreement: Hughes Electronics Corporation and Boeing Satellite Systems, Mar. 4, 2003, https://www.pmddtc.state.gov/sys_attachment.do?view=true&sys_id=c29d3605db15df00d0a370131f961905.

20. Consent Agreement: General Motors Corporation and General Dynamics Corporation, October 25, 2004, https://www.pmddtc.state.gov/sys_attachment.do?view=true&sys_id=4d8df205db15df00d0a370131f96196b.

21. *Id*.

22. Regarding Violations of the Arms Export Control Act and the International Traffic in Arms Regulations, July 14, 2010, https://www.pmddtc.state.gov/sys_attachment.do?view=true&sys_id=671dbec1db15df00d0a370131f9619c3.

23. *Id*.

24. Consent Agreement: AAR International, Inc., July 15, 2010, https://www.pmddtc.state.gov/sys_attachment.do?&view=true&sys_id=5b1df649db99db0044f9ff621f9619ac.

25. *See* Zimmer Dental, Inc., Jan. 4, 2008, https://home.treasury.gov/system/files/126/01112007.pdf.

26. *See* GE Security, Sept. 7, 2007, https://home.treasury.gov/system/files/126/09072007.pdf.

27. *See* 31 C.F.R. § 560.215.

28. *See* Kollmorgen Corporation, Feb. 7, 2019, https://home.treasury.gov/system/files/126/20190207_kollmorgen.pdf.

29. *Id*.

30. *Id*.

31. *Id*. ("If OFAC had determined this case was egregious, the base civil monetary penalty amount for the Apparent Violations would have been $750,000.").

32. *Id*. ("In conjunction with this enforcement action, OFAC is sanctioning Evren Kayakiran, the Elsim manager primarily responsible for the conduct that led to the Apparent Violations, pursuant to Executive Order 13608, "Prohibiting Certain Transactions With and Suspending Entry Into the United States of Foreign Sanctions Evaders With Respect to Iran and Syria" ("E.O. 13608"). E.O. 13608 authorizes the Secretary of the Treasury to sanction any foreign person determined to have "violated, attempted to violate, conspired to violate, or caused a violation" of the ITSR.").

33. *See* AppliChem GmbH, Feb. 14, 2019, https://home.treasury.gov/system/files/126/20190214_applichem.pdf.

34. *Id*.

35. *See generally* A Framework for OFAC Compliance Commitments, May 2, 2019, https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf; Export Compliance Guidelines: The Elements of an Effective Export Compliance Program, Jan. 2017, https://www.bis.doc.gov/index.php/documents/pdfs/1641-ecp/file; and Compliance Program Guidelines, Dec. 14, 2016, https://www.pmddtc.state.gov/sys_attachment.do?view=true&sys_id=35c9a068db995f00d0a370131f9619bb. As of this writing, DDTC reports that it is still working on a more robust set of compliance guidelines modeled after the foregoing OFAC and BIS documents.

36. *See* Press Release, Dep't of Justice, Justice Department Settles Immigration-Related Discrimination Claim Against International Law Firm (Aug. 29, 2018), https://www.justice.gov/opa/pr/justice-department-settles-immigration-related-discrimination-claim-against-international-law.

37. *See* IPSA International Services, Inc., August 10, 2017, https://home.treasury.gov/system/files/126/20170810_ipsa.pdf.

38. *See generally* Dep't of the Treasury, *Guidance on the Provision of Certain Services Relating to the Requirements of U.S. Sanctions Laws*, Jan. 12, 2017, https://home.treasury.gov/system/files/126/compliance_services_guidance.pdf.

39. *See* American Express Travel Related Services Company, Inc., July 22, 2013, https://home.treasury.gov/system/files/126/20130722_american_express_trs.pdf (OFAC imposed a civil penalty on a U.S. company for business with Cuba by its foreign subsidiaries, even though OFAC acknowledged that some of the third countries involved "had adopted 'antidote' measures (blocking statutes) prohibiting compliance with" OFAC's Cuba embargo. OFAC stated: "at the time of the apparent violations, [the U.S. company's] compliance program was inadequate, given the nature of [its] operations, to detect and prevent Cuba travel bookings, particularly from countries that had adopted antidote measures . . . OFAC also considered as a relevant factor the legal obligations placed on [the U.S. company] by U.S. law and antidote measures adopted by many of the jurisdictions in which [its] foreign branch offices and subsidiaries operate, but, given the facts and circumstances of this case, did not assign any mitigating or aggravating weight to this factor under the Guidelines.").

40. *C.f.* 22 C.F.R. § 126.1, requiring disclosures when arms-embargoed countries or nationals thereof are involved in the violation.

41. 22 C.F.R. § 122.4(a)(2).

42. *Id*. § 122.4(c).

43. *Id*.

44. *Id*. § 122.4(b).

45. *See* 5-Day Notice Guidance, https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=0bdbbfd8db069f00d0a370131f961931; *see generally* Material Changes Guidance, https://www.pmddtc.state.gov/?id=ddtc_kb_article_page&sys_id=f7cb9f4adbb95b00d0a370131f961992; Notification of Change for Mergers, Acquisitions, and Divestitures, https://www.pmddtc.state.gov/?id=ddtc_kb_article_page&sys_id=fc8aaa9adb74130044f9ff621f9619c3#tab-mad.

46. *Id.*

47. *See* Guidance for the submission of General Correspondence requests for the amendment of existing ITAR authorizations due to U.S. Entity Name/Address and/or Registration Code Changes, Jan. 14, 2015, https://www.pmddtc.state.gov/sys_attachment.do?view=true&sys_id=2d56c6b8db959f00d0a370131f961940.

48. 15 C.F.R. § 750.10(b).

49. *Id*.

50. *Id*. § 750.10(a).

51. A "transaction" is defined to mean: "whether proposed or completed: (a) A merger, acquisition, or takeover, including: (1) The acquisition of an ownership interest in an entity; (2) The acquisition of proxies from holders of a voting interest in an entity; (3) A merger or consolidation; (4) The formation of a joint venture; or (5) A long-term lease or concession arrangement under which a lessee (or equivalent) makes substantially all business decisions concerning the operation of a leased entity (or equivalent), as if it were the owner; (b) An investment; or (c) The conversion of a contingent equity interest." 31 C.F.R. § 800.249.

52. *Id*. § 800.213(d).

53. Material non-public technical information is defined to mean information that (1) "[p]rovides knowledge, know-how, or understanding not available in the public domain, of the design, location, or operation of critical infrastructure, including without limitation vulnerability information such as that related to physical security or cybersecurity," or (2) "[i]s not available in the public domain and

is necessary to design, fabricate, develop, test, produce, or manufacture a critical technology, including without limitation processes, techniques, or methods." 31 C.F.R. § 800.232.

54. The regulations clarify that category (B) applies "unless the U.S. business can demonstrate that at the time of the completion date of the transaction it had or will have neither the capability to maintain nor the capability to collect any identifiable data within one or more categories" of sensitive personal data on greater than one million individuals.

55. Genetic test is defined to mean "an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, that detects genotypes, mutations, or chromosomal changes." It does not include "(i) an analysis of proteins or metabolites that does not detect genotypes, mutations, or chromosomal changes; or (ii) an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition that could reasonably be detected by a health care professional with appropriate training and expertise in the field of medicine involved." 42 U.S.C. 300gg–91(d)(17).

56. *See* 31 C.F.R. part 802.

57. Foreign persons who have, in the prior five years, been determined to have violated certain U.S. sanctions, export controls, or investment laws, committed other felony crimes, or settled related allegations are not eligible for excepted investor status. *See* 31 C.F.R. § 800.219. Similarly, persons no longer meeting the excepted investor criteria within a three-year period following the completion date of the transaction are "not an excepted investor with respect to the transaction from the completion date onward." *Id.* Substantially similar provisions are also contained CFIUS's real estate regulations at section 802.216.

58. 50 U.S.C. § 4565(d)(1).

59. 31 C.F.R. § 800.401(c)(2).

60. In cases involving interest in a general partner, managing member, or equivalent person, "the national or subnational governments of a single foreign state will be considered to have a substantial interest in such entity only if they hold 49 percent or more of the interest" in that general partner, managing member, or equivalent. The regulations further provide that "for purposes of determining the percentage of voting interest held indirectly by one entity in another entity, any voting interest of a parent will be deemed to be a 100% voting interest in any entity of which it is a parent." *Id*. § 800.401.

61. *Id*. § 800.503(a).

62. *Id*. § 800.503.

63. *Id*. § 800.505.

64. *Id*. § 800.508.

65. 50 U.S.C. § 4565(k)(5)(A).

66. 31 C.F.R. § 800.506. Only the President has the authority to actually suspend or prohibit a transaction.

67. *Id*. § 800.402.

68. *Id*. § 801.407.

69. *See id*. § 800.1101–.1108; *id*. § 802.1101–.1108.

70. *See* BIS Seminar Schedule, https://www.bis.doc.gov/index.php/compliance-a-training/current-seminar-schedule.

Sample Preliminary Due Diligence Information Request List: Export Controls and Sanctions[1]

Please answer the following questions and provide documentation where requested for the target company and any entities owned or controlled by the target company:

I. Structure of the Company's Business

A. Does the company export any products, technology, or services? NO/YES
B. Does the company's business involve products/technologies that are controlled under U.S. export regulations? NO/YES
C. Does the company have any foreign subsidiaries, or any controlling interest in a foreign corporation, partnership, joint venture, or other business entity? NO/YES (List any applicable entities and the countries in which they are located)
D. Are there any foreign entities that form part of the company's supply chain? NO/YES (List any such entities and the supplies they provide, and the countries in which they are located)
E. Does the company conduct any research, development, production or other activities outside the U.S., including in partnership or other contractual relationship with third parties? NO/YES (Explain)
F. Does the company use any foreign agents/intermediaries or distributors/resellers? NO/YES (Explain)
G. Does the company employ any foreign persons within the U.S. (including contractors)? NO/YES (if yes, please answer the following questions)

1. Are there any Technology Control Plans (TCPs) in place for any such foreign person employees? NO/YES (Provide copy)
2. Does any such foreign person employed in the U.S. have access to any information subject to ITAR or EAR controls, including electronic (e.g., database) access? NO/YES (Explain)
    a. If yes, has the company assessed whether a license is required, and if so, has authorization been received from the relevant agency to permit such access? NO/YES (Provide copy)

H. Does the company have or use any servers or other electronic infrastructure in foreign countries (including through third parties such as cloud service providers)? NO/YES (List the countries and describe the use(s))

I. Please provide an organizational chart for the company, identifying personnel responsible for export compliance.

II. Compliance Policy

A. Does the company have a written export controls or sanctions compliance program, policy, or procedures? NO/YES (Provide copy)

B. Does the company have a training program for export controls or sanctions compliance? NO/YES (Provide copy of training manuals/procedures and any relevant certifications)

C. Does the company screen for denied or restricted parties? NO/YES (If yes, please answer the following questions)
    1. What are the triggers for when such screening is required?
    2. Which lists does the company screen against and how is that screening conducted (e.g., manual or automated)?
    3. Who is responsible for the due diligence and screening?
    4. How is the due diligence and screening documented?
    5. What is the procedure when there is a potential match to one of the relevant lists?

D. Does the company have an export controls or sanctions audit/assessment program? NO/YES (Provide copy of the written procedures and reports from the last five years)

III. Export Documentation

For the questions in A–E, please respond for the last five years, and please provide copies of any correspondence with the agencies listed here.

A. Department of Commerce
    1. Does the company have export licenses issued by BIS? NO/YES (Provide copies)
    2. Does the company export or re-export items listed on the Commerce Control List? NO/YES (If so, provide a list of all such CCL items and classifications, showing the parties involved in all such export transactions in the past five years, including the end-users, and their locations)

B. Department of State
    1. Does the company manufacture or export defense articles, or furnish defense services? NO/YES (If so, provide a list of all such defense articles and/or services, and all exports of such articles/services, showing the parties involved in such export transactions, including the end-users, and their locations)
    2. Does the company have any export licenses or other authorizations issued by DTCC? NO/YES (Provide copies)
    3. Is the company registered under 22 CFR Part 122 as a manufacturer or exporter? NO/YES (expiration date)
    4. Is the company registered as a broker under 22 CFR Part 129? NO/YES (expiration date)
    5. Who is the company's ITAR senior Empowered Official or senior person responsible for export compliance? (Provide contact information)
    6. Has the company made any ITAR-reportable political contributions, fees, or commissions within the last five years? NO/YES (List and explain)
    7. Is the company or any of its senior officials generally ineligible to participate in activity regulated under the ITAR as described in 22 CFR Section 120.1(c)(2)? NO/YES (Explain)

C. Department of the Treasury
    1. Does the company (or any entity controlled by the company) export to or engage in other business transactions, directly or indirectly, with Cuba, Iran, North Korea, Syria, Crimea, the so-called Donetsk or Luhansk "People's Republics," or any other

territory sanctioned by the U.S. government? NO/YES (List all such territories and explain business relationships)
    2. Does the company have any licenses issued by Treasury/OFAC? NO/YES (Provide copies)

D. Other U.S. Government Agency Jurisdiction
    1. Has the company received export licenses or authorizations from other U.S. Government agencies? NO/YES (List)

E. Foreign Government Agency Jurisdiction
    1. Does the company have export licenses or authorizations issued by foreign governments? NO/YES (Provide copies)

F. Does the company have a procedure for classifying products and technology under the USML and the CCL? NO/YES (Provide copy)

G. Who is responsible for classifying products and technology under the USML and the CCL? (Provide contact information)

H. Please provide sample documentation for five transactions with foreign entities during the past five years (for both commercial and defense end-users, if applicable), from the expression of interest through the fulfillment of the order.

IV. Export Controls and Sanctions Compliance and Violations

A. Is the company aware of any potential noncompliance by the company with export controls or sanctions laws or regulations within the past five years and that has not been disclosed to the regulating government agency? NO/YES (Explain)

B. Has the company filed any disclosures (voluntary or directed) of suspected noncompliance with export controls or sanctions laws or regulations?

C. Has the company been subject to any fines, penalties, suspensions of export privileges, or any other enforcement activity or corrective action by any government agency, U.S. or foreign, for suspected noncompliance with export controls or sanctions laws or regulations? NO/YES (List)

D. Has the company received any inquiries, including but not limited to subpoenas, from a government agency regarding export controls or sanctions compliance? NO/YES (Explain)

E. Does the company have a process for investigating and reporting instances of possible non-compliance with export controls and

sanctions laws or regulations? NO/YES (Explain)

F. What changes has the company made to ensure that any past violations of export controls or sanctions laws or regulations do not recur?

V. Recordkeeping

A. What are the company's policies and procedures for recordkeeping and reporting in accordance with export controls and sanctions laws and regulations? (Explain and provide copies of written procedures)

---

1. The type of information that should be sought during a merger & acquisition due diligence review will necessarily vary depending on the nature of the transaction. Therefore, this sample list, which assumes the target is a U.S. company, should be tailored to each particular situation.

11

Nuclear Export Controls

William E. Fork and Elina Teplinsky (United States) and Martha Harrison and Oksana Migitko (Canada)

11.1 Introduction

Although there are important peaceful uses for nuclear and nuclear-related goods and technologies, including for nuclear energy production, some technologies used in these activities are also capable of being diverted for the production of nuclear weapons. The potential for states to acquire the materials and technologies to develop nuclear weapons capabilities has generated strong support for national and international nuclear nonproliferation mechanisms. Many states have implemented comprehensive regulatory controls on the import and export of nuclear and nuclear-related goods and technologies to ensure these items are used only for nonexplosive and peaceful means. This chapter provides an overview of the international nuclear export control regime and the licensing requirements, policies, and international obligations that frame the export and import controls of nuclear and nuclear-related materials in the United States and Canada.

11.2 International Nuclear Export Control Regime

The Treaty on the Non-Proliferation of Nuclear Weapons (NPT)[1] provides the legal basis for the key aspects of the international nuclear export control regime. The NPT, which entered into force in 1970, granted nonnuclear weapon states (NNWS)[2] access to nuclear material, equipment, and technology for peaceful purposes so long as these states committed not to develop nuclear weapons.

Article IV of the NPT underscores the "inalienable right of all the Parties to the Treaty to develop research, production and use of nuclear energy for peaceful purposes without discrimination. . . ." This inalienable right, however, is subject to a state's conformity to other provisions of the NPT. Under Article III.1, NNWS undertake to conclude safeguards

agreements with the International Atomic Energy Agency (IAEA). Additionally, under Article III.2, all parties to the treaty pledge not to provide

> (a) source or special fissionable material, or (b) equipment or material especially designed or prepared for the processing, use or production of special fissionable material, to any non-nuclear-weapon State for peaceful purposes, unless the source or special fissionable material shall be subject to [IAEA safeguards established under Article III.1].

Recognizing that materials and technologies used in peaceful nuclear programs could be used to develop weapons, several NPT nuclear supplier states sought to determine what specific equipment and materials could be shared with NNWS under the NPT, and under what conditions. These nuclear supplier states formed the Zangger Committee in 1971 with a view of harmonizing the interpretation of nuclear export control policies under Article III.2 for NPT nuclear supplier states. In 1974, the Zangger Committee published a "trigger list" of nuclear-related goods (i.e., equipment that will trigger safeguards as a condition of supply) to assist NPT nuclear supplier states in identifying equipment and materials that should be subject to export controls.

India's explosion of a nuclear device in 1974 led nuclear supplier states to establish the Nuclear Suppliers Group (NSG) to further regulate nuclear-related exports beyond those provided for in the NPT. The NSG added technologies to the original Zangger Committee trigger list and agreed on a set of guidelines incorporating the trigger list. The NSG guidelines were first published in 1978 as IAEA Document INFCIRC/254. In 1992, in response to concerns that export control provisions then in force had not effectively prevented Iraq, a party to the NPT, from pursuing a clandestine nuclear weapons program through acquiring dual-use items not covered by the NSG guidelines, the NSG established a second set of guidelines for transfers of nuclear-related dual-use material, equipment, and technology. The dual-use guidelines were published as Part 2 of INFCIRC/254 and the original guidelines published in 1978 became Part 1 of INFCIRC/254 (collectively, NSG Guidelines).

The NSG is a voluntary regime and the NSG Guidelines are implemented by each NSG member in accordance with its national laws and practices. Decisions on export applications are taken at the national level in accordance with national export licensing requirements. Some states, such as the United States, have export control regimes that predate

the establishment of the NSG Guidelines. Other states have adopted regimes that mirror the NSG Guidelines in many ways. States can also choose to adhere to the Guidelines even if they are not members of the NSG.

NSG members review the Guidelines periodically to ensure that they are up to date and continue to meet evolving nuclear proliferation challenges. Because the NSG Guidelines are incorporated into the export control regimes of most NSG member states, familiarity with the NSG Guidelines is important in understanding export controls on nuclear and nuclear-related items.

11.3 United States: Export Controls

(a) Overview

The United States, one of the first countries to develop the use of nuclear energy for peaceful purposes, first catalyzed international civil nuclear cooperation through its "Atoms for Peace" program. The United States was also one of the first countries to control nuclear trade and nuclear-related assistance. U.S. controls over the exports and re-exports of nuclear materials, equipment, and technologies predate the establishment of an international nuclear export control regime. Today, the United States has a complex and comprehensive system of controls over nuclear civilian, dual-use, and military items and related technologies and software.

- **What is regulated?** The primary laws governing exports of nuclear material and equipment are promulgated under the U.S. Atomic Energy Act of 1954 (AEA),[3] as amended by the Nuclear Non-Proliferation Act of 1978[4] and interpreted by several sets of regulations issued by U.S. federal agencies.
- **Where to find the regulations.** The U.S. Nuclear Regulatory Commission (NRC) controls the exports of certain nuclear material and equipment under the AEA, as specified in the NRC's regulations at 10 C.F.R. part 110. The U.S. Department of Energy (DOE) controls the export of certain nuclear technologies and specific nuclear reactor and nuclear weapons technologies under the AEA and various

nonproliferation mandates. The DOE regulations are set out at 10 C.F.R. part 810.

- **Who is the Regulator?** The export and re-export of nuclear and nuclear-related commodities and technologies are regulated by the NRC, the DOE, the U.S. Department of Commerce (DOC), and the U.S. Department of State (DOS).

(b) Federal Statutes and Authorities

The import and export of nuclear and nuclear-related items, technology, and software in the United States is primarily controlled in accordance with the requirements of the AEA, as amended. Four U.S. agencies have jurisdiction over nuclear and nuclear-related exports. The two key nuclear export control agencies are the NRC and the DOE. Each agency's jurisdiction is designed to be exclusive of the other and is divided as follows:

- The NRC controls the exports of certain nuclear material and equipment (e.g., equipment within or attached directly to a reactor vessel) under the AEA, as specified in the NRC's regulations at 10 C.F.R. part 110.
- The DOE controls the export of certain nuclear technologies and specific nuclear reactor and nuclear weapons technologies (e.g., nuclear-related information, technology and software) under the AEA and various nonproliferation mandates. The DOE regulations are set out at 10 C.F.R. part 810.

Further, the DOC and the DOS have jurisdiction over the exports and re-exports of certain nuclear-related items, technologies, and software:

- The DOC, through its Bureau of Industry and Security (BIS), is responsible for implementing and enforcing the Export Administration Regulations (EAR).[5] The EAR regulates the export and re-export of commercial items that it views as having "dual-use," that is, both commercial and military or proliferation applications. Furthermore, the EAR regulates exports of systems and equipment that support the nuclear reactor and steam-generating systems, called the balance of plant (BOP), and their related technology.
- The DOS controls the export of defense articles and services under the International Traffic in Arms Regulations (ITAR).[6] These are

items and services that, at the time of export, are considered inherently intended for military use. ITAR-controlled defense articles, services, and technology are listed in the U.S. Munitions List.

(c) NRC Export Controls

The NRC controls the export and re-export of nuclear reactors and nuclear reactor equipment and components, and sources special nuclear and by-product materials in accordance with the requirements of the AEA. The NRC may only issue an export license if the recipient country provides assurances that meet the export criteria set forth in AEA sections 127 and 128 and if the NRC determines that the export will not be inimical to national security. These assurances include a pledge of peaceful use of supplied items, IAEA safeguards over supplied items, maintenance of adequate physical protection measures, and agreement to seek consent of the United States prior to retransfer of supplied items. Some of the AEA export criteria can only be satisfied through pledges made in bilateral peaceful nuclear cooperation agreements entered into pursuant to section 123 of the AEA (123 Agreement). For this reason, the NRC can only authorize certain exports of nuclear equipment and materials if a 123 Agreement is in force between the United States and the recipient country.

With respect to nuclear reactors, the NRC exercises export control authority over any equipment especially designed or made for use in a nuclear reactor. For illustrative purposes, the NRC states that a nuclear reactor includes the items within or attached directly to the reactor vessel, the equipment that controls the level of power in the core, and the components that normally contain or come in direct contact with or control the primary coolant of the reactor core.[7] Examples include reactor pressure vessels, complete reactor control rod systems, reactor primary coolant pumps, and reactor control rod drive mechanisms. This illustrative list is similar to the portion of the NSG Guidelines' "trigger list" that concerns nuclear power reactors, equipment, and components.[8] The NRC also exercises export control authority over radioactive materials, which include source, special, and by-product materials. Appendix P to 10 C.F.R. part 110 incorporates internationally harmonized guidance for the import and export of radioactive sources as set out in the IAEA Code of Conduct on the Safety

and Security of Radioactive Sources (IAEA Code)[9] and the IAEA Guidance on the Import and Export of Radioactive Sources.[10]

Certain exports—depending on the commodity exported and its destination—may be exported under an NRC general license (i.e., no license application required). In particular, certain minor nuclear reactor components can be exported to destinations listed at 10 C.F.R. § 110.26(b). Such countries include, for example, Canada, France, Japan, the Republic of Korea, Taiwan, and the United Kingdom. General licenses are also available for exports of small quantities of special, source, and certain types of by-product material and deuterium (all subject to concentration limitations and other parameters)[11] as well as imports of by-product, source, or special nuclear material if the U.S. consignee is authorized to receive and possess the material.[12] Other items require the exporter to obtain an NRC-specific export license. This is conducted by submitting NRC Form 7, Application for NRC Export or Import License, Amendment, Renewal or Consent Request(s), and a fee in accordance with 10 C.F.R. §§ 110.31 and 110.32, and meet the applicable criteria provided in 10 C.F.R. § 110.42.

(d) DOE's Part 810 Regulations

The U.S. DOE regulations concerning "assistance to foreign atomic energy activities," codified at 10 C.F.R. part 810, implement the broadly stated requirements of section 57b of the AEA. Section 57b forbids "any person to directly or indirectly engage in the production of any special nuclear material outside the United States," except when provided for in an agreement for cooperation or when authorized by DOE.[13] The DOE's regulations at part 810 provide DOE's interpretation of this prohibition, indicate activities that require authorization by the Secretary of Energy, and set out reporting requirements for controlled activities. Part 810 regulations apply to activities conducted by U.S. companies and persons within the United States and abroad and extend to the activities of subsidiaries or contractors under their direction, supervision, responsibility, or control.[14]

In February 2015, the DOE issued a final rule revising part 810, the first comprehensive update of the regulation since 1986. The revised regulation replaced the previous list of restricted destinations with an affirmative "generally authorized destinations" list. The revisions also provided more detail regarding the activities and technologies that are within the scope of

part 810 and established new and expanded general authorizations. The revised rule took effect as of March 25, 2015.[15]

Part 810 applies to transfers of technical data or provision of assistance involving the activities set out in 10 C.F.R. § 810.2(b). These activities can essentially be divided into two main categories: nuclear fuel cycle activities and commercial nuclear power activities. Nuclear fuel cycle activities include conversion, enrichment, fuel fabrication, reprocessing, and the production of heavy water, but do not include mining or milling. Commercial nuclear power activities include "development," "production," or "use" (as those terms are defined in § 810.3) of nuclear reactors and key nuclear systems and components (i.e., the Nuclear Steam Supply System). The revised regulation also links the part 810 technology controls to the NRC's reactor, equipment, and materials controls by establishing at 10 C.F.R. § 810.2(b)(9) a catchall for the transfer of technology for the development, production, or use of equipment or material listed at Appendices A–K to part 110.

Part 810 regulations do not apply to exports controlled by any other agency, including the NRC, BIS, or State. Part 810 regulations also do not apply to publicly available information, publicly available technology, or the results of fundamental research (as those terms are defined in 10 C.F.R. § 810.3).

Part 810 provides for two types of authorizations: general and specific. A general authorization allows for a company to engage in certain activities without the need to secure prior authorization from the DOE. Generally authorized activities are listed in 10 C.F.R. § 810.6 and include at 10 C.F.R. § 810.6(a) an authorization to engage in activities involving commercial nuclear reactors with countries listed in Appendix A to part 810. The Appendix A list consists of countries with which the United States has 123 Agreements, with the exceptions of China and Russia. Activities controlled under part 810 but excluded from the scope of the general authorization specified in § 810.6 require specific authorization (essentially a license) from the Secretary of Energy. This includes engaging in any activity subject to part 810 with countries not listed in Appendix A to part 810 and certain nuclear fuel cycle activities (e.g., enrichment and reprocessing), which are never subject to general authorization regardless of the destination.

Exporters seeking a specific authorization from the DOE must submit a request in accordance with the parameters set out in 10 C.F.R. § 810.11.

DOE does not provide a form for part 810 applications; therefore, all applications are submitted in free form. Secretary of Energy personally signs each specific authorization issued to an exporter; although recent amendments to the AEA have enabled the Secretary to delegate his authority, the DOE has yet to adopt delegation procedures. The Secretary will approve an application for specific authorization based on a determination, with concurrence of the DOS and after consultation with the NRC, the DOC, and the U.S. Department of Defense, that the activity will not be inimical to the interest of the United States. In making this determination, the Secretary considers several factors, including whether the United States has an agreement for nuclear cooperation with the recipient country, whether the recipient country is a party to the NPT, whether the recipient country has entered into an agreement with the IAEA for the application of safeguards on all its peaceful nuclear activities, and other nonproliferation conditions.

(e) Retransfer Controls in 123 Agreements

The United States has entered into agreements on civilian nuclear cooperation, commonly known as 123 Agreements, with more than 25 states and groups of states, including Japan, Republic of Korea, China, India, Russia, and the member states of the European Atomic Energy Community. These 123 Agreements are a legal perquisite to the NRC's ability to issue licenses for the exports of major nuclear reactor components and nuclear material. 123 Agreements provide for two types of U.S. consent rights over U.S.-supplied nuclear commodities transferred under these Agreements: (1) retransfer consent rights—a requirement that the recipient state obtain prior approval from the United States before retransferring items supplied under the agreement to a third country; and (2) reprocessing consent rights—a requirement that nuclear material transferred pursuant to these Agreements and special nuclear material produced through the use of transferred nuclear material and certain equipment (e.g., plutonium that is produced through the irradiation of fuel in reactors) may only be reprocessed upon agreement of the parties.

123 Agreements can also include additional conditions. An example is the landmark U.S.–India 123 Agreement, which lifted a three-decade-long U.S. moratorium on nuclear-related trade with India that was imposed when

India conducted a nuclear test in 1974. The 2006 Hyde Act,[16] which allowed for the implementation of the 123 Agreement under U.S. law, placed additional conditions on nuclear exports to India. These conditions include additional approval requirements, limitations on the scope of licenses, intellectual property protection requirements, and enhanced reporting. For example, the act requires that India provide assurances that U.S. technology transferred to India will not be retransferred without prior U.S. consent, even in the case of domestic transactions within India. In other agreements, such as those with the UAE and Taiwan, countries have agreed to forgo enrichment and reprocessing in the future.

(f) Penalties and Enforcement

Violations of U.S. nuclear export control laws and regulations are subject to civil and criminal penalties. Permanent and temporary injunctions and restraining orders to prevent violations of part 110 and part 810 are possible. Although the DOE's jurisdiction to impose criminal penalties was long-standing (fines and prison sentences of up to ten years apply, and offenses committed with intent to injure the United States or to aid any foreign nations can bear a life sentence[17]), the agency's civil penalty authority was unclear until a recent mandate from Congress confirmed it and mandated for the DOE to conduct a civil penalties rulemaking. The DOE issued a draft rule on October 3, 2019, proposing procedures for imposing civil penalties for violations of part 810. The proposed rule sets a maximum penalty per violation per day at $102,522. A final rule has not yet been implemented. Violations of part 110 are subject to civil fines of up to $140,000 per violation[18] and criminal penalties in the form of a fine of up to $5,000 or imprisonment up to two years, or both; offenses committed with intent to injure the United States or with intent to secure an advantage to any foreign nation can be punished by a fine of up to $20,000 or by imprisonment up to 20 years, or both.[19]

The NRC will normally take enforcement action for violations of requirements related to import and export of NRC regulated radioactive material. Specifically, the import and export of the radioactive material (1) within the scope of an NRC license and (2) with implementation of any security programs that may be required are two examples of matters of importance where violations of corresponding requirements warrant

consideration of escalated enforcement action.[20] For example, on September 17, 2020, the NRC issued a Notice of Violation to International Isotopes, Inc. (INIS) for a Severity Level III violation. The violation involved multiple exports of by-product material by INIS to an embargoed destination without a specific license. Specifically, on three occasions, INIS exported by-product material in four separate shipments to Iraq, an embargoed destination, without the required NRC-specific license. However, because INIS had not been the subject of escalated enforcement actions within the two years prior to the violation, and because the company submitted comprehensive corrective actions to the NRC, the NRC did not apply a civil penalty.

11.4 Canada: Nuclear Export Control Policy

(a) Overview

Although Canada renounced interest in nuclear weapons development shortly after World War II, Canada remains an active participant in the nuclear economy, and is a major exporter of uranium and radioisotopes for medical and industrial purposes.[21] Through Atomic Energy of Canada Ltd., a Canadian Crown Corporation, Canada has also been involved in the construction of CANDU nuclear power plants in several countries,[22] including Argentina, China, India, Pakistan, Romania, and South Korea.

While Canada has strong business interests in the commercial market for nuclear technologies and goods, it also imposes strict regulatory controls on the export of these items to ensure compliance with its nuclear nonproliferation policies and international commitments. Canada is a signatory to the NPT.[23] Before it will consider nuclear cooperation with a non-nuclear-weapon state, Canada requires the state to become a party to the NPT or commit to an equivalent international legally binding agreement and accept the application of IAEA safeguards.[24] Canada is also a founding member of the Zangger Committee of the IAEA and the NSG.[25]

In 2010, Canada ended a decades-long restriction on trade in nuclear-related goods with India when the two countries signed a nuclear cooperation agreement.[26] Like the United States, Canada had prohibited nuclear trade with India as a result of India’s diversion of plutonium for use

in a nuclear explosive device in 1974. The plutonium was produced in a reactor that had been provided by Canada for peaceful nuclear purposes.[27] The NSG ban on nuclear trade with India that was imposed as a result of this activity was lifted in 2008.[28] The Canada-India Nuclear Cooperation Agreement allows Canadian firms to export and import controlled nuclear materials, equipment, and technology to and from India to facilities subject to IAEA safeguards. It also provides assurances that nuclear material, equipment, and technology originating in Canada will be used only for civilian, peaceful, and nonexplosive purposes.[29]

- **What is regulated?** The import and export of nuclear and nuclear-related goods and technologies is primarily regulated under the Nuclear Safety and Control Act[30] (NSCA) and the Nuclear Non-proliferation Import and Export Control Regulations[31] (NNIECR).
- **Where to find the regulations?** The statutory authority of the NNIECR is the NSCA. The NNIECR sets out the import and export licensing application requirements for a prescribed list of controlled nuclear and nuclear-related substances, equipment, and technologies detailed in its Schedule. The Export and Import Permits Act[32] (EIPA) sets out import and export permit requirements.
- **Who is the regulator?** The Canadian Nuclear Safety Commission (CNSC) is the federal authority that implements regulatory controls for the production, use, storage, and movement of nuclear material in Canada. Export Controls Operations Division of Global Affairs Canada (GAC) oversees permit requirements under the EIPA.

(b) Statutes and Federal Authorities

The import and export of nuclear and nuclear-related goods and technologies in Canada is primarily controlled through the NSCA, which came into force on May 31, 2000, and the NNIECR.

The CNSC, established under the NSCA, is the federal authority that implements regulatory controls for the development, production, use, storage, and movement of nuclear material in Canada.[33] The import and export of nuclear substances, prescribed equipment, information, and technology is subject to regulatory control through the CNSC licensing

regime, as well as through permit requirements under the EIPA administered by GAC.

The CNSC licensing and compliance process is structured to ensure that nuclear imports and exports meet Canada's regulatory requirements, nuclear nonproliferation policy, and international obligations and commitments.[34] The principle underlying these measures is that controlled nuclear substances, material, equipment, and technology transferred between Canada and other countries should only be used for peaceful and nonexplosive purposes.

(i) Import and Export Licensing of Nuclear and Nuclear-related Items

Importers and exporters of nuclear and nuclear-related goods and technologies in Canada must obtain and comply with CNSC licenses controlling the international transfer of these goods. The NNIECR sets out the import and export licensing application requirements for a prescribed list of controlled nuclear and nuclear-related substances, equipment, and technologies described in detail in its Schedule.[35] It is particularly important for exporters to review whether an export, despite having non-nuclear-related commercial application, is nevertheless controlled by the NNIECR as a dual-use nuclear substance, equipment, or information, or technology.[36]

The categories in the Schedule to the NNIECR are:

- A.1. Nuclear substances (including special fissionable material such as plutonium and uranium, as well as nuclear grade graphite)
- A.2. Nuclear equipment (including nuclear reactors and specially designed components)
- A.3. Parts for nuclear equipment identified in A.2
- A.4. Nuclear information and technology (including technical data such as drawings and operating manuals)
- B.1. Dual-use nuclear substances
- B.2. Dual-use nuclear equipment
- B.3. Dual-use nuclear information and technology

The basic license application requirements include a detailed description of the substance, equipment, or information and its classification in the Schedule, as well as the intended end-use and end-use

location.[37] Where the application relates to a controlled substance included in Category I, II, or III of the Nuclear Security Regulations,[38] the application must also outline the measures that will be taken to facilitate Canada's compliance with the Convention on the Physical Protection of Nuclear Material.[39] In addition to the enumerated license application requirements, the CNSC also has broad authority under the NNIECR to request any additional information necessary to satisfy the CNSC that the licensee is qualified to carry on the activity, the activity makes adequate provisions for the protection of the environment, health, and safety, and takes all measures required to implement international obligations.[40] Application forms for a license to import nuclear items, and a license to export nuclear and nuclear-related dual-use items, are available for download on the CNSC website.[41] Once completed, application forms must be returned to the CNSC, addressed to the Licensing Administrator, Safeguards Accounting and Technology Division, Directorate of Security and Safeguards.

In 2010, the NNIECR was amended to reflect changes to the NSG Guidelines that had taken place since the NNIECR came into force in 2000. The changes reflect advances in nuclear and nuclear-related technologies and changing proliferation risks.[42] Select amendments include new notes that aim to clarify obligations and reduce regulatory burden on exporters, as well as a requirement for new end-use control for nuclear-related dual-use items to make regulations consistent with international controls.[43]

(ii) Import and Export Licenses for Risk-Significant Radioactive Sources

(A) Export of Risk-Significant Radioactive Sources

Transaction-specific export licenses from CNSC are required to export risk-significant radioactive sources listed in Category 1 and 2 of Table I of the IAEA Code.[44] Substances such as Curium 244 and Plutonium 238 above certain threshold activity levels are included in these categories. These licensing requirements reflect the Canadian government's commitment to working to meet the standards of the Code and IAEA Guidance on the Import and Export of Radioactive Source.[45]

Export licenses can contain any term or condition and are issued at the discretion of a designated officer of the CNSC. The CNSC advises that

exporters should provide sufficient details in their application for the CNSC to effectively evaluate compliance with its standards. Assessment by the CNSC includes consideration of the risk that a risk-significant radioactive source may be diverted for other purposes, as well as a review of whether the regulatory controls of the importing state provide sufficient safeguards for the source to be managed safely and securely. Where an application relates to the export of risk-significant substances in Category 1 of Table I of the IAEA Code, such as certain radionuclide typically used in radiothermal generators, irradiators, and radiation teletherapy, the CNSC will consult with the importing state authority as part of its assessment of the application.[46]

Generally speaking, a license to export a risk-significant radioactive source is required for each export transaction or specific set of transactions that are expected to occur within a specified period of time. The CNSC service standards for review of these license applications is typically within three weeks following receipt of a completed application. That said, the CNSC suggests submitting these license applications at the earliest opportunity, as processing periods can vary depending on factors such as whether the substance falls within Category 1 or Category 2, the required international communications and consultations, and the availability of information on the importer, among other factors.[47]

(B) Import of Risk-Significant Radioactive Sources

Unlike export license requirements for risk-significant radioactive sources, importers of these substances are not required to obtain a transaction specific license. Licensees authorized to possess risk-significant radioactive sources may import these sources without a specific import license from CNSC provided the activity complies with the general import authorization in their possession license.[48] The CNSC requires prior import notifications from the exporting facility or exporting state authority for the import of all Category 1 radioactive sources. Additionally, the import of Category 1 radioactive sources into Canada is subject to prior import consent from the CNSC.[49]

(iii) Export and Import Permits Act

In addition to CNSC licensing requirements, the international transfer of nuclear and nuclear-related goods and technologies may also be subject to export controls under the EIPA where the item appears on the Export Control List (ECL).[50] Nuclear and nuclear-related items are principally outlined in Group 3—Nuclear Non-Proliferation and Group 4—Nuclear-Related Dual Use of the List.[51] Where an item is regulated under the NSCA and EIPA, both an export permit and export license are required.

The export permit process is administered by GAC. Applicants may apply for an export permit through the New Export Controls Online system (NEXCOL). NEXCOL is an internet-based system that allows applicants to apply for export control documents electronically. Alternatively, applicants may submit paper applications for export permits; however, some processing delay may result.[52]

Where applications are filed with each agency, both agencies consult with each other to coordinate licensing and permit decisions. Where the CNSC refuses to issue a license, GAC will typically defer to this decision and consequently deny the issuance of an export permit.[53] Exporters of Group 3 and 4 items should submit their export permit and licensing applications to the Export Controls Operations Division of GAC and to the CNSC separately.[54] In 2021, GAC issued 67 permits of Group 3 items and 49 export permits for Group 4 items.[55]

(iv) Brokering Controls

In September 2019, Canada became a State Party to the UN Arms Trade Treaty (ATT),[56] a treaty establishing standards for international trade in a broad range of conventional arms that currently counts more than 100 State Parties. To meet its ATT obligations, Canada amended the EIPA[57] and adopted a package of brokering regulations, namely, the Brokering Control List,[58] Brokering Permit Regulations,[59] Regulations Specifying Activities that Do Not Constitute Brokering,[60] General Brokering Permit No 1,[61] and General Export Permit No 47.[62]

The newly established legislative scheme imposes export controls over brokering activities with respect to a broad range of items, including nuclear nonproliferation and nuclear-related dual-use goods and technologies.[63] This is a significant development for Canadian industry

members, as this is the first time such controls have been introduced in Canada.

The EIPA defines brokering as an activity aimed "to arrange or negotiate a transaction that relates to the movement of goods or technology included in a Brokering Control List from a foreign country to another foreign country."[64] This means that the import or export of goods or technology in or out of Canada are not covered by the new brokering regulations.

Canada's commitments under the ATT require that exports be assessed to determine whether there is an "overriding risk" that the grant of a permit on certain brokering activity would contribute to the following:

- Undermining of peace and security;
- A serious violation of international humanitarian law or international human rights law;
- An offence under international conventions or protocols relating to terrorism or transnational organized crime to which Canada is a party; or
- Serious acts of gender-based violence or serious acts of violence against women and children.[65]

If it is determined that there is a substantial risk that the intended export or brokering activity would result in any of these negative consequences, and such risk cannot be mitigated, the permit application must be denied. In its administrative guidance explaining the application of the substantial risk test, the Canadian government describes the threshold as being met where "compelling evidence exists of a connection between the proposed export and the negative consequences."[66] This clearly suggests an evidence-based assessment, as opposed to one that considers hypothetical or speculative risks. Notably, this is the first instance in which such humanitarian factors have been expressly incorporated into the Canadian export/import controls framework.

(c) Judicial Consideration: *R. v. Yadegari*

The 2010 conviction of Mahmoud Yadegari in *R. v. Yadegari*[67] on offences related to the attempted exportation of pressure transducers to an individual in Iran provided a rare opportunity for the judiciary to consider Canadian

export controls that apply to nuclear and nuclear-related goods and technologies. *R. v. Yadegari* is the first conviction under the NSCA, and marks the first charge against a Canadian under the United Nations Act (UN Act).[68] In addition to these charges, Mr. Yadegari was convicted for various offences under the EIPA, Criminal Code,[69] and the Customs Act.[70] The Trial and Ontario Court of Appeal decisions set out a useful illustration of the interaction of various export controls that apply to nuclear-related goods, and the judicial approach to enforcing these controls.

In 2009, Mahmoud Yadegari procured a number of pressure transducers from a foreign supplier, and then attempted to export a number of these items from Canada to Iran. While pressure transducers have commercial applications in medical sterilization and food freeze-drying, they are also capable of being used in the enrichment of uranium through gas centrifugation.[71] Mr. Yadegari did not obtain any export licenses or permits, and removed labels identifying the items as pressure transducers. The shipment was intercepted by authorities before the transducers crossed Canadian borders.

While Mr. Yadegari argued that the transducers did not meet threshold content and accuracy requirements and were therefore not subject to export restrictions, the trial judge found and the Court of Appeal affirmed that the technical specifications of the pressure transducers met the technical parameters in the specifications set out in the IAEA Information Circular 254, and were therefore restricted under the Regulations Implementing the United Nations Resolutions on Iran.[72] They also determined that the technical characteristics of the pressure transducers described in the specifications were essentially the same as those described under the NSCA and the EIPA,[73] and therefore required the appropriate regulatory approvals for export outlined in those authorities.

The judicial discussion of sentencing principles underscores the serious nature and international ramifications of activities involving the transfer of nuclear-related goods. The trial judge and the Court of Appeal agreed that breaches of UN Act, NSCA, and the EIPA were of "paramount significance" given the potential harm involved in the actions of the appellants, and that sentencing "should promote responsibility in the offender given the potential harm to the global community."[74] Mr. Yadegari was originally sentenced to 20 months in jail in addition to 15½ months of

presentence custody. This sentence was later reduced by the Ontario Court of Appeal decision by three months.[75]

To date, the *Yadegari* case is the only case in which the Canadian nuclear export control regime has been given any substantive judicial consideration.

---

1. 729 U.N.T.S. 161. NPT was signed on July 1, 1968, and came into force on March 5, 1970.
2. Five states are recognized by the NPT as nuclear weapon states (NWS): China, France, Russia, the United Kingdom, and the United States. All other states are NNWS.
3. 42 U.S.C. §§ 2011 *et seq*.
4. 22 U.S.C. §§ 3201 *et seq*.
5. For a detailed review of the EAR, see Chapter 3.
6. For a detailed review of the ITAR, see Chapter 2.
7. *See* 10 C.F.R. part 110, app. A.
8. *See* INFCIRC/254 part 1, annex A.
9. Int'l Atomic Energy Agency (IAEA), *Code of Conduct on the Safety and Security of Radioactive Sources (IAEA/CODEOC/2004)*, Vienna, 2004, http://www-ns.iaea.org/tech-areas/radiation-safety/code-of-conduct.asp.
10. 70 FR 37993, July 1, 2005; 71 FR 20340, Apr. 20, 2006.
11. 10 C.F.R. § 110.21–110.24.
12. *Id*. § 110.27.
13. DOE's rules define "special nuclear material" as "(1) plutonium, (2) uranium-233, or (3) uranium enriched above 0.711 percent-by-weight in the isotope uranium-235." *Id*. § 810.3.
14. *See* 10 C.F.R. § 810.2(a).
15. 80 FR 9359.
16. 22 U.S.C. §§ 8001 *et seq.*; Pub. L. 109–401.
17. 10 C.F.R. § 810.15.
18. For continuing violations, each day is a separate violation. AEA, Sec. 234.
19. AEA Sec. 223.
20. NRC Enforcement Policy (June 7, 2012), available in the NRC's Agencywide Document Access and Management System (ADAMS) at ML12132A394.
21. Canadian Nuclear Ass'n, *Transportation of Nuclear Substances in Canada*, Mar. 31, 2015, https://cna.ca/2015/03/31/transportation-of-nuclear-substances-in-canada; World Nuclear Ass'n, *Uranium in Canada*, 2019, https://world-nuclear.org/information-library/country-profiles/countries-a-f/canada-uranium.aspx#:~:text=Cigar%20Lake%20mine.-,Rabbit%20Lake,mined%20underground%20in%20recent%20years.
22. *See* Nuclear Power in Canada, https://www.world-nuclear.org/information-library/country-profiles/countries-a-f/canada-nuclear-power.aspx (last updated Aug. 2022).
23. The NTP was signed by Canada on July 23, 1968.
24. *Canada's Nuclear Non-proliferation Policy*, 1985, https://inis.iaea.org/collection/NCLCollectionStore/_Public/21/020/21020770.pdf.
25. Canadian Nuclear Safety Comm'n, *Non-proliferation: Import/Export Controls and Safeguards*, Aug. 25, 2017, http://www.nuclearsafety.gc.ca/eng/resources/non-proliferation/index.cfm.
26. Global Affairs Canada, *Agreement between the Government of Canada and the Government of the Republic of India for Co-Operation in Peaceful Uses of Nuclear Energy ("the Canada-India Nuclear Cooperation Agreement")*, June 27, 2010, https://www.treaty-accord.gc.ca/text-texte.aspx?

id=105192;News Release, Government of Canada, Canada-India Nuclear Cooperation Agreement (Nov. 6, 2012), https://www.canada.ca/en/news/archive/2012/11/canada-india-nuclear-cooperation-agreement.html.

27. Ian Anthony, Christer Ahlström & Vitaly Fedchenko, *Reforming Nuclear Export Controls—The Future of the Nuclear Suppliers Group*, SIPRI Research Report No. 22, at 7 (2007), https://www.sipri.org/sites/default/files/files/RR/SIPRIRR22.pdf.

28. Mark Hibbs, *The Future of the Nuclear Suppliers Group*, Carnegie Endowment for Int'l Peace, 2011, https://carnegieendowment.org/files/future_nsg.pdf, Somini Sengupta & Mark Mazzetti, *Backed by U.S., India Is Approved for Nuclear Trade*, N.Y. TIMES, Sept. 7, 2008, http://www.nytimes.com/2008/09/07/world/asia/07iht-india.1.15946952.html?_r=1. The NSG waiver permits NSG country members to engage in nuclear trade for civilian nuclear power purposes with India, despite India not being a member of the NSG group or a signatory to the NPT. India agreed to IAEA safeguards.

29. *Supra* note 26.

30. S.C. 1997, c. 9. The predecessor statute of the NSCA was the Atomic Energy Control Act.

31. SOR/2000-210.

32. R.S.C., 1985, c. E-19.

33. *Supra* note 30 at sections 8, 9. Prior to the establishment of the CNSC under the NSCA, the regulation of the Canadian nuclear industry was conducted by the Atomic Energy Control Board.

34. Canadian Nuclear Safety Comm'n, *Import and Export Controls*, http://nuclearsafety.gc.ca/eng/nuclear-substances/import-and-export-controls/index.cfm (last modified Feb. 10, 2022).

35. *Supra* note 31. The list of substances described in the Schedule to the NNIECR is reproduced, with some modifications, from International Atomic Energy Agency Information Circulars INFCIRC/254/Rev.9/Part 1, INFCIRC/254/Rev.7/Part 2 and INFCIRC/209/Rev.2.

36. Lawrence Herman, *Export Controls and Economic Sanctions: A Guide to Canadian Trade Restrictions*, Carswell, Toronto, 2011, at 3-3. *See also* Master Tech Inc. v. Canada (Public Safety and Emergency Preparedness), 2015 FC 1395, *aff'd* 2019 FCA 4, and more generally our discussion of *R. v. Yadegari* (July 6, 2010), Toronto, Mocha J (Ont. C J), *aff'd* 2011 ONCA 287, for analysis on how a dual-use item may fall within certain technical parameters and therefore subject to export restrictions.

37. *Supra* note 31 at section 3(1).

38. SOR/2000-209.

39. *Supra* note 31 at section 3(1)(h); INFCIRC/274/Rev.1.

40. *Supra* note 31 at section 3(2)).

41. *Supra* note 34.

42. The revision and implementation of the amended regulations involved, among other activities, a pre-consultation with existing licensees and stakeholders, consultation with the Export Control Division of GAC, as well as the collection of feedback from licensees and stakeholders. Canadian Nuclear Safety Commission, *Amendments to the Non-Proliferation Import and Export Control Regulations: Pre-Consultation Disposition Report* at 1 http://nuclearsafety.gc.ca/eng/pdfs/Reports/NNIECR_Disposition_Report_from_Pre_Publication_in_Part_1-e.pdf.

43. *Id*.

44. Canadian Nuclear Safety Comm'n, *Safeguards and Non-proliferation. Import and Export*. REGDOC-2.13.2, Version 2, at pp. I, 7, Apr. 2018, http://www.nuclearsafety.gc.ca/eng/acts-and-regulations/regulatory-documents/published/html/regdoc2-13-2-ver2/index.cfm.

45. *See* the *Guidance on the Import and Export of Radioactive Sources*, IAEA, https://www-pub.iaea.org/MTCD/Publications/PDF/8901_web.pdf.

46. *Supra* note 34.

47. *Supra* note 44. at section 5.4.

48. Id. at section 5.5.
49. Id. at section 12.2.
50. SOR/89-202. A detailed description of controlled items is included in Global Affairs Canada, *A Guide to Canada's Export Controls*, Dec. 2021, https://www.international.gc.ca/trade-commerce/guides/export_control_list-liste_exportation_controlee_2021.aspx?lang=eng. Exporters should note that some nuclear and nuclear-related items not listed on the Export Control List are controlled under the NSCA and regulations, and require licenses from the CNSC prior to export. *See* Section F.9 of *Export and Brokering Controls Handbook*, Aug. 2019 (Export Controls Handbook), https://www.international.gc.ca/trade-commerce/controls-controles/reports-rapports/ebc_handbook-cce_manuel.aspx?lang=eng.
51. Nuclear-related goods and technologies may also appear in other sections of the list, including the catchall provisions of Item 5505, which imposes permit requirements on an item if it is determined that the end use could be related to the development or production of certain weapons, including nuclear weapons. *See generally* Global Affairs Canada, *Export Controls over Goods and Technology for Certain Uses—Notice to Exports*, Mar. 2011, http://www.international.gc.ca/controls-controles/systems-systemes/excol-ceed/notices-avis/176.aspx?lang=eng&view=d.
52. *Export Controls Handbook, supra* note 50, at section E. 2.
53. Herman, *supra* note 36.
54. *Export Controls Handbook, supra* note 50, at section F.9.
55. 2021 Exports of Military Goods, Foreign Affairs and International Trade Canada, https://www.international.gc.ca/trade-commerce/controls-controles/reports-rapports/military-goods-2021-marchandises-militaries.aspx?lang=eng#:~:text=Most%20of%20Canada's%20military%20exports,in%202021%20(%241.749%20billion).
56. XXVI-8, New York, Apr. 2, 2013, https://treaties.un.org/doc/publication/mtdsg/volume%20ii/chapter%20xxvi/xxvi-8.en.pdf.
57. *An Act to Amend the Export and Import Permits Act and the Criminal Code*, S.C. 2018, c. 26; *Order Amending the Export Control List (Arms Trade Treaty)*, SOR/2019-223.
58. SOR/2019-220.
59. SOR/2019-221.
60. SOR/2019-222.
61. SOR/2019-229.
62. SOR/2019-230.
63. *Supra* note 58.
64. *Supra* note 32.
65. *Id. at* section 7.3(1).
66. Government of Canada, *Questions and Answers: Strengthening Canada's Export Control Program*, Mar. 20, 2019, https://www.international.gc.ca/trade-commerce/consultations/export_controls-controle_exportations/QandA-QetR.aspx?lang=eng.
67. R. v. Yadegari (July 6, 2010), Toronto, Mocha J (Ont. C J) (Yadegari Trial Decision), *aff'd* 2011 ONCA 287 (Yadegari Appeal Decision).
68. R.S.C. 1985, c. U-2.
69. R.S.C. 1985, c. C-46.
70. R.S.C. 1985, c. 1 (2d Supp.). Mr. Yadegari failed to obtain a Certificate of Exemption pursuant to section 20 of the Iran Regulations, an export permit pursuant to section 7 of the EIPA, and a license pursuant to section 26 of the NCSA. Mr. Yadegari failed to report the export of these goods to the Canada Border Services Agency, as required by law, and also failed to report the export of goods with a value over $2,000 and also made a false declaration of their value.
71. Yadegari Appeal Decision, *supra* note 67, at para. 2.

72. SOR/2007-44. These regulations were enacted under the UN Act to uphold Canada's obligation under the UN Security Council Resolution 1737m UNSCOR, 2006, UN DOC. S/RES/1737, which imposed sanctions on Iran for its failure to adhere to its obligations under the NPT. The regulations prescribe it an offence to "knowingly sell, supply or transfer, directly or indirectly," certain products to any person in Iran or for the benefit of Iran (section 3). The list of proscribed goods and technology are set out in IAEA Information Circular *Communications Received from Certain Member States Regarding Guidelines for Transfers of Nuclear-related Dual-Use Equipment, Materials, Software and Related Technology*, UNIAEA OR, 2006, UN Doc. INFCIRC/254/Rev. 7/Part 2, and include pressure transducers that meet certain technical parameters.

73. *Supra* note 31, section B.2.2.8; *supra* note 32.

74. *Supra* note 67, Yadegari Appeal Decision, at para. 95.

75. *See* Pub. Prosecution Serv. of Canada, *Decision Released from the Ontario Court of Appeal*, Apr. 12, 2011, https://www.ppsc-sppc.gc.ca/eng/nws-nvs/2011/12_04_11.html.

12

Export Controls and Economic Sanctions in Argentina

Diego Fissore[1]

12.1 Overview

What Is Regulated: The shipment or transportation from a place in Argentina to a place outside Argentina of goods and technology outside of Argentina, by any means (land, water, or air under Argentine sovereignty), is considered to be an export and it is regulated by the Customs Code or *Código Aduanero* (Law 22.415, "CA") and by the regulation of the *Dirección General de Aduanas* ("DGA," i.e., Customs) and *Administración Federal de Ingresos Públicos* ("AFIP," i.e., Argentine Tax Authority).

Among other things, the CA regulates the mandatory registration of exporters with DGA, the DGA's control authority, export licenses, type of exports subject to control, and the applicable penalties in case of noncompliance with regulations.

Argentine export controls establish rules for the export of military materials and dual-use goods and items under the framework of the international treaties to which the country is a party to and that are related to the development and trade in products and technologies classified as dual-use and military items.

Dual-use and military items include a wide range of goods and technologies that may be used for or in connection with the creation of weapons or for military end use. The controlled items include results of

intellectual activity, including IP rights, as well as the performance of works and the provision of services.

Sanctions and penalties are dealt with in Section 12.9 herein.

Where to Find the Regulations: Argentine laws and regulations are available in Spanish on the official InfoLEG website: http://infoleg.gob.ar. The relevant legislation and regulations are available through the following links:

- CA: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16536/texact.htm
- http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/108616/texact.htm
- http://servicios.infoleg.gob.ar/infolegInternet/anexos/45000-49999/45445/texact.htm
- https://www.afip.gob.ar/exportaSimple/
- http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/63378/norma.htm

Who Is the Regulator: Export controls and sanctions in Argentina fall under the authority of the federal government and are governed by the customs laws adopted by the national congress. The main Argentine body regulating exports is the Customs Office, or DGA, as previously defined.

The CA contains all export control regimes and governs the activities of the DGA. There may be specific applicable regulations to exports, depending on the item, and then authorizations by specific authorities regulating safety of exports or sensitive goods may be required.

Foreign trade in military items and dual-use items is within the sphere of competence of the Ministry of Defense (**MoD**), as well as of the Sensitive Exports and Military Material National Commission, or *Comisión Nacional de Control de Exportaciones Sensitivas y Material Bélico (CNDESyMB)*, which is formed by representatives of the Ministry of Defense, Ministry of Foreign Affairs, Ministry of Public Production/Public Works and representatives of Argentina Nuclear Regulator, Argentine Space Activity Regulator, the Institute of Scientific and Technical Investigation of the Armed Forces and the DGA.

How to Get a License: Argentine export controls apply to individuals and legal entities seeking to export materials classified as sensitive materials

and/or dual-use military items in Decree 603/1992, as amended. In order to obtain an export control license for goods included in those categories, a seller (applicant) should prepare and execute an application for a license together with a standard set of documents, pay state duties as applicable, and apply to the CNDESyMB. The CNDESyBM will evaluate the applications for an export license, case by case, and the criteria with which they will be reviewed will be Argentina's firm commitment to the nonproliferation of weapons of mass destruction, and the relevant international treaties that it is a party to.

Key Websites

- MoD: https://www.argentina.gob.ar/defensa
- CA: https://www.afip.gob.ar/aduana/institucional/
- AFIP (Tax Authority): http://www.afip.gob.ar/home/index.html
- DGA: https://www.afip.gob.ar/aduanaDefault.asp
- *Agencia Nacional de Materiales Controlados* (ANMaC, National Agency of Controlled Materials) (formerly RENAR): https://www.argentina.gob.ar/justicia/anmac/normativa

12.2 Structure of the Laws and Regulations

(a) International Treaties

As mentioned earlier, Argentina is a signatory to a number of multilateral international treaties on export controls, and its national regulations are based on such treaties. In particular, Argentina has ratified the following:

- The Latin-American Non-Proliferation of Nuclear Weapons Treaty (Tlatelolco Treaty, 1967)
- The Treaty on Non-Proliferation of Nuclear Weapons (NPT, 1968)
- The Convention on Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (1972)
- The Convention on Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (Chemical Weapons Convention) (1993)
- The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1995)

- The Australia Group (AG)
- The Nuclear Suppliers Group (NSG)
- The Zangger Committee (ZC)
- The Missile Technology Control Regime (MTCR)

The preceding treaties have been incorporated into Argentine national law through the following laws:

- The Latin-American Non-Proliferation of Nuclear Weapons Treaty (Tlatelolco Treaty, 1967); Law 24.272
- The Convention on Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (1972); Law 21.938
- The Treaty on Non-Proliferation of Nuclear Weapons (NPT, 1968); Law 24.448
- The Convention on Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (1993); Law 24.534

(b) Argentina and Mercosur

Argentina is a party of the *Mercado Común del Sur* (**Mercosur**). The states that are members of Mercosur are Argentina, Brazil, Paraguay, Uruguay, and Bolivia. Associate states are Bolivia, Ecuador, Guyana, Chile, Peru, and Surinam. While Mercosur establishes a customs union and the free movement of goods between member states, each member state has its own export control regulations.

(c) Argentine National Laws and Regulations on Export Controls

Argentine laws on export controls are primarily based on the Wassenaar regulations, but differ in some details. The main Argentine laws on dual-use items include the following:

- Law 12.709, dated September 26, 1941, on Military Production (Law 12.709)
- Law 20.010, dated December 11, 1972, on Amendments to Law 12.709 (Law 20.010)

- CA Law No. 22.415, dated March 2, 1981. This is the main legal act that establishes the basic principles of Argentine export control and implements regulations on export control licensing and supervision.
- Decree 1097/1985, dated June 14, 1985, on Creation of the CNDESyMB (Decree 1097)
- Governmental Decree No. 603/92, dated April 9, 1992, on Sensitive Exports and Military Material Exports Regime (Decree 603)
- Customs Resolution 1046/92, dated July 24, 1992, on Customs Classification of Goods (CR 1046)
- Decree 1291/93, dated June 24, 1993, on Amendments of Annex B Decree 603/92 (Decree 1291)
- Joint Resolution 1373/3728/1634 Ministries of Defense, Foreign Affairs and Economy and Public Works, dated December 15, 1993, on Amendments to Decree 603 re Chemical Substances (JR 1373)
- Governmental Decree No. 657, dated May 8, 1995, on Military Materials Control System (Decree 657)
- Joint Resolution 59/23/26 Ministries of Defense, Foreign Affairs and Economy and Public Works, dated January 9, 1995, on Controls on Nuclear Exports (JR 59)
- Joint Resolution 125/2097/41 Ministries of Defense, Foreign Affairs and Economy and Public Works, dated March 3, 1998, on Additions to Annex B Decree 603/92 on Chemical Substances (JR 125)
- Decree No. 101, dated February 1, 2000 (Decree 101)
- Decree No. 437, dated May 30, 2000, on Annexes D and E, and Amendments to Decree 603/92 (Decree 437)
- Law 26.247 (Law 26.247)
- Joint Resolution 52/52/52 Ministries of Defense, Foreign Affairs and Public Works, dated July 23, 2019, on Export Controls Military and Dual Use Materials (JR 52)

(d) Controlled Lists

Argentine lists of dual-use and other controlled items are established by the annexes to JR 52, which are the ones that replace the annexes to Decree 603/92. These annexes are updated and amended from time to time, in general following the recommendations of the international groups to which

Argentina is a party to as a result of the international treaties listed in 12.6 herein.

Currently, the following lists of military materials and dual-use items are included in relevant export control lists in Argentina:

- The List of Equipment, Software and Technology of the Missile Technology Control Regime (Annex I to JR 52, replacing Annex A, Decree 603)
- The List of Chemical Substances Subject to Control by the National Government; the List of Dual-Use Chemical Facilities and Equipment and Associated Computer Technology and Technology Systems, the List of Dual-Use Biological Equipment and Associated Technology and Computer Systems, the List of Human and Animal Pathogens and Toxins for Export Controls, and the List of Vegetable Pathogens (Annex II to JR 52, replacing Annex B, Decree 603)
- The List of Nuclear Products or Products of Nuclear Use; the Directives for the transference of Double-Use Nuclear Equipment, Materials and Software and of Related Technology; and the List of Dual Use Nuclear Equipment, Materials and Software and Related Technology (Annex III to JR 52, replacing Annex C, Decree 603)
- The List of Military Material (Annex IV to JR 52, replacing Annex D, Decree 603)
- The List of Dual-Use Materials and Technology (Annex V to JR 52, replacing Annex E, Decree 603)

12.3 What Is Regulated: Scope of the Regulations

The delivering outside of Argentina, by any means (land, water or air under Argentine sovereignty) of any type of material or good is considered to be an export and is regulated—which does not mean controlled—by the CA and by the corresponding regulations of the DGA and AFIP.

Pursuant to sections 9 and 10 of the CA, the same regime as goods applies to exports that include scientific and technical information (i.e., technology), results of intellectual activity and IP rights, performance of works. Argentine export controls may also extend to re-exports or transfers.

The CA regulates the mandatory registration of exporters with the DGA, the DGA's control authorities, shipping licenses, types of covered

exports, and applicable penalties in case of noncompliance with regulations.

As to military items and dual-use items, Argentine export controls apply to any items falling under the lists of controlled items mentioned in Section 12.2(d). Exportation of such items from Argentina would be subject to special export control clearance, that is, the exporter of record would need to obtain an export control license (or other type of authorization that may be issued or be required by specific regulation) issued by a competent body responsible for export control clearance of the particular products.

Argentine export controls also provide a "catchall" clause, by which exporters of record must obtain an export control license for items that do not fall under any of the controlled lists, but the exporters understand that the end-user will or could apply such items for military end-use purposes, which are mentioned in the relevant regulations as "used as weapons of mass destruction."

Argentine export control requirements apply to any type of export regarding items included in the lists in 12.2(d). This may include actual shipments of dual-use goods including dual-use technology on documents and other fixed media (irrespective of the origin of the goods/technology), hand carries by individuals, and intangible transfers by means of electronic correspondence, intranet, electronic downloads, fax, or telephone (for example, if relevant controlled parts are read out or described).

If a product, by its description, HS classification, technical characteristics, or offend-use may potentially fall under Argentine export control regulations, a special export license must be obtained from the CNDESyMB prior to exportation (Decree 603/92, sections 6, 11, and 14, as amended). As a general rule, such a license should not be granted if there are reasonable grounds to conclude that the relevant materials will be used to manufacture weapons of mass destruction. In addition, exporters of items that are not included in the lists indicated in Section 12.2(d) must request a prior export license when it is known, or there are grounds to have suspicions, that the exported elements will be used to manufacture weapons of mass destruction.

Therefore, in the process of analyzing an export from Argentina of any issue that falls in the lists included in 12.2(d). herein or materials that are not in them but may be used in the production of military material, it is recommended to analyze whether the items in question are likely to fall under Argentine dual-use export control regulations; and instruct your

Argentine counterpart to make the required arrangements and legal actions in order to comply with Argentine export controls (i.e., prepare the necessary documentation, obtain permit documents, etc.).

12.4 Who Is Regulated?

The activities of all exporters, regardless of their nationality and nature (individuals, legal entities, private or public entities, among others) are subject to the CA and export controls. Exporters are those who export, or who cause the export, of goods or technology from Argentina.

12.5 Classification

(a) Classification of Dual-Use Items

The lists of controlled items in Section 12.2 (d) provide a general description of controlled goods. Dual-use items include those described in the following sections of the lists:

- List of Dual-Use Chemical Facilities and Equipment and Associated Computer Technology and Technology Systems (JR 52, Annex II, replacing Annex B, Decree 603)
  - Installations and Manufacturing Equipment
  - Toxic Gas Monitors, Monitoring Systems and its special detector components
- List of Dual-Use Biological Equipment and Associated Technology and Computer Systems (JR 52, Annex II, replacing Annex B, Decree 603)
  - Equipment
  - Associated Technology
  - Software
- List of Dual-Use Nuclear Equipment, Materials and Software and Related Technology (Annex III to JR 52, replacing Annex C, Decree 603)
  - Item 1. Industrial Equipment.
  - 1.A. Equipment, Assembling and Components
  - 1.B. Production and Trials Equipment

- 1.C. Materials
- 1.D. Software
- 1.E. Technology
- 2. Materials
- 2.A. Equipment, Assembling and Components
- 2.B. Production and Trials Equipment
- 2.C. Materials
- 2.D. Software
- 2.E. Technology
- 3. Equipment and Components for the Serration of Uranium Isotopes
- 3.A. Equipment, Assembling and Components
- 3.B. Production and Trials Equipment
- 3.C. Materials
- 3.D. Software
- 3.E. Technology
- 4. Equipment Related to Heavy Water Production Plants
- 4.A. Equipment, Assembling and Components
- 4.B. Production and Trials Equipment
- 4.C. Materials
- 4.D. Software
- 4.E. Technology
- 5. Trial and Measurement Equipment for the Development of Nuclear Explosives
- 5.A. Equipment, Assembling and Components
- 5.B. Production and Trials Equipment
- 5.C. Materials
- 5.D. Software
- 5.E. Technology
- 6. Component for Nuclear Explosive Devices
- 6.A. Equipment, Assembling and Components
- 6.B. Production and Trials Equipment
- 6.C. Materials
- 6.D. Software
- 6.E. Technology

- List of Dual-Use Materials and Technology (Annex V to JR 52, replacing Annex E, Decree 603, replacing Annex E, Decree 603)

- Item 1. Special Materials and Related Equipment
- Item 2. Materials' Treatment
- Item 3. Electronics
- Item 4. Computers
- Item 5. I. Telecommunications.
- Item 5. II. Information Security
- Item 6. Systems, Equipment and Components
- Item 7. Navigation and Avionics
- Item 8. Marine Equipment
- Item 9. Propulsion and Aerospace Materials

HS codes are not included in the preceding lists, so the exporter needs to consider the description of goods/technologies and their technical characteristics. Other lists of controlled items (i.e., on missile weapons, chemical and biological items) provide descriptions and HS classifications.

(b) Classification of Military Items

JR 52 updated all lists of export-controlled items related to military use. Annexes I, II, III, and IV to JR 52 provide with the lists a description of each relevant item, which are in addition to the List of Dual-Use items mentioned in the preceding section.

- List of Equipment, Software and Technology of The Missile Technology Control Regime (Annex I to JR 52, replacing Annex A, Decree 603)
  - Category I, Item 1. Complete Systems
  - Category I, Item 2. Subsystems Used for Complete Systems
  - Category II, Item 3. Equipment and Components for Propulsion
  - Category II, Item 4. Propellants, Chemical Components and Propellants Production
  - Category II, Item 5. (Reserved for future use).
  - Category II, Item 6. Structure Materials Production, Pyrolytic Deposition and Densification and Structural Materials
  - Category II, Item 7. (Reserved for future use)
  - Category II, Item 8. (Reserved for future use)
  - Category II, Item 9. Instrumentation, Navigation and Goniometric
  - Category II, Item 10. Flight Control
  - Category II, Item 11. Avionics

    - Category II, Item 12. Launching Support
    - Category II, Item 13. Computers
    - Category II, Item 14. Analogical and Digital Converters
    - Category II, Item 15. Trials Installations and Equipment
    - Category II, Item 16. Modelling, Simulation and Integration Design
    - Category II, Item 17. Observability Reduction (Stealth)
    - Category II, Item 18. Protection against Nuclear Effects
    - Category II, Item 19. Other Complete Systems
    - Category II, Item 20. Other Sub-Complete Systems
- The List of Chemical Substances Subject to Control by the National Government (Annex II to JR 52, replacing Annex B, Decree 603)
- The List of Human and Animal Pathogens and Toxins for Export Controls, (Annex II to JR 52, replacing Annex B, Decree 603)
- The List of Vegetable Pathogens (Annex II to JR 52, replacing Annex B, Decree 603)
- The List of Nuclear Products or Products of Nuclear Use (Annex III to JR 52, replacing Annex C, Decree 603)
    - Equipment
    - Software
- The List of Military Material (Annex IV to JR 52, replacing Annex D, Decree 603)
    - The military list includes weapon/goods, vehicles/parts/spare parts, technical documentation, works/services.

12.6 General Prohibitions/Restrictions/Requirements

Every exportation of controlled items from Argentina must be carried out under the authority of an export license. Violating this requirement exposes the exporter to law-enforcement consequences, including severe penalties. Such enforcement activities may occur even with respect to products/services/information that do not expressly fall under export control requirements but where there is a risk that they may be used, or where it could be suspected that they may be destined for military end-use purposes.

12.7 Licensing/Reasons for Control

(a) Types of Export Control Licenses and Permits for Dual-Use Items

The general purpose of the regulation related to export controls of military materials and dual-use materials is that suppliers in Argentina should not authorize exports of equipment, materials, software, or related technologies specified in the relevant legislation for use by a non-nuclear-weapon State in an activity related to explosive nuclear devices or an activity of the nuclear fuel cycle not subject to safeguards or, in general, when there is an unacceptable risk of diversion to these types of materials or equipment, or when exports are contrary to the objective of avoiding proliferation of nuclear weapons, or when there is an unacceptable risk of diversion to acts of nuclear terrorism.

In order to achieve that end, there is a series of regulations related to export controls, which are briefly described here.

In essence, all exports of military materials, chemical products, nuclear materials, including equipment, materials, technology, software, and/or ancillary items, included in the lists to the annexes to Decree 603, as amended and currently as they are in JR 52, are prohibited without a license issued by the CNDESyMB.

Pursuant to Decree 1097/1985, the CNDESyMB must first authorize even the negotiations related to the possible export of military materials.

And Decree 603 states that nuclear, military materials (missiles and related technology) and chemical precursors require a prior license granted by the CNDESyMB (sections 3, 11, and 14). It also states that, in principle, the export of equipment, materials, technology, assistance, and services related to uranium enrichment, reprocessing of combustibles, heavy water and plutonium production, and missiles is forbidden if it is suspected that they may be used for the manufacturing of military weapons, mentioned in the regulations and weapons of mass destruction (sections 6, 12, and 14); and that the exports of enriched uranium, reactors and associated technology, and missiles is forbidden unless there is a treaty with the importing country (section 7).

Violations of the system stated by Decree 603 are offences under the CA and the Criminal Code.

Section 1 of Decree 657 establishes that prior to issuing an export license, it must require an End User Certificate, which confirms the end

user in the country of importation and that the exported goods or technology will not be re-exported without that the approval of the relevant Argentine authorities. The certificate must have a one-year validity. The relevant Argentine authority reserves the right to authorize or not the future re-exports of the relevant materials.

Pursuant to Decree 657, Argentina reserves the right to control the re-export of controlled goods or technology to verify that it was sent to the final end user.

Decree 437 states that certain equipment that are considered to be "civil use weapons" included in its Annex D, currently modified by Resolution 52, will be subject to control by the *Registro Nacional de Armas* or National Registry of Weapons (RENAR). Items considered to be civil use weapons are subject to simplified administrative filing requirements as listed in section 4 of Decree 437.

Law 26.247 regulates the import and export of chemical products under the Chemical Weapons Convention. Section 13 thereof prescribes related reporting requirements and forbids the import and/or export of products included in Lists 1, 2, and 3 of the Chemical Weapons Convention.

Resolution 52 similarly governs the transfer of nuclear equipment, materials, and dual-use software and related technology (Annex III, Part II).

(b) Export Control Licensing Procedure

Export administrative regulations and proceedings apply to all exports from Argentina.

To export (with few exceptions such as items carried abroad by travelers, and by other types of noncommercial exports such as personal items), all persons must first register with the National Registry of Exporters, or *Registro de Exportadores e Importadores*, which is in charge of the DGA. To that end, a form should be filed (OM 1228-E), together with the following documentation:

- Evidence of the registration in the relevant office of corporations
- Bylaws of the relevant entity
- Registration with the local tax authority and fiscal domicile
- Evidence of solvency (a bond may be posted in this respect)
- Good conduct certificate or equivalent document

- Determination of authorized persons to sign documentation related to foreign commerce and Customs

After that registration is obtained, administrative filings are necessary with the DGA in order to obtain DGA clearance of the export. The purpose of those filings is, mainly, to control the quality of the exported goods and eventually to have access to information for fiscal purposes.

Specific types of goods or assets may require a specific license, as it is the case of any the items included in the lists that are the annexes to Decree 603, prior license approval by the CNDESyMB has to be obtained.

As indicated above in Section 12.7(a), section 1 of Decree 657 establishes that prior to issuing an export license, the CNDESyMB must require an End User Certificate, which informs who the export beneficiary is and that the materials being exported will not be re-exported without that the approval by the Argentine relevant authorities. The certificate will have a one-year validity. The relevant Argentine authority reserves the right to authorize or reject the future re-exports of the relevant materials.

Pursuant to Decree 657, Argentina reserves the right to control the exported items after the export has been completed to verify that it was sent to the end user identified in the end-use certificate.

After the export is approved, an administrative decision is issued by the MoD (Decree 437, section 3).

12.8 General Licenses/License Exceptions

As to imports of general goods and merchandise, Resolution No. 523/17 from the former Secretary of Commerce, modified by Resolution 1/20 issued by the Secretary of Commerce, Technology and Administration of Foreign Trade (SIECyGCE), establishes that all the tariff positions of the Common Nomenclature of the Mercosur (N.C.M.) with final import destination for consumption will have to file for an Automatic Import License, with the exceptions of the tariff positions included in Annex II of said Resolution 523/2017, as amended, which should file for a Non-automatic Import License.

12.9 Penalties, Enforcement, and Voluntary Disclosures

(a) Administrative Penalties

The CA sets penalties for violations of the CA or administrative regulations related to imports or exports. The penalties are in the form of fines amounting to the price of products involved in the violation, and may include the confiscation of the goods or technology.

The statute of limitation period for this type of violation is as prescribed by the CA, and it is five years as from the 1st of January of the year following the year of occurrence of the penalized fact or of its verification, in the latter case, if it was not possible to know when the penalized fact took place (CA, sections 934 and 935).

(b) Criminal Penalties

Section 867 of the CA states that imprisonment of 4 to 12 years will be imposed to persons that commit the crime of smuggling or of illegal exportation from Argentina, as well as to the persons that in any manner would hinder the application of the relevant export laws, when those crimes are related to nuclear items; explosives; aggressive chemicals or related materials; weapons, ammunition, or materials that are considered materials for war; or substances or items that, by their nature, quantity, or characteristics, could affect national security. The criminal sanctions stated herein may be even higher if the relevant violation may also constitute the commission of an additional crime with a stricter sanction.

Special regimes may apply additional sanctions. For instance, Law 26.247 imposes fines of up to $pesos1,000,000 to the persons or entities that do not comply with Law 26.247 and the Chemical Weapons Convention, and if such violation is also a crime, prison from 1 to 15 years could be imposed to the offender, depending on the crime.

(c) Enforcement

Administrative penalties are enforced by the DGA. Administrative proceedings are started in the DGA and they may be subject to court appeals.

Criminal investigations are initiated by the filings of accusations, which may be started by the DGA, and they are tried in the Criminal Federal Courts of the jurisdiction where the alleged crime has been committed.

(d) Voluntary Disclosure

Argentine entities or individuals are not legally required to report violation of Argentine laws. In other words, the failure to report a violation is not itself an additional offence.

However, when companies that operate in foreign trade note that, as a consequence of an involuntary error, they have incurred a customs violation, they have the chance to make a “self-report” of such error. The self-report grants a substantial reduction in the applicable penalty as a benefit (the equivalent of 25 percent of the minimum fine provided for the offense in question must be paid). In addition, the fact is not registered as an infringement precedent for the company.

This possibility applies mainly to errors in the custom declarations of goods and it is provided for by section 917 of the CC.

12.10 Recent Export Enforcement Matters

There has been no information published as to recent enforcement actions related to dual-use materials.

12.11 Special Topics

(a) Re-export

Re-export of controlled items may be subject to special clearance under Argentine export controls. Re-export is the transfer of controlled items by the initial end user to any third parties, including in the territory of Argentina. The CNDESyMB reserves the right to authorize any re-export.

(b) Recordkeeping

In principle, all exports—including that of dual use materials—have the recordkeeping requirements. The recordkeeping requirements for dual-use goods depends of the type of good and final uses involved. Also, for dual-use goods, depending on the item, prior registrations and licenses may be necessary.

The mandatory retention period is, approximately, of ten years as from the year of the export, which ends up being 11 years (according to AFIP Resolution General 2721/09 (RG 2721) section 5).

The recordkeeping obligation is on the person declaring the export, who may be the customs' agent or the exporter.

Fines applicable to recordkeeping violations are stated in RG 2721 AFIP and they refer to the relevant sections related to penalties and sanctions in the Customs Code, or CC. The CC has a chapter dedicated to penalties and sanctions, which includes the penalties applying to formal violations and also to custom crimes. The events are called "other violations" (section 994, CC, which provides for fines ranging from 500 pesos to 10,000 pesos") since there is no specific provision for "non-keeping the proper registration." But the final amount of the penalty may vary according to the degree and importance of the violation.

(c) How to Be Compliant When Exporting Out of Argentina

It is of the essence that prior to any export a thorough review of regulations for the specific good to be exported is carried out with the customs agent and trade law experts. Regulations and interpretations thereof change very frequently.

---

1. Diego Fissore is a lawyer at G. Breuer in Argentina. https://www.gbreuer.com.ar/index.php/en/our-team-diego-fissore/.

13

Export Controls and Economic Sanctions in Australia

Andrew Hudson[1]

13.1 Overview

Australia regulates the movement of goods, services, and persons passing across our international barrier. In general, there are no restrictions on movement across state borders, and there is a provision in the Australian Constitution Act 1901 that guarantees freedom of movement of goods, services, and persons. However, there were some internal limits of movement across state borders relating to the COVID-19 pandemic, including “lock downs,” which stopped movement of “nonessential” goods and services and required some persons from other states to observe “quarantine” before full entry to the arrival state. Those restrictions have now been largely released. For current purposes, I propose to focus on Australian export controls and implementation of Australia’s “sanctions” regime.

This chapter provides an overview of the structure and authority of Australian sanction laws; how they are created; and the scope of activities, entities, and persons to whom they apply.

13.2 Overview of General Export Controls

The export controls regime in Australia exists in a number of different legislative spaces, but we thought it was more useful to focus on the main

legislation and other regulation governing the export of goods.

Part VI of the Australian Customs Act 1901[2] (Customs Act) prescribes that regulations may be created to govern the export of certain goods. This is effected through the Customs (Prohibited Exports) Regulations 1958.[3] This act, the regulation, and the controls are administered by the Australian Border Force (ABF), which is part of the Department of Home Affairs.

There are export controls to be found in other areas, such as the Export Control Act 2020[4] and rules and regulations made under that act. This act largely applies to biosecurity issues and is administered by the Department of Agriculture, Fisheries and Forestry (DAFF).[5]

There is also specific legislation for "Defence Export Controls."[6] This covers the Defence Trade Controls Act 2012,[7] the Customs Act (and regulations), and the Weapons of Mass Destruction (Prevention of Proliferation) Act 1995[8] and associated regulations.[9] From the defense perspective, Australia is also party to a number of important international controls such as the Missile Technology Control Regime and the Wassenaar Agreement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. These controls are administered by the Department of Defence (DOD).

In more recent times, Australia has moved to impose significant additional import controls on goods originating from Russia and Belarus or due to be exported to Russia and Belarus. This has included additional customs duties on goods originating from Russia and Belarus as summarized in the ABF Notice[10] and the temporary removal of customs duties on goods imported from Ukraine, summarized in the ABF Notice.[11] The additional import duties have been imposed arising from the conflict between Russia and Ukraine and have been extended (see https://www.abf.gov.au/help-and-support-subsite/CustomsNotices/2022-45.pdf). The majority of sanctions[12] imposed have been imposed pursuant to Australian autonomous sanctions regime, which are discussed in more detail in section 13.4 of Chapter 13.

13.3 Overview of Economic Sanctions

Australia's economic sanctions, also known as financial sanctions, are utilized by the Australian federal government (also known as the Commonwealth government) as a tool of international diplomacy and a means to influence governments, entities, or persons outside of Australia by "preventing material assistance to regimes engaged in violations of international standards and norms, including human rights abuses, acts of aggression and destabilizing actions."[13] Australia's sanctions regime reflects those of "like-minded" states and multilateral actions intended to influence matters of international concern:

> . . . sanctions regime[s] are imposed only in situations of international concern, including the grave repression of human rights, the proliferations of weapons of mass destructions or their means of delivery, or armed conflict. Modern sanctions regimes impose highly targeted measures designed to limit the adverse consequences of the situations, to seek to influence those responsible for it to modify their behaviours and to penalise those responsible.[14]

Australian sanctions laws work in conjunction with other restrictions on the movement of goods deemed to require control on import or export for other reasons as well as restrictions on financial transactions. However, the purpose of this chapter is to focus on controls arising from sanctions.

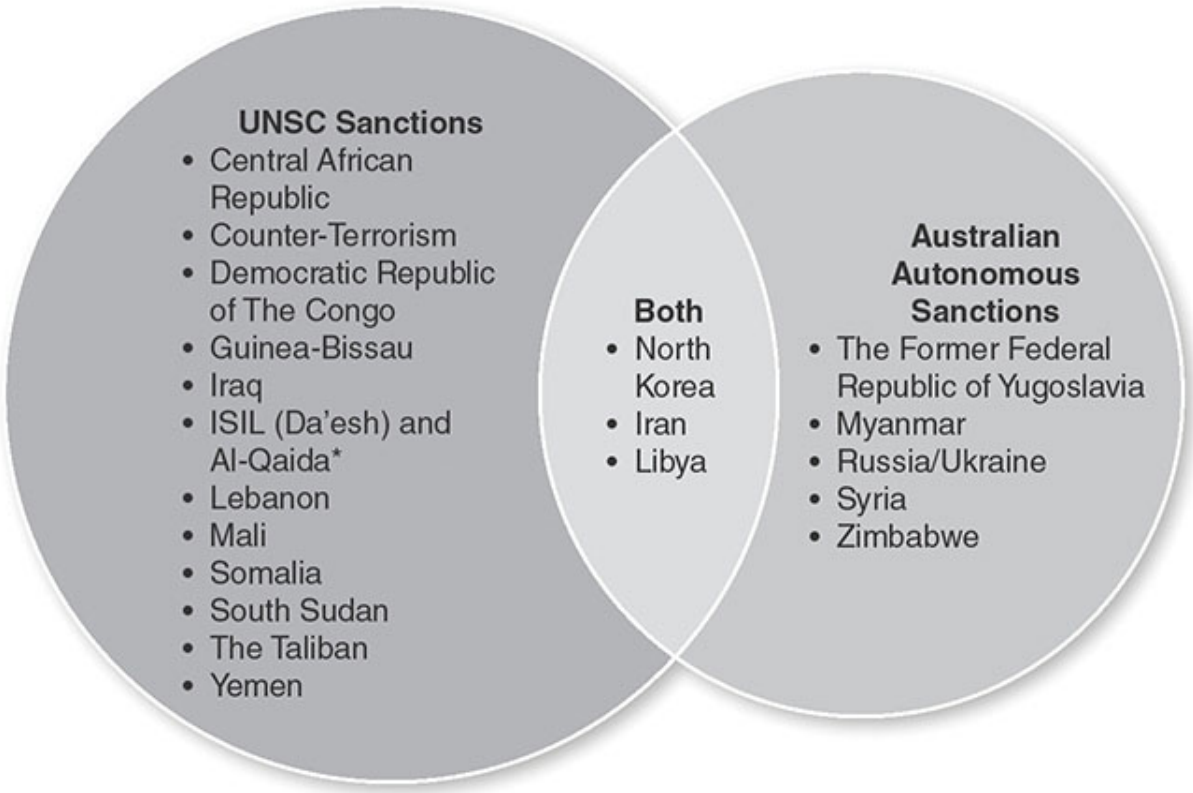
13.4 Australian Sanctions Laws

Australian sanctions laws implement the UN Security Council decisions and resolutions to impose sanction measures (UN Security Council Sanctions), incorporating them into domestic law. This is effected through the Charter of the United Nations Act 1945 (UN Act).[15] Australian laws also provide for additional "autonomous" sanctions measures (Autonomous Sanctions) to be imposed unilaterally or in conjunction with other like-minded states, whether independent of UN Security Council Sanctions or intended to complement them. In Australia, Autonomous Sanctions are imposed through the Autonomous Sanctions Act 2011 (Cth)[16] (Autonomous Act). Both the UN Act and the Autonomous Act have associated regulations and statutory instruments such as the Autonomous Sanctions Regulations 2011[17] (Autonomous Sanctions Regulations). More recently, Australia has moved to impose "thematic sanctions" by way of amendments to the Autonomous Sanctions Act. The new legislation is

known as the Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021.[18]

However, for current purposes, the "thematic sanctions" will be considered as part of the Australian Autonomous Sanctions.

A graphic representation of the interaction of the UN Security Council sanctions and Australian Autonomous Sanctions follows:



(a) What Is Regulated?

The UN Act, the Autonomous Act, and the associated regulations and statutory instruments use the following common terms to describe the types of sanction measures and what those measures prohibit:

- Making a "sanctioned supply" of "export sanctioned goods";
- Making a "sanctioned import" of "import sanctioned goods";
- Providing a "sanctioned service";
- Engaging in a "sanctioned commercial activity";
- Dealing with a "designated person or entity";
- Using or dealing with a "controlled asset"; or

- The entry into or transit through Australia of a “designated person” or a “declared person.”

(b) Where to Find the Regulations

Australia’s statutes and subsidiary legislation (regulations and other legislative instruments) can be accessed through the Federal Register of Legislation (formerly known as ComLaw) at https://www.legislation.gov.au/.[19]

Other laws of the Commonwealth may be declared to be a “sanction law” under section 6 of the Autonomous Act. Laws that have been specified as a sanctions law are set out in the Autonomous Sanctions (Sanction Law) Declaration 2012 (Cth),[20] which is intended to be an index to all laws to which the provisions of the Autonomous Act are intended to apply. For current purposes, these include certain provisions of the Autonomous Sanctions Regulations and Regulations 11, 11A, 11B, and 11E of the Customs (Prohibited Exports) Regulations 1958 (Cth)[21] (Prohibited Export Regulations). Most recently, this includes new listings in February 2022 in relation to Ukraine.

Further information about Australia’s current sanctions regimes, the regulations made in respect of those regimes, and other regulatory requirements, are provided on the Department of Foreign Affairs and Trade (DFAT) website.[22]

(c) Who Is the Regulator?

From January 1, 2020, the Australian Sanctions Office (ASO) became the Australian government’s sanctions regulator. According to DFAT, as the sanctions regulator, The ASO:

- Provides guidance to regulated entities, including government agencies, individuals, businesses, and other organizations on Australian sanctions law;
- Processes applications for, and issues, sanctions permits;
- Works with individuals, businesses, and other organizations to promote compliance and help prevent breaches of the law;
- Works in partnership with other government agencies to monitor compliance with sanctions legislation; and

- Supports corrective and enforcement action by law enforcement agencies in cases of suspected noncompliance.

The ASO is located within DFAT's Legal Division in the International Security, Humanitarian and Consular Group. As a result, administration of the sanctions laws and regulations is ultimately undertaken by DFAT.

Under the Autonomous Act, the Minister for Foreign Affairs (Minister) is granted broad executive powers in the administration of the sanctions laws. Other agencies with administrative responsibilities include the following:

- DOD
- DFAT
- Defence Export Control Agency (DEC) (an agency within the DoD)
- Australian Federal Police (AFP)
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Australian Securities and Investment Commissions (ASIC)
- ABF as a part of the Department of Department of Home Affairs
- DAFF
- Reserve Bank of Australia (RBA)

13.5 Scope of the Regulation

(a) Territorial Application of the Laws to Persons and Entities

Australia's UN Security Council Sanctions and Autonomous Sanctions laws apply to any person in Australia, any person using an Australian flagged vessel or aircraft, any Australian citizen or body corporate anywhere in the world, and any Australian body corporate, in respect of the actions of a third-party body corporate or entity, wherever incorporated or situated, if the Australian body corporate exercises effective control.

(b) Extraterritorial Application to Persons or Entities

There is also scope under principles of international law for the Commonwealth government to enforce its sanctions laws against persons and entities whose actions have effect in Australia or on an Australian citizen or Australian body corporate. Although generally Australian statutes

are presumed to extend only to the territorial limits of Australia, the Commonwealth government has a constitutional power to legislate extraterritorially utilizing the "external affairs power" under section 51 (xxix) of the Australian Constitution.

Division 2 of Part 3 of the UN Act, relating to penalties and injunctions, and Division 2 of Part 2 of the Autonomous Act, relating to injunctions and invalidation of authorizations are expressed to have extraterritorial effect. In addition, the acts each provide that the regulations made under them may be expressed as having extraterritorial effect. Offences under the Autonomous Act relating to providing false or misleading information in respect of sanctions laws, and the offence provisions under the UN Act are also expressed as subject to the extended geographical jurisdiction under section 15.1 of the Criminal Code (Cth), which gives these provisions extraterritorial effect.

In enforcing sanctions laws extraterritorially, the Commonwealth government may have recourse to arrangements made under extradition treaties entered into with foreign governments. Further enforcement powers to make applications for extradition of persons (or respond to applications from foreign governments for extradition of persons from Australia) are set out in the Extradition Act 1988 (Cth) and the Mutual Assistance in Criminal Matters Act 1987 (Cth). The application of sanctions laws can therefore be said to apply to any person or entity whose actions have a sufficient nexus with Australia, provided that the actions are within the scope of those laws expressed as having extraterritorial application. Essentially, Australian sanctions laws apply to anyone within Australia and to Australian nationals (individuals and entities) outside Australia.

13.6 Prohibition Relating to the Supply of "Export Sanctioned Goods"

(a) Meaning of "Sanctioned Supply"

A "sanctioned supply" is the direct or indirect supply, sale, or transfer, without authorization, of "export sanctioned goods" in relation to a country, or a part of a country designated by the Minister. Export sanctioned goods are set out in the Table in Regulation 4 of the Autonomous Sanctions

Regulations and differ depending on the country to which they are being supplied.

There are several steps required to determine whether goods are export sanctioned goods. The first step is to consider whether the intended recipient, beneficiary, or the use of the goods is in relation to a country or a part of a country that is subject to the Australian Autonomous Sanction regime or a UN Sanction regime. If the recipient or beneficiary is in a country or part of a country subject to Australian sanction measures, the second step (discussed next) is to determine whether the particular goods intended to be supplied are "sanctioned export goods" under the applicable sanction regime.

(b) Meaning of "Export Sanctioned Goods"

In respect of autonomous sanction measures, the second step to identify whether something is a sanctioned supply requires an analysis of whether the goods might broadly fit within the categories set out in the Autonomous Sanctions Regulations. The export sanctioned goods for countries subject to autonomous sanctions measures are set out in the Table in Regulation 4 of the Autonomous Sanctions Regulations. Sub-regulation 4(2) of the Autonomous Sanctions Regulations[23] provides for the Minister to specify, by legislative instrument, certain items as export sanctioned goods for the countries referred to in the Table to that sub-regulation. In addition to a description of the goods, reference should be had to the corresponding Australian Harmonized Export Commodity Classification (AHECC) Code, also listed in the instruments including them in the sub-regulation when determining whether a good is subject to sanction measures.

Other types of goods are specified in the regulations and legislative instruments in respect of a particular sanction regime and can be identified in those instruments by reference to "other writing" or list-based references which identify the export sanctioned goods. In addition, reference can be made to the explanatory memorandum associated with the instruments, which includes the goods as export sanctioned goods.

There is some uncertainty as to whether goods are only "proscribed" if they meet both the AHECC code and the description. If a person considers that the goods in question only match the AHECC code or only match the description but not both, an inquiry should be submitted through the new

“Pax” system (Pax) maintained by DFAT, which commenced on October 1, 2020.[24]

(c) Arms and Related Matériel

“Arms or related matériel,” sometimes referred to as “arms or related lethal materiel” or “weapons or military equipment” are included in the definition of export sanctioned goods in some UN Security Council sanctions regimes and in the Autonomous Sanctions Regulations in respect of a number of countries.

The “non-exhaustive” definition of arms or related matériel is set out in UN Charter Act, which is consistent with the definition in Regulation 3 of the Autonomous Sanctions Regulations. The Australian definition of this term includes any of the following:

- Weapons
- Ammunition
- Military vehicles and equipment
- Spare parts and accessories for the things mentioned above
- Paramilitary equipment

The definition of this concept in Australian law for both UN Security Council and Australian autonomous sanctions regimes is not considered to be exhaustive. Consequently, not all goods that are considered arms or related matériel are listed in the preceding definition, and DFAT is required to make a determination based on the nature of the good, its proposed or actual end use, and the end user of the good.

There are essentially three steps to determine if goods fall within the scope of arms or related materiel:

- Step 1: Consider whether the goods are of a type listed in the definition in Regulation 3 of the Autonomous Sanctions Regulations, being weapons, ammunition, military vehicles and equipment or spare parts or accessories, or paramilitary equipment;
- Step 2: If goods are not of a type specified in step one or it is uncertain then the Defence and Strategic Goods List (DSG List) should be reviewed to determine if the goods are of a type in that DSG List;

- Step 3: If the goods are not listed on the DSG List then an inquiry can be submitted through the Pax system.

Where it is not clear whether a particular good falls within the scope of arms or related matériel, a person intending to supply the goods is required to submit an inquiry application through the Pax system.

13.7 Prohibition Relating to “Sanctioned Imports”

Regulation 4A of the Autonomous Sanctions Regulations sets out import prohibitions applying to the import, purchase, or transport of “import sanctioned goods” as set out in the table to the regulation. Whether goods are import sanctioned goods is determined by sub-regulation 4A (2) of the Autonomous Sanctions Regulations.

13.8 Prohibitions in Relation to Providing a “Sanctioned Service”

The prohibition on providing a “sanctioned service” is closely related to the prohibitions on engaging in sanctioned commercial activity and prohibitions on dealing with designated persons and controlled assets. These prohibitions are broad and carry significant risk of inadvertent and/or technical breaches across a range of industries in Australia.

According to Regulation 5 of the Autonomous Sanction Regulations, a “sanctioned service” is the provision to a person of technical advice, assistance or training; financial assistance; a financial service; another service; or if it assists with, or is provided in relation to, a sanctioned supply.

A “financial service” is further defined to include services pertaining to investment, financial advice, brokering, insurance, and reinsurance. In drafting these regulations, terms such as “financial services” and “financial assistance” have been left deliberately broad in the Autonomous Sanctions Regulations so as to capture a range of conduct such as investment brokering, insurance, and trading in securities. Further, terms such as “control,” “directly or indirectly,” “use,” “deal,” and others contained in the Autonomous Sanctions Regulations also broaden the scope of sanctioned activities and have significant implications for compliance management.

Financial assistance and financial services that assists with or are provided in relation to a sanctioned import are also prohibited as a sanctioned service.

Regulation 5 of the Autonomous Sanctions Regulations also set out country-based measures that apply to specific country-based activities. Importantly, a sanctioned service for the purpose of the Autonomous Sanctions Regulations is also the provision to a person of an investment service if it assists with, or is provided in relation to, a sanctioned commercial activity.

13.9 Designated Persons or Entities

Persons or entities can be designated as being subject to Australian sanction measures under the Autonomous Act or the UN Act. All such proscribed persons and entities are listed in the Consolidated List available on the DFAT website.

(a) UN Security Council Designations

Australia has an automatic direct legal obligation to "freeze" assets of parties subject to UN designations. The UN Dealings Regulations[25] implements Australia's obligations under the UN Charter to freeze assets and prevent assets being made available to all persons and entities designated by the UN Security Council as being subject to sanction measures. The UN Dealings Regulations require the Minister to list a person or entity under subsection 15(2) of the UN Act if the Minister is satisfied that the person or entity is mentioned in paragraph 1(c) of UN Security Council Resolution 1373.

Further designations may be made by the Governor General under Section 18 of the UN Act in order to give effect to UN Security Council decisions that relate to terrorism and dealing with assets that Australia is obliged to implement under section 25 of the UN Charter. These designations are made in accordance with subsection 18(3) of the UN Act by the definition of "designated person or entity" in the UN Dealings Regulations incorporating the lists of persons designated in the country-specific sets of UN Regulations. The Minister may also list an asset or class

of assets if satisfied that the asset, or class of assets, is owned or controlled by a designated person or entity.

(b) Autonomous Sanctions Designations

The Autonomous Regulations provide the Minister power to *declare* a person so as to prevent them from entering or remaining in Australia or to *designate* a person or entity. Regulation 6 of the Autonomous Sanctions Regulations authorizes the Minister to designate a person or entity

- if the Minister is satisfied the person or entity is contributing to the proliferation of weapons of mass destruction; or
- for a country listed in the table of Regulation 6 of the Autonomous Regulations

(c) Dealing with a Designated Person or Entity

Australian sanctions laws prohibit any dealing that "directly or indirectly, makes an asset available to, or for the benefit of, a designated person or entity" and the making available of that asset is not authorized by a permit.[26]

As with the UN Act and related regulations, the Autonomous Act and Autonomous Sanctions Regulations also prohibit dealing with assets owned or controlled by designated persons or entities, and prohibit dealings with such persons. The term "freezable asset" under the UN Act takes the concept one step further by prohibiting dealing or use of assets derived or generated from an asset controlled or owned by a designated person or entity.

(d) Identifying Designated Persons and Entities and Controlled Assets

DFAT maintains the Consolidated List of designated persons and entities, including the names, known aliases, and any registration numbers that may assist with identifying the person or entity and the date of designation.

Asset holders and other Australian persons engaging in activity that may be subject to sanction measures can access the Consolidated List of

designated persons and entities under Australian Sanctions Laws on the DFAT website.[27]

There exists some ambiguity under Australian sanctions law as to whether an entity of which one or more major shareholders are designated persons, or which is otherwise controlled by a designated person, but which itself is not on the Consolidated List, should also be subject to the sanction measures made in relation to designated entities.

Whilst Australia's sanctions legislation does not provide a detailed definition around what specifically constitutes effective control of a designated entity, the Corporations Act 2001 offers what may be a helpful definition of effective control, which states in section 910B that "having the capacity to determine the outcome of decisions about the body corporate's financial and operating policies" is sufficient to constitute control of a body corporate. This takes into account the practical influence that can be exerted and any practice or pattern of behavior affecting the body corporate's financial or operating policies.

While the provisions of the Corporations Act 2001 are not directly applicable to Australia's sanctions restrictions, they may be somewhat persuasive in determining what constitutes control of a body corporate under Australian law.

Australian persons can also request DFAT to provide access to software called LinkMatchLite (LML), which is designed to assist in matching input names with names on the Consolidated List. LML is somewhat limited as a compliance tool, as it does not provide indication of relationships between the input name and any name on the Consolidated List. LML does assist in identifying matches where there is slight variation in spelling or other details or aliases.

Asset holders may also request the assistance of the AFP pursuant to Regulations 23 and 24 of the Autonomous Sanctions Regulations to determine whether an asset is controlled or owned by a person or entity on the Consolidated List. To facilitate these requests for assistance, a referral process has been agreed between DFAT, the AFP, and asset holders represented by the Australian Bankers' Association and the major banks.[28]

Under the UN Dealings Regulations and the Autonomous Sanctions Regulations, the AFP is required to use its best endeavors to help a person making such a request. The AFP's response must state whether the AFP considers that it is likely that the asset is owned or controlled by a

designated person or entity, or it is unlikely that the asset is owned or controlled by a designated person or entity, or it is unknown whether the asset is owned or controlled by a designated person or entity. These regulations do not limit the obligations of a reporting entity under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.[29]

13.10 Controlled Assets and Freezable Assets

A "controlled asset" under Regulation 3 of the Autonomous Sanctions Regulations means an asset owned or controlled by a designated person or entity.

A "freezable asset" under the UN Act is an asset owned or controlled by a proscribed person; listed by the Minister under section 15 of the UN Act; or derived or generated from a listed asset or an asset owned or controlled by a proscribed person or entity.

A person contravenes the Autonomous Sanctions Regulations and the UN Act, and commits an offence, if that person holds a controlled asset or a freezable asset and uses or deals with the asset or allows the asset to be used or dealt with, or facilitates the use of the asset or dealing with the asset and that person does not have an authorization or permission to do so under the relevant Australian sanctions laws. These offences are strict liability offences and have extraterritorial effect.

13.11 Engaging in a Sanctioned Commercial Activity

The Autonomous Sanctions Regulations proscribe "sanctioned commercial activities" in relation to specific countries or part of countries in Regulations 5A, 5B, 5C, and 5CA. The prohibitions apply to these activities in relation to parties set out in the tables to those regulations. Australian persons are proscribed from engaging in a sanctioned commercial activity that includes the:

- Acquisition of an interest in a designated entity;
- Extension of an interest in a designated entity;
- Establishment of a joint venture with a designated entity;
- Participation in a joint venture with a designated entity; or
- Granting of a financial loan or credit to a designated entity.

Specific Autonomous Sanctions Regulations are included for commercial activities in relation to specific countries.

Despite these express proscriptions, the Minister also possesses wide powers to suspend sanctions for specified activities, by legislative instrument, if he or she is satisfied that it is in the national interest to do so pursuant to Regulation 5D of the Autonomous Sanctions Regulations. This allows the Autonomous Sanctions Regulations to reflect international standards and adapt to the current attitudes of the international community and UN Security Council.

13.12 Authorizations and Permits

(a) Overview of Permits

Pursuant to Regulation 18 of the Autonomous Sanction Regulations, the Minister may grant a permit in order for a person to do the following, which, in the absence of a permit, contravene an autonomous sanction:

- Make a sanctioned supply;
- Make a sanctioned import;
- Engage in a sanctioned commercial activity;
- Provide a sanctioned service;
- Make an asset available to a designated person or entity; or
- Deal with a controlled asset.

Activities proscribed under the UN Security Council sanctions regimes may also be permitted by the Minister if the UN Regulations for the relevant UN Security Council sanctions regime provide for permissions. UN Regulations for each regime can provide for a permit by incorporating any of the sub-regulations 5(3) to 5(7) of the UN Dealing Regulations.

The Autonomous Sanctions Regulations adopt similar language and administrative processes for permit applications as those in respect of UN Security Council sanctions.

(b) Obtaining a Permit

Generally, a person will apply for a permit through the Pax system, which commenced on October 1, 2020, although the Minister does have authority

to grant a permit at the Minister's initiative. Before granting a permit, the Minister must be satisfied that it would be in the national interest to do so, and also be satisfied of any other matter specified in the UN Regulations or specified in the Autonomous Regulations as applicable to the particular type of permit. It should be noted that queries and applications under the previous system, the Online Sanctions Administration Scheme (**OSAS**), will be finalized under the OSAS.

(c) Permit Conditions

Conditions may also be attached to the permit. Contravention of a permit condition is an offence under the Autonomous Act.[30] A person must retain all records and documents relating to an application for a permit or an authorization under an Australian sanctions law and any records or documents relating to that person's compliance with the permit or authorization conditions, for a period of five years from the last day on which the person acted under the authorization. If upon application the permit or authorization was not granted, a person is nevertheless required to retain records or documents relating to the application for a period of five years from the day on which the application was made.

(d) Permit to Deal with a Controlled Asset, Person, or Entity

Upon application, and the Minister's satisfaction of the relevant criteria, a person may be issued a permit to deal with a designated entity or person or deal with controlled assets, which would otherwise be proscribed by Australian sanctions laws. The types of dealing that can be permitted under the Autonomous Act and Autonomous Regulations are a "basic expense" dealing, a "contractual dealing" or a "legally required dealing." The categories of permits generally correspond with categories contained within country-specific UN Security Council sanctions that impose asset freeze obligations, including Resolution 1373.

(i) Basic Expense Dealing

A dealing is a basic expense dealing if it involves a payment to a designated person or entity; or a payment to a person or entity acting on behalf of, or at the direction of, a designated person or entity; or a payment to an entity

owned or controlled by a designated person or entity; or a use or dealing with a controlled asset; and the dealing is necessary for basic expenses, including any of the following: foodstuffs, rent or mortgage, medicines or medical treatment, taxes, insurance premiums, public utility charges, reasonable professional fees, reimbursement of expenses associated with the provision of legal services, or fees or service charges that are in accordance with a law in force in Australia for the routine holding or maintenance of frozen assets.

(ii) Legally Required Dealing

A dealing is a legally required dealing if it involves a payment to a designated person or entity; or a payment to a person or entity acting on behalf of, or at the direction of, a designated person or entity; or a payment to an entity owned or controlled by a designated person or entity; or a use or dealing with a controlled asset; and the dealing is necessary to satisfy a judicial, administrative, or arbitral lien or judgment that was made prior to the date on which the person or entity became a designated person or entity, provided that the dealing is not for the benefit of a designated person or entity.

(iii) Contractual Dealing or Required Payment Dealing

A dealing is a contractual dealing under the Autonomous Act and a required payment dealing under the UN Act if the dealing is a payment to apply interest or other earnings due on accounts holding controlled assets;[31] or required under contracts, agreements, or obligations made before the date on which those accounts became accounts holding controlled assets. If the account into which the payment is paid is frozen, then the payment will also be frozen once received.

(iv) Extraordinary Expense Dealing

Under the UN Dealing Regulations, further provision is made for a dealing necessary for an extraordinary expense. This type of expense dealing is not provided under the Autonomous Sanctions Regulations.

13.13 General Prohibitions/Restrictions/Requirements

(a) Contravening a Sanctions Measure

Australian sanctions laws establish serious criminal offences for contravening a sanctions measure or a condition of a sanctions permit. Section 16 of the Autonomous Act provides that it is an offence to contravene a sanctions law or the condition of any permit or authorization granted under a sanctions law. This penalty upon conviction for individuals is up to ten years in prison and/or a fine the greater of $555,000 (2,500 penalty units) or three times the value of the transaction. The level of a penalty unit has increased to $275 per penalty unit for offences after 1 January 2023. The offence for a body corporate is punishable upon conviction by a fine of up to the greater of three times the value of the relevant transaction or transactions (if this can be calculated) or $2,2000,000 (10,000 penalty units).

Liability is imposed on a "strict liability" basis. However, a body corporate may rely on the defense that it took reasonable precautions, and exercised due diligence, to avoid contravening the sanction law or authorization concerned. The onus of establishing this defense will rest with the defendant.

These penalties make the consequences for contravening Australia's autonomous sanctions consistent with a contravention of Australian laws implementing UN Security Council sanctions.

According to the Explanatory Memorandum[32] for the Autonomous Bill, the origin of the strict liability offence for bodies corporate in the UN Act is Recommendation 2 of the report, dated November 24, 2006, of the Inquiry into certain Australian companies in relation to the UN Oil-for-Food Program conducted by Commissioner the Honourable Terence R.H. Cole AO RFD QC (the Cole Inquiry[33]). Following a recommendation of Commissioner Cole, the UN Act introduced strict liability criminal offences with severe penalties in order to ensure a sufficient deterrence effect for bodies corporate. It is intended that the "reasonable precaution" defense provides a balance for the severe penalty and strict liability offence provisions for bodies corporate. The added anticipated benefit of providing this defense was that it encourages a culture of compliance monitoring and risk management.

(b) Giving False or Misleading Information

Australian sanctions laws establish serious criminal offences for giving false or misleading information to a Commonwealth entity in connection with the administration of an autonomous sanction law (section 17 of the Autonomous Act) or a UN sanction enforcement law (section 28 of the UN Act).

Section 19 of the Autonomous Act and section 30 of the UN Act provide that the CEO of a designated Commonwealth entity (as defined in section 4 of the act) may give a person a written notice requiring information or documents to be provided for the purpose of determining whether a sanction law has been or is being complied with. If a person fails to comply with such a notice under either act, a person commits an offence punishable by 12 months' imprisonment.

Generally a person is likely to provide information to a Commonwealth entity if (1) that person holds an asset that is, or it is suspected to be, a controlled asset, or (2) in connection with an application for a permit or an authorization under Autonomous Sanctions Regulation 18, or (3) in response to a notice to provide information given by the CEO of a designated Commonwealth entity for the purpose of determining whether a sanctions law has been or is being complied with. In practice, self-reporting of noncompliance or potential noncompliance is a fourth circumstance in which information might be provided to the Commonwealth.

Subsection 17(1) of the Autonomous Act creates an offence for providing information that is false or misleading to a Commonwealth entity. Subsection 17(2) of the Autonomous Act creates an offence of providing false or misleading information to another person where the first person is reckless as to whether the second person will provide that information to a Commonwealth entity. In respect of both offences, the information or document must be misleading in a material particular.

Parliament has deliberately drafted these offences to be broad, choosing the term "in connection with" to capture a much broader scope of activity than would have been captured by a narrower requirement of direct relevance to the administration of a sanctions law. Similarly, the offence for recklessly providing information that may be false or misleading was intentionally drafted to criminalize a wider scope of activity than would have been captured by the term "knowingly." The Foreign Affairs, Defence and Trade Legislation Committee (Committee) considering these provisions were concerned that the offence provisions should provide adequate

incentive for persons to provide information and documents to the Commonwealth in order to monitor compliance and ensure that unjustifiable risk is not taken as to whether the information was false or misleading.

Both offences under section 17 of the Autonomous Act are punishable by up to ten years in prison and/or a fine of 2,500 penalty units ($555,000 as of July 1, 2020) and have extraterritorial application. This means that a person can commit an offence from outside of Australia.

(c) Effect of False or Misleading Information in a Permit Application

Significantly, under section 15 of the Autonomous Act, an authorization granted under the Autonomous Sanctions Regulations, including a permit, license, permission, consent, or approval is taken never to have been granted if information contained in or accompanying the application for the authorization was false or misleading in a material particular or omits any matter which the information or document provided is misleading in a material particular.

Consequently, if false or misleading information is provided in an application for a permit, a person relying on that permit is liable for an offence of providing false information under section 17 of the Autonomous Act and will have committed an offence in carrying out the activity for which the permit was sought.

Section 15 of the Autonomous Act reflects the offences created under section 28 of the UN Act in relation to providing false or misleading information in relation to the administration of UN sanctions enforcement laws.

(d) Noncompliance with a Notice to Give Information or Documents

DFAT or the CEO of a designated Commonwealth entity may issue a notice requiring a person to give information or documents, including under oath, for the purpose of determining whether a sanction law has been or is being complied with. The person must comply with the notice despite any other law of the Commonwealth, a state, or a territory. The person is not excused

from complying on the ground that the information or documents might tend to incriminate him or her. Failure to comply is an offence punishable by 12 months in prison.

13.14 Penalties, Enforcement

(a) Enforcement and Investigations

Enforcement and investigations powers are partly provided in the legislation and partly through arrangements between the relevant regulatory bodies. Enforcement mechanisms rely on persons and entities undertaking effective compliance programs and reporting on activity to DFAT and other financial regulators. The power to require information or documents to be given to a designated Commonwealth entity[34] is also a powerful investigation and enforcement tool, as it overrides any obligation under any other law of the Commonwealth, states, or territories.

Part 2, Division 2 of the Autonomous Act creates mechanisms for the enforcement of sanctions. These mechanisms are:

- Injunctions to restrain persons or entities from a contravention, or apprehended contraventions, of sanctions under section 14 of the Autonomous Act, and
- The invalidation of authorizations (such as licences, permissions, consents, or approvals granted to persons or entities to engage in conduct or activities that would otherwise be prohibited by sanctions), where such authorizations are obtained through the provision of materially false or misleading information, under section 15 of the Autonomous Act.

Sections 14 and 15 of the Autonomous Act apply in respect of matters arising pursuant to regulations made under section 10 of the Autonomous Act and are not expressed to apply to the broader scope of “sanctions laws” specified in an instrument made in accordance with section 6(1) of the Autonomous Act.

Accordingly, offences against “sanctions laws” are generally dealt with under sections 16 and 17 of the Autonomous Act. However, the enforcement mechanisms available in respect of contraventions are determined by the provisions of the relevant sanctions law itself.

13.15 Defenses

(a) Reasonable Precaution Defense for Corporations

It is a defense for a body corporate if it proves that it took reasonable precautions, and exercised due diligence, to avoid contravening a sanctions measure or a condition of a sanctions permit.

What constitutes "reasonable precautions" and "due diligence" depends on the circumstances. A body corporate would have to demonstrate that it thoroughly considered sanctions issues before undertaking an activity. As a first precautionary step, it is advisable to immediately inform DFAT of any changes to an activity that may raise sanctions issues.

(b) Preserving Value—Dealing with a Freezable Asset

Under section 20 of the UN Act it is a defense to a charge of dealing with a freezable asset if the individual or corporation proves that the dealing was solely for the purpose of preserving the value of the asset. The defendant bears the legal burden of establishing the elements of this defense in accordance with section 13.4 of the Criminal Code.

13.16 Key Websites

- The Consolidated List is a list of all persons and entities who are subject to targeted financial sanctions or travel bans under Australian sanctions laws: https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list.
- Details of the new Pax system to secure permits and make inquiries can be found at https://pax.dfat.gov.au/sncPortal/s/.
- Details about the sanctions regimes currently implemented under Australian laws are found at https://www.dfat.gov.au/international-relations/security/sanctions.
- Department of Foreign Affairs and Trade—"who we are"—found at https://www.dfat.gov.au/international-relations/security/sanctions/who-we-are.

---

1. The author, a partner at Rigby Cooke Lawyers, Melbourne, Australia, (https://www.rigbycooke.com.au/) and would like to thank his colleague Alexander Uskhopov, who

provided the vital sanity check (and improvement) on the update to this chapter.

2. Part VI of the Australian Customs Act 1901, https://www.legislation.gov.au/Details/C2017C00219.

3. Customs (Prohibited Exports) Regulations 1958, https://www.legislation.gov.au/Details/F2021C00313. For a useful summary of the prohibited goods, see https://www.abf.gov.au/importing-exporting-and-manufacturing/prohibited-goods/list-of-items (last updated Apr. 14, 2022).

4. Export Control Act 2020, https://www.legislation.gov.au/Details/C2020C00192.

5. Australian Gov't Dep't of Agriculture, Fisheries and Forestry, *Export Goods Controlled by the Department*, https://www.agriculture.gov.au/biosecurity-trade/export/controlled-goods (last updated Dec. 1, 2020).

6. For details on Defence Export Control legislation, see Australian Gov't Defence, *Legislation, Regimes and Agreements*, https://www.defence.gov.au/business-industry/export/controls/export-controls/legislation-regimes-agreements (last visited Dec. 19, 2022).

7. Defence Trade Controls Act 2012, https://www.legislation.gov.au/Details/C2012A00153.

8. Weapons of Mass Destruction (Prevention of Proliferation) Act 1995, https://www.legislation.gov.au/Details/C2016C01072.

9. For a summary of each piece of legislation, see Australian Gov't Defence, *Defence Export Controls*, https://www.defence.gov.au/business-industry/export/controls (last visited Dec. 19, 2022).

10. https://www.abf.gov.au/help-and-support-subsite/CustomsNotices/2022-21.pdf.

11. https://www.abf.gov.au/help-and-support-subsite/CustomsNotices/2022-32.pdf.

12. For more comprehensive details on the range of sanctions and other controls, see Australian Gov't Dep't of Foreign Affairs & Trade, *Russia Sanctions Regime: Why Are Sanctions Imposed?*, https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/russia-sanctions-regime (last visited Dec. 19, 2022).

13. Autonomous Sanctions Bill 2010, Second Reading Speech, House of Representatives Hansard, at 4113 (May 26, 2010), https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2F2010-05-26%2F0022%22.

14. Response of the Minister for Foreign Affairs, quoted in Parliamentary Joint Committee on Human Rights, Human Rights Scrutiny Report, 28th report of the 44th Parliament, at 19 (Sept. 17, 2015), https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2015/Twenty-eighth_Report_of_the_44th_Parliament.

15. Charter of the United Nations Act 1945 (UN Act), https://www.legislation.gov.au/Details/C2016C00742.

16. Autonomous Sanctions Act 2011 (Cth), https://www.legislation.gov.au/Details/C2016C00247.

17. Autonomous Sanctions Regulations 2011, https://www.legislation.gov.au/Details/F2011L02673/.

18. Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021, https://www.legislation.gov.au/Details/F2021L01855.

19. https://www.legislation.gov.au/Details/C2016C01072.

20. Autonomous Sanctions (Sanction Law) Declaration 2012 (Cth), https://www.legislation.gov.au/Details/F2012C00629

21. Regulations 11, 11A, 11B and 11E of the Customs (Prohibited Exports) Regulations 1958 (Cth), *supra* note 3.

22. https://www.dfat.gov.au/international-relations/security/sanctions/Pages/about-sanctions.

23. Sub-regulation 4(2) of the Autonomous Sanctions Regulations, https://www.legislation.gov.au/Details/F2011L02673/.

24. More details of the “Pax” system are set out later in the chapter, and may also be found on the ASO website, https://pax.dfat.gov.au/sncPortal/s/.

25. Charter of the United Nations (Dealing with Assets) Regulations 2008, http://classic.austlii.edu.au/au/legis/cth/num_reg_es/cotunwar2008n29o2008658.html.

26. *Id*. r 14(1).

27. https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list.

28. The relevant form is available at https://www.afp.gov.au/contact-us/forms and should be sent to the AFP at the AFP Operations Coordination Centre on AOCC-Client-Liaison@afp.gov.au.

29. Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

30. The Autonomous Act, Part 3, Section 16, https://www.legislation.gov.au/Details/C2016C00247.

31. Under the Autonomous Regulations only. This is not provided for specifically under the UN Dealing Regulations.

32. According to the Explanatory Memorandum, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4432.

33. Cole Inquiry, https://apo.org.au/node/3765.

34. Section 19 of the Autonomous Act and section 30 of the UN Act.

14

Export Controls and Economic Sanctions in Brazil

Vera Kanas Grytz[1]

14.1 Overview

What Is Regulated: The Brazilian export controls system controls the exportation of certain goods and services. It does not impose controls for exports to named persons and institutions.

Some products are subject to stricter controls in their exportation due to characteristics that make them "sensitive goods." Law 9112, of October 10, 1995, defines sensitive goods as dual-use goods and goods of use in the nuclear, chemical, and biological areas.

Dual-use goods are goods of general application that may be relevant for war applications. Goods of use in the nuclear area are those that contain elements of interest to the development of nuclear energy, as well as installations and equipment used for its development or for the several peaceful applications of nuclear energy. The list of nuclear use goods is based in the guidelines of the Nuclear Supplier Group (NSG), of which Brazil is a member.

Chemical and biological goods are those relevant for any war application and their precursors. The lists of chemical and biological goods are based in the guidelines of the Convention on Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction; on the Convention on Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological)

and Toxin Weapons and on Their Destruction; and on the Missile Technology Control Regime (MTCR), of which Brazil is a member.

Directly linked services are also subject to export controls related to sensitive goods. The operations that provide specific information or technology necessary to the development, production, or use of the referred product, including in the form of technical data or technical assistance, are considered as services directly linked to a product.

Furthermore, defense products are subject to the National Policy on Export and Import of Defense Products and may be subject to controls by the Ministry of Defense. Defense products include goods, services, work, or information, including arms, ammunition, means of transport and communication, military clothing and materials of individual and collective use for defense activities.

Brazil also applies special controls for several products for security, health, environment, and other public policy reasons. A prior consent to export these products is required.

Brazil imposes restrictions or embargoes on exports for some countries strictly based on the decisions agreed in the scope of the United Nations and other international organizations. Brazil does not unilaterally impose embargoes or economic boycotts and sanctions.

Finally, a few products are subject to export tariffs of up to 150 percent. These products include cigarettes and arms and ammunition. These tariffs for cigarettes and arms and ammunition apply only to exports to South and Central America and the Caribbean.

Where to Find the Regulations: The most important regulations regarding export controls are the following:

- Law no. 9112, of October 10, 1995, which defines sensitive goods and related services and imposes the procedures for exporting such goods
- Decree 9.607, of December 12, 2018, which establishes the National Policy for Export and Import of Defense Products
- Ordinance of the Secretary for Foreign Trade no. 23, of July 14, 2011, which establishes the export requirements to export operations as well as the list of embargoed countries

Regulations are also imposed by each governmental body or agency responsible for controlling sensible goods to be exported.

Who Is the Regulator: The Inter-Ministerial Commission of Export Controls of Sensitive Goods is responsible for drafting regulations, criteria, procedures, and mechanisms related to the export controls of sensitive goods and directly related services. The Commission is also responsible for preparing the list of sensitive goods. It is coordinated by the Ministry of Science, Technology and Innovation and also composed by the Ministry of Defense, the Ministry of Economy, the Ministry of Justice, and the Ministry of Foreign Affairs.

The Ministry of Defense is responsible for defining the defense products that are subject to control and for granting export licenses for defense products. The Ministry of Foreign Affairs is responsible for authorizing the request for preliminary negotiations for the export of defense products and coordinate actions with the UN Security Council.

The Secretary of Foreign Trade of the Ministry of Economy (SECEX) is responsible for administering export operations.

Governmental bodies and agencies may also impose regulations for exports of specific products. The entities that may be required to grant authorization for export of specific products are the National Agency of Electric Energy (ANEEL); National Oil Agency (ANP); National Agency of Sanitary Vigilance (ANVISA); National Commission of Nuclear Energy (CNEN); Army, Subsecretary of Foreign Trade Operations (SUCEX of SECEX); National Department of Mineral Production (DNPM); Federal Police, Brazilian Institute for Environment and Renewable Natural Resources (IBAMA); Ministry of Science, Technology and Innovation (MCTI); and Ministry of Defense.

How to Obtain an Export License: Controlled products require a license prior to exportation. In Brazil, the government's websites do not disclose a consolidated list of sensitive goods and defense products, but only general information about the matter. The lists are only available at the respective ordinances and resolutions mentioned in Section 14.2(c) However, the exporter may verify if a product is subject to export control (for example, because it is considered a sensitive good or defense product) by checking the administrative controls applicable to the respective tariff classification of the product (Mercosur Common Nomenclature (NCM), an eight-digit code based on the Harmonized System) at the Single Window for Foreign Trade System. In this system, there is a tool that allows one to simulate an

operation so as to check the applicable controls—it is the last link in the Key Website list that follows.

If the product is subject to control, the exporter should request the license (LPCO) through the Single Window for Foreign Trade System, submitting the required documents and information, and the competent agency or governmental body shall approve the license. The documents and information required for obtaining such licenses vary according to each regulatory body, and the authorization of more than one entity may be required.

Exports of sensitive goods, including dual use goods, are subject to the approval by the MCTI. Export of defense products are subject to the approval of the Ministry of Defense. Please refer to Section 14.7 for further information on these licenses.

Key Websites:

- Information on sensitive goods: https://www.mctic.gov.br/mctic/opencms/institucional/bens_sensiveis/index.html
- National Policy on the Import and Export of Defense Products: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9607.htm
- SECEX—Ordinance no. 23 of July 14, 2011: http://www.siscomex.gov.br/legislacao/secex/
- Information about the controlled products (based on the respective tariff classification): https://portalunico.siscomex.gov.br/talpco/#/simular-ta?perfil=publico

14.2 Structure of the Laws and Regulations

(a) International Treaties

Brazil participates in a series of international treaties related to export controls of sensitive goods. Notably, Brazil participates in the following treaties:

- The Convention on Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (1993)
- The Convention on Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (1972)
- The Nuclear Suppliers Group (NSG)
- The Missile Technology Control Regime (MTCR)

Brazil is not a member of the Wassenaar Arrangement or Australia Group.

(b) Brazil National Laws and Regulations on Export Controls

The overall structure of the Brazilian export controls system is composed of laws and regulations from different governmental bodies, as follows.

Export controls of sensitive products are regulated by Law no. 9112, of October 10, 1995. This law defines sensitive products, including dual use goods, and related services and creates the Inter-Ministerial Commission for the Export Control of Sensitive Goods. Exporters of sensitive goods must comply with requirements based on international conventions and regimes related to chemical, biological, nuclear, and missile technologies. The list of sensitive goods can be found at the respective regulations mentioned in Section 14.2(c).

Decree 9607, of December 12, 2018, establishes the National Policy of Exportation and Importation of Defense Products. Products included in the list of defense products are subject to control upon exportation by the Ministry of Defense. The list of defense products can be found in Ordinance of the Secretary of Defense Products of the Ministry of Defense no. 1714, of April 27, 2020.

Other agencies and governmental bodies responsible for granting export licenses to controlled products, due to health, environment, security, and other public reasons also have their own regulations applicable upon exportation of these products.

(c) Controlled List

Sensitive goods, including dual use goods, and related services are listed in the following documents:

- Controlled List of the Chemical Area: updated by Ordinance of the Ministry of Science and Technology no. 437, of June 14, 2012 (https://www.mctic.gov.br/mctic/export/sites/institucional/legislacao/Arquivos/Anexo_Port_MCTI_437_2012-Bens-Sensiveis.pdf)
- Controlled List of the Nuclear Area: Ordinance of the Ministry of Science, Technology and Innovation no. 1405/2014, of December 29, 2014, disclosing Resolution of the Interministerial Commission of Control on the Exports of Sensitive Goods no. 23, of November 18, 2014 (https://www.mctic.gov.br/mctic/export/sites/institucional/legislacao/Arquivos/Anexos_Port_MCTI_1405_2014-Bens-Sensiveis.pdf)
- Controlled List of the Biological Area: updated by Resolution Interministerial Commission of Control on the Exports of Sensitive Goods no. 13 of March 10, 2010 (https://www.mctic.gov.br/mctic/export/sites/institucional/arquivos/legislacao/209072.pdf)
- Controlled List of the Missiles Area: Ordinance of the Ministry of Science, Technology and Innovation no. 181, of March 4, 2016 (https://www.mctic.gov.br/mctic/export/sites/institucional/arquivos/legislacao/238861.pdf)
- Ordinance of the Secretary of Defense Products of the Ministry of Defense no. 1714, of April 27, 2020, establishes the List of Defense Products (http://www.in.gov.br/web/dou/-/portaria-n-1714/seprod/sg-md-de-27-de-abril-de-2020-254213468)

Finally, information about other products subject to export licenses by other agencies and governmental bodies can be found at the Single Window for Foreign Trade, based on the tariff classification of the product.

(d) Brazil and UN Security Council Sanctions

Please refer to Section 14.2(f) for further information.

(e) Brazil National Laws on Economic Sanctions

Brazil strictly follows the sanctions imposed by the Security Council of the United Nations, based on Law 13810/2019, which regulates freezing of assets owned by individuals, companies and entities, as well as the national

designation of individuals that are investigated or accused of terrorism or of financing terrorist acts. The country does not unilaterally impose sanctions.

Please refer to item (f) following for further information.

(f) Brazil Sanctioned Parties Lists

Ordinance of the Secretary for Foreign Trade no. 23 of July 14, 2011 (as amended) establishes, in article 254, the prohibition of exports of determined products to the following countries ("Countries with peculiarities"), in accordance with UN Security Council Resolutions:

- Iraq
- Somalia
- Sierra Leone
- North Korea
- Democratic Republic of Congo
- Sudan
- Eritrea
- Libya

Generally speaking, the following products cannot be exported to sanctioned countries: arms, ammunition, military equipment, and vehicles. Some countries are subject to restrictions on broader or narrower list of products.

Brazil does not impose sanctions on named persons or institutions.

14.3 What Is Regulated: Scope of the Regulations

Brazilian export controls system is focused on the types of goods to be exported.

Law 9112, of October 10, 1995, imposes controls related to sensitive goods and related services, which comprise:

- Sensitive goods: goods that can be used in the production of weapons; dual-use goods; and goods used in the nuclear, chemical, or biological areas;
- Dual-use goods: products that can be used for purposes of war, even if they have been developed for civil applications; and

- Services related to sensitive goods: services related to the supply of information or technology for the development of sensitive goods.

These sensitive goods and services are directly linked and classified as to their nature in four major areas: nuclear, chemical, biological, and projectile, according to the specific treatment internationally provided. Export of these products are not forbidden but they are subject to prior approval by the Ministry of Science, Technology and Innovation. Please refer to Sections 14.7(a) and 14.7(b) for further information on how to obtain such licenses.

Decree 9.607, of December 12, 2018, imposed controls on the exportation of defense products. Defense products are defined as goods, services, work, or information, including arms, ammunition, means of transport and communication, military clothing and materials of individual and collective use for defense activities, excluding administrative activities.

Export of listed defense products shall be subject to prior approval upon exportation by the Ministry of Defense. Please refer to Section 14.7(c) for further information on how to obtain such a license.

Many goods are subject to other kinds of control, imposed mainly for safety, health, security, or environment reasons. Products subject to control are usually chemicals, pharmaceuticals, wood products, some vehicles and aircraft, mineral fuels, fish and crustaceans, raw hides and skins, arms and ammunitions, and live animals.

Each competent agency or governmental body has its own procedures and requirements for the granting of authorization for the export of controlled products and more than one agency may need to approve the export of a specific product. These requirements may be based on international conventions or on national policies.

Finally, Brazil imposes sanctions to “countries with peculiarities,” based on the sanctions imposed by the UN Security Council. Export to these countries of some products (usually, military goods) is forbidden.

14.4 Who Is Regulated

All Brazilian companies and individuals domiciled or with residency in the country and exporting from Brazil are subject to compliance with export controls and economic sanctions.

Please note that, under the Brazilian customs laws, only Brazilian entities may perform customs clearance for exportation.

Brazilian regulations do not apply to importers in third countries, or any other agent outside Brazil. Brazilian regulations also do not apply to Brazilian goods once they have been exported to a third country.

14.5 Classification

(a) Classification of Dual-Use Items

Dual-use goods are products that can be used for purposes of war, even if they have been developed for civil applications. These goods are considered sensitive goods and are included in the respective lists of sensitive goods of the chemical, biological, nuclear, and missiles areas. See https://www.mctic.gov.br/mctic/opencms/institucional/bens_sensiveis/index.html.

(b) Classification of Military Items

Military items are mainly included in the list of defense products. Please note that control by other authorities may also apply depending on the product.

14.6 General Prohibitions/Restrictions/Requirements

Exports of some products can be prohibited due to protection of fauna and flora and other environmental concerns. Exports of specific chemicals are prohibited for non-signatories of the Montreal Protocol on Substances that Deplete the Ozone Layer and exports of wood in the rough are restricted and require prior approval by the Institute for Environment and Renewable Natural Resources (IBAMA). Exports of arms, ammunition, and other weapons and military equipment are prohibited when destined to countries subject to economic sanctions by the United Nations. Brazil also participates in the Kimberly Certification Programme and, thus, exports of raw diamonds require a Kimberley certificate.

For permitted products, the first step for a Brazilian company to export is to enroll with the RFB, in order to obtain a “permit to perform export

activities," known as RADAR. RFB enrollment provides access to the Single Window for Foreign Trade, which is the system that must be used for all import and export transactions in Brazil.

Some goods are subject to specific controls, and before submitting the single export declaration to the Single Window of Foreign Trade, the exporter must verify if it is necessary to request any prior export license consent of exportation to a specific governmental body or agency. This check is based on the tariff classification of the good to be exported. More than one authority may be competent to approve a determined export operation.

In addition to the specific controls imposed to some products, which require a prior approval to exportation, Brazil also imposes export restrictions or embargoes to some countries based on economic sanctions approved by the United Nations and other international organizations. The exporter must check if any of the exports are destined to one of the embargoed countries, in order to verify if the exportation is not forbidden.

14.7 Licensing/Reasons for Control

(a) Types of Export Control Licenses and Permits for Dual-Use Items

Products classified as sensitive goods, including dual-use items, are subject to export license by the Ministry of Science, Technology and Innovation.

(b) Export Control Licensing Procedure

In order to obtain the export license applicable to sensitive goods, the exporter must fulfill the requirements established in the regulations on sensitive goods. Generally speaking, the exporter must first request the Ministry of Foreign Affairs for an authorization to export. At this request, the exporter must present information about the preliminary negotiation, end-user certificate, and guarantee from government (when required). The authorities may request additional documents, such as contracts and other information about the transaction.

After the analysis by the Ministry of Foreign Affairs, the request will be sent to the Ministry of Science, Technology and Innovation, which is

responsible for granting the prior approval for exportation. The exporter must request prior approval for exportation by the Ministry of Science, Technology and Innovation at the Single Window for Foreign Trade system. After receiving the proper authorization for exportation at the Single Window for Foreign Trade, the company must follow general exportation procedures, through the Single Window for Foreign Trade System.

Please note that specific requirements may apply for each category of sensitive goods (missiles, chemical, biological, and nuclear).

(c) Import and Export License for Military Items

Defense products are subject to the National Policy on the Import and Export of Defense Products. Controlled defense products are divided in two levels. For Level 2 products, the procedure for exporting is based on two steps: preliminary procedure and exporting procedure. Level 1 products are free from adopting the preliminary procedure.

The preliminary procedure requires that the exporter request authorization to proceed with preliminary negotiations to export the product. After negotiations are concluded, the exporter must register the request to export, which shall be approved by the Ministry of Foreign Affairs and Ministry of Defense. The request for export is valid for two years and may be extended until the limit established for the execution of the negotiated agreement.

The exporting procedure requires the exporter to request, upon each export operation, an export license at the Single Window for Foreign Trade system, which shall be granted by the Ministry of Defense before products are cleared for exportation.

(d) Export Permits and Independent Expert Examination

Prior approval upon exportation may be required by several agencies and governmental bodies depending on what items are being exported:

- The National Agency for Sanitary Vigilance. ANVISA is responsible for controlling export of drugs and psychotropic and immunosuppressant substances.
- Institute for Environment and Renewable Natural Resources. IBAMA controls exports of biodiversity products such as some biological

materials, species of live animals, plants, fungus, and virus. IBAMA also controls exports of hazardous waste, regulated by the Basel Convention, and several other biological and chemical materials, such as agrochemicals and chemical spreaders.
- The National Agency for Oil controls the export of petroleum products.
- The Federal Police controls products that may be used in the illicit production of drugs.
- The Ministries of Foreign Affairs and of Defense control exports of military material.
- The Interministerial Commission for the Export Control of Sensitive Goods controls exports of sensitive goods and related services.
- The Subsecretary of Foreign Trade Operations controls exports subject to tariff quotas in the country of destination, drawback operations, and transactions of used material.
- The National Commission of Nuclear Energy controls exports of radioactive material.

These prior approvals must be requested through the Single Window for Foreign Trade System, according with the requirements imposed by each agency or body.

14.8 General Licenses/License Exceptions

(a) General Licenses

Companies engaged in international trade operations must be enrolled with the RADAR. Controlled products are subject to an export license before exportation, to be requested at the Single Window for Foreign Trade System and to be granted by the competent body, depending on the product to be exported.

Timeframes and procedures for obtaining such a license vary significantly, depending on the agency or governmental body. In several cases, such as military items, preliminary procedures are required. These preliminary procedures may include registration of the company at the respective agency or obtaining a general certification from the agency.

(b) License Exceptions

Goods that are not controlled for exportation may be exported by exporters holding a RADAR, upon registration of the single export declaration at the Single Window of Foreign Trade.

14.9 Penalties, Enforcement, and Voluntary Disclosures

(a) Administrative Penalties

Companies and their employees in every operation must comply fully with Brazilian export and customs controls. Violation of the controls related to sensitive goods may subject companies to the following penalties:

- A warning letter, in case of minor breach;
- Fines, corresponding to up to twice the value of the export;
- Forfeiture of the goods;
- Suspension of the right to export, from six months up to five years; and
- Permanent prohibition to perform foreign trade operations.

The penalties may be applied cumulatively, depending on the seriousness of the violation and the background of the operation in an administrative proceeding for such purpose. Responsibility for violation does not depend on intent or on the nature and extent of the effects of the violation.

Besides the preceding penalties, other customs penalties may apply for the violation of export controls. Penalties include fines of 20 percent to 50 percent of the customs value of the good, for exportation or attempt to export forbidden products and forfeiture of the goods, and 100 percent of the customs value of the goods if already consumed or exported in case of use of false documents, clandestine exportation, or in case of fraudulent interposition of third parties in the operation. Furthermore, other administrative penalties may be applied by agencies or governmental bodies responsible for the control of the product at issue.

(b) Criminal Penalties

From a criminal standpoint, there is no corporate criminal liability in Brazil, with the exception of environmental crimes. Nevertheless, individuals that directly or indirectly, by act or omission, conspire to violate the controls on sensitive goods may be exposed for criminal liability to one to four years of prison. Furthermore, persons involved in illicit export activities may be prosecuted for other crimes, such as smuggling and fraudulent misrepresentation.

(c) Enforcement

Export controls are enforced at customs clearance for exportation of the goods. As said earlier, controlled goods are subject to prior export license by the competent authorities. Upon customs clearance of the goods, customs authorities may conduct a documentary and physical inspection of the goods, in order to ensure that the exported goods are complying with Brazilian laws.

(d) Voluntary Disclosure

There is no specific provision authorizing voluntary disclosures for export control violations in Brazil.

(e) Recent Export Enforcement Matters

Although Brazilian regulations on export controls are not as complex as other countries, such as the United States, the Brazilian Internal Revenue Services (*Receita Federal do Brasil—RFB*) and other bodies are enhancing surveillance and enforcing the legislation more strictly. Notably, in 2018, the federal government enacted Decree 9607, instituting the National Policy on the Import and Export of Defense Products, updating old defense policies.

Brazil is also strengthening collaboration with other countries, especially in the fields of anti-corruption and implementation of multilateral agreements. This cooperation includes exchange of information and sharing of tax and customs information in order to facilitate investigations in the cooperating countries.

14.10 Special Topics

(a) Re-exports/Extraterritorial Application of Laws

Brazilian export control laws do not have extraterritorial effects. Brazilian products exported to third countries and re-exported to another country are not subject to Brazilian export controls legislation.

(b) Intangible Transfer of Technical Information

Export controls on sensitive goods apply to exportation of services directly linked to certain goods. These services include the supply of specific or technological information necessary to the development, production, or use of such goods, including the supply of technical data or technical assistance. Therefore, supply of such information is subject to the same controls required for the export of sensitive goods and must be approved by the competent authorities.

Export controls on defense products apply to services, work, or information to be employed in defense activities. Therefore, transfer of information related to defense activities must comply with the procedures established on the National Policy for the Import and Export of Defense Products.

(c) Practical Issues Related to Export Control Clearance

In accordance with Brazilian customs regulations, to export a product, the company must present the following documents:

- A commercial invoice issued by the Brazilian exporter, presenting the information regarding the identification of the product, its price, and terms of negotiation.
- The packing list, containing information about the goods to be exported, including net weight, gross weight, the packaging setting, value per unit, volume and specific contents. Requirements of the importing country must be checked with the importer of the products.
- A bill of sale (*nota fiscal*) must be issued. The goods must be accompanied by the bill of sale throughout the operation, from the exit of the exporter’s facility to the actual exportation customs clearance.

- The transporter hired by the parties must then issue a bill of lading, a document that will specify the type, quantity, and destination of the goods and attest to their shipment to the place of destination (as indicated in the commercial invoice).

Export control customs clearance is performed through the Single Window for Foreign Trade System. To have access to such system, the exporter must be enrolled in RADAR, which is the authorization to perform import and export activities in Brazil.

In the following, the exporter must check if there is any administrative control for the exportation of the product at issue, based on the tariff classification of the product. If there is any control, the exporter must require an export license (LPCO) at the system and submit the required information. The competent authorities will analyze the request and approve the license at the system.

The LPCO must also be linked to the Single Export Declaration, which must be registered at the same system and which will effectively initiate the customs clearance procedure.

(d) Recordkeeping

Brazilian customs laws require that documents related to the exportation of a product be maintained for a period of five years. Laws on sensitive goods and the National Policy for Import and Export of Defense Products do not establish requirements for recordkeeping.

(e) How to Be Compliant When Exporting to Brazil

Entities exporting to Brazil are not subject to the application of Brazilian Customs and Export Control laws. The Brazilian importer, nonetheless, must verify the controls applicable upon importation of the product at issue and may require the exporter to supply relevant documents such as certificate of origin and other authorizations and permits to be issued by the authorities from the exporting country.

Importation of Defense Products is subject to the National Policy of Import and Export of Defense Products and must follow the procedures established therein, including the import license to be granted by the Ministry of Defense.

Several other goods are subject to an import license, to be granted by the Ministry of Defense; the Army; the Federal Police; the National Agency for Sanitary Vigilance (ANVISA); the Institute for Environment and Renewable Natural Resources (IBAMA); the National Commission of Nuclear Energy; the Ministry of Science, Technology and Innovation; the national Institute of Metrology, Quality and Technology, amongst others.

(f) How to Be Compliant When Exporting from Brazil

The exporter must check if there is any administrative control for the exportation of the product at issue, based on the tariff classification of the product. If there is any control, the exporter must verify the requirements for obtaining the export license established by the competent authority and request the LPCO at the Single Window for Foreign Trade System.

Please refer to Sections 14.7(b) and 14.7(c) for the procedures for obtaining export license for sensitive goods and defense products. Please refer to Section 14.3 on the general proceeding for exporting in Brazil.

14.11 Encryption Controls

(a) General Comments

Brazil does not have any specific regulations regarding controls upon importation or exportation of encryption. Encryption products may be subject to controls applicable to sensitive goods or defense products, if the respective products are included in the lists of sensitive goods or defense products. Authorization from other agencies and governmental bodies may be required, depending on the product to be exported. If the specific product containing encryption is not included in the aforementioned lists nor is it subject to control by other agencies, the product may be exported without any prior approval by the authorities.

(b) Import Encryption Clearance Requirements

As said earlier, there are no specific requirements for importing encrypted products. Some encryption products may be subject to import controls by agencies of government authorities due to the characteristics of the product

to be imported. The importer must check if there is any control, based on the tariff classification of the product.

(c) Encryption Licensing Requirements

Import and export licenses in Brazil are based on the products. There are no general requirements based on the use of encryption. In this sense, in order to import or export an encrypted product, the Brazilian importer or exporter must check if there are any controls applicable to the product, based on the relevant tariff classification, and request the applicable license through the Single Window for Foreign Trade System.

(d) Penalties for Violation of Encryption Regulations

Not applicable.

14.12 Blocking Laws/Penalties for Compliance with Sanctions Imposed by Other Countries

Brazil applies sanctions strictly in compliance with the decisions of the UN Security Council. Brazil does not unilaterally impose sanctions and does not have any rules regarding compliance with sanctions imposed by other countries.

1. Vera Kanas Grytz is partner and head of the International Trade Practice at TozziniFreire Advogados.

15

Export Controls and Economic Sanctions in China[1]

David Tang, Jessica Cai, Roy Liu, and Rain Wang

15.1 Overview

(i) Export Control

What Is Regulated: The framework for Chinese export controls was established in 2002 and underwent a major revision in 2020 with the enactment of the Export Control Law (ECL), which came into effect on December 1, 2020. The main goals of Chinese export controls are nonproliferation of weapons, in particular weapons of massive destruction, anti-terrorism, and protection of national security. Besides the ECL, the Foreign Trade Law provides a general legal basis for the current Chinese export control regime. Article 16 of the Foreign Trade Law provides that the state may restrict or prohibit the import or export of goods or technologies for various purposes, such as national security, public interests, short supply, and protection of natural resources.

The old export controls legal framework consisted of various regulations and rules with a lower level of authority in terms of legislation, and enforcement was weak, partially due to lack of sufficient legislative authorization. Aiming to bring the legal framework to a higher level of legislative authority and empower the authorities with more enforcement power, after several rounds of deliberation, beginning in 2017, the Standing Committee of the National People's Congress passed the new Export Control Law in October 2020. The new law streamlines controls over dual-use items, military items, and nuclear items, and also introduces a number of new concepts and control measures, such as "deemed export" and "restricted parties list."

Export. Under the prior regulations, covered export activities included cross-border export under international trade, transfer by means of foreign communication, exchange, provision as a gift, tradeshow, scientific and technological cooperation, aid, service or other means. Transit, transshipment, and pass-through were also covered. The new ECL simplifies the definition of export as "the transfer of controlled items out of the People's Republic of China, and the provision of controlled items by any citizens, legal persons or non-legal-person organizations of the People's Republic of China to any foreign organizations and individuals." The latter part of the definition is a new concept in China, which is similar to the "deemed export" as under the U.S. export controls regime. Please see further discussion in Section 15.3.

Covered operator. The term "export operator" is not defined in the new ECL or in the previous regulations. In general, the primary responsible party would be the exporter of record, or the consignor (shipper) when the exporter of record acts as an agent. Under the new ECL, foreign importers and end users also have non-diversion obligations, as well as mandatory

reporting obligations to the Chinese authority when they become aware of possible changes of end user or end use.

Notably, the new ECL adds a general prohibition that no third-party service providers, including agents, transportation, mailing or delivering service providers, customs declaration brokers, third party e-commerce trading platforms, and banking service providers shall provide service to export operators who engage in unlawful exports. Knowingly providing such services would subject the third-party service provider to penalties.

Controlled items. Under the new ECL, controlled items include tangible items, technologies, and services in the following categories:

- Military items (including police equipment)
- Dual-use items (chemicals, biological items, missiles, nuclear)
- Nuclear items
- Other controlled items (precursor chemicals, civil aviation items, encryption items, etc.)
- Other technologies prohibited or restricted for exports

Notably, the new ECL expands the scope to *service* (undefined) and *anything* that has proliferation, terrorism, national security, or national interests implications.

(ii) Economic Sanctions

China does not promulgate specific laws or regulations for economic sanctions. Instead, China adopts United Nations (UN) sanction-related resolutions. With China's permanent seat in the UN Security Council, economic sanctions mandated by the resolutions of the UN Security Council become China's international obligations.

In 2019–2020, the Chinese government introduced a concept of "Unreliable Entity List" (UEL), which was formalized with the "Provisions on the Unreliable Entity List" (the "UEL Provisions") published by the Ministry of Commerce, effective September 19, 2020. The UEL Provisions lay out a mechanism to designate foreign companies to the UEL, and may impose sanction measures to designated entities.

In 2021, China enacted the Anti-Foreign Sanctions Law, effective June 10, 2021, to establish its own sanctions regime against foreign persons as a countermeasure for certain foreign discriminatory restrictive measures (e.g., economic sanctions) imposed by other countries, as well as a Chinese "Blocking Statute"—the Rules on Counteracting Unjustified Extra-territorial Application of Foreign Legislation and Other Measures (the "Blocking Rules"), effective January 9, 2021, aiming to block the application of unjustifiable extraterritorial foreign laws and measures. Please see Section 15.2(e) and (f) for more details.

Where to Find the Regulations: Generally, all Chinese laws and regulations are available on the official website of the National People's Congress.[2] Chinese export control regulations are also placed on the website of the Ministry of Commerce (MOFCOM), which is the main government authority responsible for export controls.[3]

China does not promulgate separate laws or regulations for economic sanctions. Economic sanctions mandated by the resolutions of the UN Security Council become China's international obligations. To fulfill its international obligations, the government implements the UN sanctions through a series of administrative notices. Most notices can be found from the website of the Ministry of Foreign Affairs (MFA).[4]

The counter-sanctions or countermeasures taken by China against persons or actions endangering its sovereignty and security are based on three legal instruments:

- Anti-Foreign Sanctions Law,[5]
- Rules on Counteracting Unjustified Extra-territorial Application of Foreign Legislation and Other Measures ("the Blocking Rules),[6] and
- Provisions on Unreliable Entity List.[7]

The sanctions imposed under the Anti-Foreign Sanctions Law, as announced by MFA, can be found on the MFA website.[8]

Who Is the Regulator: The State Council is the primary authority for China's export controls of most of the controlled items (except for military items). The agency in-charge is MOFCOM and its Bureau of Industry, Security, Import and Export Control.[9] Other relevant agencies include the General Customs of China; Ministry of Foreign Affairs; China Nuclear Safety Administration; the Ministry of Transport; the Ministry of Public Security; the Ministry of Industry and Information Technology; China Atomic Energy Authority; the Central Military Commission; and State Administration of Science, Technology and Industry for National Defense. The Central Military Commission and its subordinate agency, State Munition Trade Bureau, are the primary authorities for the export controls of military items.

As to economic sanctions, MFA is the primary government agency. The programs are implemented by various regulatory authorities, such as MOFCOM, the People's Bank of China (the central bank), China Banking and Insurance Regulatory Commission, China Securities Regulatory Commission, the Ministry of Transport, the General Customs of China, and the Ministry of Public Security, in their respective authority.

How to Get a License: Different licensing requirements apply based on the items to be exported and their respective control reasons.

Export License for Dual-Use Items: Before engaging in any export of dual-use items, an exporter must first obtain a Registration Certificate for Exporters of Dual-Use Items ("Registration Certificate") from MOFCOM. This registration process is described in more detail in Section 15.7(b).

For export, the exporter shall submit their application documents to the local provincial commercial authorities for verification and obtain a Dual-Use Items and Technologies Export License from MOFCOM upon its approval. The export license is required to be submitted to Customs during the exportation process. The licensing process is described in more detail in Section 15.7(b).

Export License for Military Items. For export of military items, only a limited number of specially authorized state-owned companies are authorized to participate in munitions trade. For application for Munition Export License, the export project needs to be approved first by the State Administration of Science, Technology and Industry for National Defense. Once the export contract is concluded, a Munition Export License needs to be obtained before the items can be exported. The approving and licensing authority is the State Munition Trade Bureau, which is the acting agency for the State Munition Trade Committee under the direction of the Central Military Commission. The licensing process is described in more detail in Section 15.7(c).

Export License for Restricted Technologies. An exporter shall first submit an application to MOFCOM for a pre-approval in the form of a Letter of Intent for Technology Export License.

Only after the pre-approval is granted, can the exporter negotiate and sign technology export contracts. After concluding the export contract, the exporter shall submit the relevant documents to MOFCOM to apply for the Export License for Technologies. MOFCOM has delegated the approval and licensing authority to its local counterparts at the provincial level. During the approval process, MOFCOM may have to consult with other government authorities (e.g., the authority overseeing activities related to science and technology). The licensing process is described in more detail in Section 15.7(d).

Key Websites: As to export control, MOFCOM's website is available at www.mofcom.gov.cn and provides texts of regulations, export control licensing procedures, and controlled lists. There is also an English version of the website, which contains English translation of selected laws and regulations (http://english.mofcom.gov.cn).

On December 30, 2021, MOFCOM created a new website named the China Export Control Information: http://exportcontrol.mofcom.gov.cn/. The website contains laws, regulations, FAQs, and policy documents related to China's export control system, guidance and services related to the establishment and maintenance of a proper export control compliance system, and updates on China's most recent export control-related policy moves.

As to economic sanctions, UN sanctions and Chinese anti-foreign sanctions can be found on MFA's website: https://www.fmprc.gov.cn. There is also an English version of the website available (https://www.fmprc.gov.cn/mfa_eng/).

15.2 Structure of the Laws and Regulations

(a) International Treaties

There are five major multilateral export control regimes worldwide, and China only participates in one regime, specifically the Nuclear Suppliers Group, but has committed to abide by some aspects of the other multilateral control regimes as described here:

- UN Arms Trade Treaty. China is not a signatory nation, but it largely commits to abide by the regime.
- The Nuclear Suppliers Group (NSG) for the control of nuclear-related technology. China became a member in 2004.
- The Australia Group (AG) for control of chemical and biological weapons. China is not a member. Meanwhile, China is a signatory nation of the Chemical Weapons Convention (CWC), which controls the export of certain chemical weapons and precursors.
- The Missile Technology Control Regime (MTCR) for the control of rockets and other aerial vehicles capable of delivering weapons of mass destruction. While China is not a member, it has largely agreed to abide by the regime. China applied for joining the regime in 2004 but has not yet been accepted as a member.
- The Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. China is not a member. Note that Chinese dual-use list is substantially different than the WA's scope of dual-use lists, particularly regarding Category 3 electronics, Category 4 computers, and Category 5 telecommunications, which are not on China's list of dual-use items.

(b) National Laws and Regulations on Export Controls

Beginning in the 1990s, China has gradually developed the legal framework of export controls of its own, to control the exports of military items, nuclear items, dual-use items, and other sensitive items. The major laws and regulations include:

- Administrative Measures on Import and Export License for Dual-Use Items and Technologies, enacted in 2005
- Regulations on Export Controls of Munitions, enacted in 1997 and amended in 2002
- Regulations on Export Controls of Nuclear, enacted in 1997 and amended in 2006
- Regulations on Export Controls of Nuclear Dual-Use Items and Related Technologies, enacted in 1998 and amended in 2007
- Regulations on Export Control of Missiles and Related Items and Technologies, enacted in 2002
- Regulations on Export Control of Biological Dual-Use and Related Equipment and Technologies, enacted in 2002
- Regulations on Administration of Controlled Chemicals, enacted in 1995 and amended in 2011
- Regulations on Administration of Precursor Chemicals, enacted in 2005 and amended in 2016
- Regulations on Administration of Technology Import and Export, enacted in 2001 and last amended in 2020
- Administrative Measures on Prohibition and Restriction of Technology Export, enacted in 2001 and amended in 2009
- Regulations of Administration of Commercial Encryption, enacted in October 1999
- Encryption Law, enacted in 2019 and effective January 1, 2020
- Export Control Law, enacted in October 2020 and effective December 1, 2020

(c) Controlled Lists

China has promulgated three different kinds of controlled lists, for (1) dual-use items and technology; (2) technologies prohibited or restricted from export; and (3) munitions.

1. Dual Use Items and Technologies Import and Export Licensing Catalogue ("**Dual Use Catalogue**");
    - Nuclear Items and Related Technologies
    - Nuclear Dual-Use Items and Related Technologies
    - Biological Dual-Use Items and Related Equipment and Technologies
    - Controlled Chemicals
    - Certain Chemicals and Related Equipment and Technologies
    - Missiles and Missile-related Items and Technologies
    - Precursor Chemicals (Group I)
    - Precursor Chemicals (Group II)
    - Certain Parts of Dual-Use Products and Technology
    - Certain Special Civil Use Products and Technology
    - Commercial Encryption Items
2. Catalogue of Technologies Prohibited or Restricted from Export ("**Technology Catalogue**"), first published in 2008, amended in 2020, and recently revised on Dec. 30, 2022 for public comments
3. Catalogue of Controlled Munitions of 2002 ("**Munitions Catalogue**")

(d) China and UN Security Council Sanctions

China implements UN sanctions through administrative notices. Generally, the MFA first initiates a notice to notify various government agencies of relevant UN Security Council resolutions and to urge the agencies to implement economic sanctions mandated by the resolutions. Various regulatory authorities, such as MOFCOM, the General Customs of China, the People's Bank of China, China Banking and Insurance Regulatory Commission, China Securities Regulatory Commission, and the Ministry of Transport, then issue notices to implement measures in their respective jurisdictions.

Specific sanction resolutions are implemented primarily in the following two ways:

1. Implementation without Additional Domestic Rules to UN Resolutions

   Under most scenarios, UN sanction-related resolutions are implemented by the government by means of administrative notices attaching UN resolutions, without any additional domestic rules for government agencies. For example, on April 28, 2016, the Ministry of Transportation simply forwarded Resolution 2278 of the UN Security Council (sanctions against Libya that impose sanctions including arms embargo, travel ban, assets freeze, and prohibition of illegal oil exports), without adding additional domestic rules to implement this resolution. The Ministry of Transportation also urged all the relevant departments to take responsible measures and strictly implement the UN resolution.
2. Implementation with Additional Domestic Rules to UN Resolutions

   Another method to implement UN resolutions is by adding relevant government agencies' additional rules and interpretations, which is more common in the banking area. For example, the China Banking and Insurance Regulatory Commission has issued a number of notices adding rules to implement UN economic sanctions resolutions, such as to urge banks to remain on high alert over businesses and transactions involving sensitive countries or regions, and to prevent organizations or individuals from using financial institutions for supporting terrorism, money laundering, and other illegal activities.

In some limited cases, China does not implement sanctions from UN due to the political positions of the government. For example, UN sanctions against Sudan have not been implemented in China.

(e) Chinese National Laws on Economic Sanctions

China does not promulgate separate laws or regulations for economic sanctions. In most cases, the government implements the UN economic sanctions through a series of administrative notices. See Section 15.2(d). China has enacted a number of laws and regulations in 2020 and 2021 to establish its own counter-sanctions regime.

(i) Unreliable Entity List

On September 19, 2020, MOFCOM promulgated the Provisions on the Unreliable Entity List (the "UEL Provisions"). The UEL targets foreign entities whose activities are considered to have endangered the national sovereignty, security, and development interests of China, or undermined the legitimate rights and interests of Chinese enterprises, other organizations, or individuals. Please see further detailed discussions in Section 15.13.

(ii) Blocking Rules

On January 9, 2021, MOFCOM promulgated the Rules on Counteracting Unjustified Extra-territorial Application of Foreign Legislation and Other Measures (the "Blocking Rules"), which are designed to block the application of certain foreign laws and measures that are determined to have the effect of unjustifiably prohibiting or restricting transactions between Chinese persons and third-country persons. Please see further detailed discussions in Section 15.14.

(iii) Anti-Foreign Sanctions Law

On June 10, 2021, the Anti-Foreign Sanctions Law of People's Republic of China (AFSL) was adopted by the Standing Committee of the National People's Congress (NPC) and signed into law by the chairman of the PRC.

Before the AFSL was enacted, the Foreign Trade Law (2016, as amended) provided the general legal basis for imposing sanctions and the National Security Law (2015) provided legal authority for the State Council to take actions as necessary when there was a national security concern.

Now, the AFSL has become the primary authority for the Chinese government to impose its own sanctions. The law primarily targets those foreign individuals/organizations that are considered to be actively pursuing or involved in enacting "discriminatory restrictive measures" against China. Any individuals or organizations that directly or indirectly participate in the formulation, decision-making, or enforcement of the "discriminatory restrictive measures" may be placed on the counter-sanctions list. Related individuals and entities of the listed individuals or organizations may also be subject to countermeasures.

Please see further detailed discussions in Section 15.15.

(f) Chinese Sanctioned Parties Lists

China has adopted the sanction lists of the UN Security Council. It is also changing its position to establish its own list of sanctioned individuals and entities under the ASFL and the UEL.

Prior to the AFSL being enacted, the Chinese government (i.e., MFA) had begun its sanctions on certain individuals and entities who were viewed as responsible for activities interfering in China's internal affairs, or for their involvement in foreign unilateral sanctions on Chinese entities and individuals. On July 23, 2021, MFA announced sanctions on seven U.S. persons, directly citing the authority under the AFSL, including former U.S. Secretary of Commerce Wilbur Louis Ross, Chairman of U.S.–China Economic and Security Review Commission (USCC) Carolyn Bartholomew, former Staff Director of Congressional-Executive Commission on China (CECC) Jonathan Stivers, DoYun Kim at the National Democratic Institute for International Affairs, senior program manager of the International Republican Institute (IRI) Adam Joseph King, China Director at Human Rights Watch Sophie Richardson, and Hong Kong Democratic Council.[10] The sanction measures being imposed were not specified.

Under the AFSL, MFA or other relevant departments of the State Council will issue orders announcing the determination, suspension, modification, or cancellation of the counter-sanction listing and countermeasures. The restrictions on those entities typically include banning the targeted persons and their families from entering China (including Hong Kong, Macao), freezing assets in China, and restricting transactions with organizations and individuals in China.

Currently, MFA announces its sanctions through its press conferences, and has not yet established a list of foreign persons subject to the counter-sanctions. Far more than 90

individuals and organizations have been sanctioned by MFA.[11] The following chart provides the links to specific web pages indicating the sanctions as of February 2023. On Dec. 23, 2022, MFA introduced the counter-sanction list and designated two individuals.

Date	Links
12/2/2019	https://www.mfa.gov.cn/web/wjdt_674879/fyrbt_674889/201912/t20191202_7815504.shtml
7/13/2020	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202007/t20200713_693288.html
7/14/2020	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202007/t20200714_693290.html
8/10/2020	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202008/t20200810_693328.html
10/26/2020	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202010/t20201026_693454.html
11/30/2020	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202011/t20201130_693509.html
1/21/2021	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202101/t20210121_693590.html
3/22/2021	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202103/t20210322_9170710.html
3/26/2021	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202103/t20210327_9170714.html
3/27/2021	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/202103/t20210327_9170817.html
5/26/2021	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202105/t20210526_9170752.html
7/23/2021	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/202107/t20210723_9170832.html
12/21/2021	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202112/t20211221_10473754.html
12/30/2021	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202112/t20211230_10477568.html
2/21/2022	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202202/t20220221_10644075.html
3/31/2022	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202203/t20220331_10658285.html
8/5/2022	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202208/t20220805_10735987.html
8/12/2022	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/202208/t20220812_10742448.html
12/23/2022	https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202212/t20221223_10994393.html

As to the UEL, China establishes a working mechanism with the involvement of relevant departments of central state organs (the "working mechanism") to be responsible for administering the UEL regime. Foreign persons who are (1) endangering the national sovereignty, security, or development interests of China; or (2) suspending normal transactions with an enterprise, other organization, or individual of China or applying discriminatory measures against an enterprise, other organization, or individual of China, which violates normal market transaction principles and causes serious damage to the legitimate rights and interests of the enterprise, other organization, or individual of China, might be designated. The UEL Provisions further set out a menu of measures the government can choose from, which includes (1) restricting or prohibiting the foreign entity from engaging in China-related import or export activities; (2) restricting or prohibiting the foreign entity from investing in China; (3) restricting or prohibiting the foreign entity's relevant personnel or means of transportation from entering into China; (4) restricting or revoking the relevant personnel's work permit, status of stay, or residence in China; (5) imposing a fine of the corresponding amount according to the severity of the circumstances; or (6) other necessary measures. On Feb. 16, 2023, Lockheed Martin Corporation and Raytheon Missiles & Defense were designated to the UEL for endangering the national sovereignty, security, and development interest of China.

15.3 What Is Regulated: Scope of the Regulations

(a) The Scope of Export Control

(i) Export Activities

A. Export

Covered export activities include cross-border exports under international trade, and transfers by means of foreign communication, exchange, provision as a gift, tradeshow, scientific and technological cooperation, aid, service or other means.

Exports to domestic free trade zones or bonded locations/facilities are not cross border, and thus are not covered. Exports from free trade zones or bonded locations/facilities to overseas are subject to export controls.

B. Re-export

The ECL expands the scope of the law to cover "re-exports," but the term is not defined. The term "re-export" is mentioned in the context together with transit, transshipment, pass-through, re-export and export from special customs supervision areas under Article 45. It is unclear what the purpose is and how the government intends to exert controls over re-exports, as the drafters offered no explanation in this regard. It should be noted that in the 2017 MOFCOM draft, a definition of "re-export" was provided as "the export from overseas to other foreign destination of controlled items or foreign products containing a certain amount of Chinese controlled items by value." Such definition was removed in later drafts and not included in the final law.

C. Deemed Export

The ECL also expands the scope of export to cover "deemed export." The term "deemed export" is not specified in the law but is implied under the definition of "export control," which reads as "the provision of controlled items from PRC citizens and entities to foreign individuals and entities." Thus, the provision of controlled technologies to a foreign person within China is now regulated and would require an export license.

Arguably, by literal reading of a prior regulation (i.e., Administrative Measures on Import and Export License for Dual-use Items and Technologies of 2005), the words "export by the means of foreign communication, exchange, cooperation, and service" theoretically could already have covered the transfer of technologies from PRC persons to foreign persons.

D. Transit, Transshipment, and Pass-through Shipment

Transit, transshipment, and pass-through shipment of controlled items are also covered. The terms "transit" and "transshipment" are not defined under the ECL. However, pursuant to the Chinese Customs Law, "transit goods" are those transported through Chinese territory by land; "transshipment goods" are those not transported overland through Chinese territory, but stop to change the means of transport at a place where a Customs office is established; and "pass-through shipment goods" are those entered into Chinese territory but exited through the original transporting ocean or air vessels.

E. In-country Transfer

While the term "in-country transfer" is not specified in the ECL, a change of end user would require prior approval from the Chinese government. Without such a prior approval for a change in end user, the exporter or the original end user could risk being placed onto a restricted parties list. It is also a breach of commitment as provided in the end user certification: "[w]e guarantee that we will not transfer the above-said . . . (commodity name) to any third party without the consent of the Chinese government."

(b) Controlled Items

Under the ECL, controlled items include goods, technologies, and services of the following:

- Military items (equipment, specialized production machinery, and other relevant goods, technologies, and services used for military purposes);
- Dual-use items (goods, technologies, and services that are for both civil and military purposes or contribute to an increase in military potential, especially those that may be applied to design, develop, produce, or use weapons of mass destruction and their means of delivery);
- Nuclear items (nuclear materials, nuclear equipment, nonnuclear materials for reactor use, and relevant technologies and services);
- Other controlled items (precursor chemicals, civil aviation items, encryption items, etc.), and
- *Anything* that has proliferation, terrorism, national security, or national interests implications.

Note that technical materials and data related to the preceding items are also controlled.

The ECL does not provide definitions regarding "goods," "technologies," or "services." Under China Customs Law, goods are physical items. As to "technologies," since those existing export control administrative regulations remain effective, we provide certain definitions under the existing regulation as references. For example, under the Export Control List on Missiles and Related Items and Technologies, "technology" means knowledge required for the "development," "production," or "use" of items listed and which can be imparted in the form of "technical information" or "technical assistance." "Technology" does not include technology in "open domain technology" or "basic scientific research."

It is noted that, although software is not specified in the ECL, when it is exported in tangible forms (e.g., in a CD-ROM), it falls under the category of "goods"; when exported in intangible forms (e.g., emails or internet downloading), it falls under "technologies." Under the Export Control List of Nuclear Dual Use Items and Relevant Technologies, the controls over software do not cover (1) software normally available to the public through retail sales without any restrictions and that is to be installed by the user itself without further support from the supplier (what is commonly referred to as "mass market" by the Wassenaar Arrangement members), or (2) software for public use (software that has been used in the public and there is no need to impose restrictions for further use in expanded purpose).

As to "services," it is newly covered by the ECL, but unfortunately not defined under the law. "Service" has never been covered in prior existing regulations, except for the technologies that might be transferred in the means of technical service. The drafters of the ECL did not explain what "services" are covered or the reason for the decision to cover services.

(c) The Scope of Economic Sanctions

As the relevant UN Security Council's resolutions are adopted entirely by the government of China as part of its international obligations, economic sanctions and measures specified in the resolutions are implemented in China. China's UN-based economic sanctions apply to those sanctioned countries and designated persons as specified in the resolutions.

As to China's own sanctions, the Chinese government has now established its own sanctions regimes under the Anti-Foreign Sanctions Law and the UEL Provisions. Please see discussions at Sections 15.2(e) and (f).

15.4 Who Is Regulated?

As to export control, the primary party subject to export controls would be the exporter, and/or the consignor (shipper) when the exporter acts as an agent. The new ECL imposes certain reporting obligations on foreign importers and end users, and provides legal ramifications in case of diversion.

Notably, the new ECL also imposes responsibilities over third-party service providers, including agency, transportation, mailing or express courier service providers, customs declaration brokers, and third party e-commerce trading platforms, as well as banking service providers. These service providers are prohibited from knowingly providing service to export operators who engage in unlawful exports.

As to economic sanctions, PRC persons and persons within PRC territory are subject to PRC jurisdiction for the purpose of sanctions. Foreign persons might be subject to the AFSL and the UEL Provisions.

In addition, under PRC Criminal Law, foreign persons could be subject to criminal liabilities when committing a crime (1) within the PRC territory, (2) outside of the PRC territory but against the PRC or its citizens, or (3) specified in international treaties to which the PRC is a signatory state or of which it is a member and the PRC exercises criminal jurisdiction over such crimes within its treaty obligations.

15.5 Classification

(a) Classification of Dual-Use Items

Unlike the U.S. regime or WA regime, the Chinese government does not create a classification system for dual-use items (e.g., the ECCN adopted in the United States). Rather, MOFCOM's Dual-Use Catalogue provides the harmonized tariff codes (HS codes) of dual-use items for industry users. The HS codes are only for reference purposes, as the description in the Dual-Use Catalogue is dispositive. MOFCOM's Dual-Use Catalogue is updated annually, with the current one updated on Dec. 30, 2022 and effective in January 2023.[12]

The Dual-Use Catalogue is divided into 11 categories as follows:

- Category 1: Nuclear Items and Related Technologies
  1. Nuclear material
  2. Nuclear reactors and the equipment and components specially designed for reactors
  3. Nonnuclear materials used for nuclear reactors
  4. Reprocessing plant of irradiation components and the equipment specially designed or manufactured for the components
  5. Plant for manufacturing fuel element and the equipment specially designed or manufactured for it
  6. Separation plant of uranium isotope and the equipment specially designed or manufactured for it (except for the analysis instrument)
  7. Plant for production or concentration of heavy water, deuterium and deuteride, and the equipment specially designed or manufactured for them
  8. Uranium and plutonium transformation plant used for manufacturing fuel element and separating uranium isotope as defined by (5) and (6), and the equipment specially designed or manufactured for them

- Category 2: Nuclear Dual-Use Items and Related Technologies
  1. Industrial equipment
  2. Materials
  3. Separation equipment and parts of uranium isotope
  4. Relevant equipment of heavy water factory
  5. Test and measurement equipment used in the development of nuclear explosive devices
  6. Components of a nuclear explosive device
  7. Temporarily controlled items

- Category 3: Biological Dual-Use Items and Related Equipment and Technologies
  1. Human or zoonotic pathogens
  2. Plant pathogens
  3. Animal pathogens
  4. Toxins and its subunits
  5. Genetic elements and genetically modified organisms
  6. Dual-use biological equipment
  7. Related technology

- Category 4: Controlled Chemicals
  1. Chemicals that can be used as chemical weapons
  2. Chemicals that can be used as precursors for the production of chemical weapons
  3. Chemicals that can be used as the main raw materials for the production of chemical weapons

- Category 5: Certain Chemicals and Related Equipment and Technologies
  1. Chemicals
  2. Production equipment of relevant chemicals
  3. Special detector and gas monitoring system
  4. Related technology

- Category 6: Missiles and Missile-related Items and Technologies
  1. Complete vehicle
  2. Power system
  3. Navigation
  4. Materials
  5. Electronic device
  6. Control system
  7. Warhead
  8. Ground equipment
  9. Propellant
  10. Software
  11. Other parts and accessories
  12. Design, testing, and production facilities and equipment
  13. Related technology
  14. Temporarily controlled items

- Category 7: Precursor Chemicals (Group I)

- Category 8: Precursor Chemicals (Group II)
- Category 9: Certain Dual-Use Products and Technology
- Category 10: Certain Special Civil Use Products and Technology
- Category 11: Commercial Encryption Items
  1. System, equipment, and components
  2. Testing, inspection, and production equipment
  3. Software
  4. Technology

(b) Classification of Munitions

The Munitions Catalogue contains the following categories:

- Category 1: Small arms and light weapons
- Category 2: Artillery and other launchers
- Category 3: Ammunition, mines, sea mines, bombs, anti-tank missiles, and other explosive devices
- Category 4: Tanks, armored vehicles, and other military vehicles
- Category 5: Military engineering equipment and facilities
- Category 6: Military ships and their special equipment and facilities
- Category 7: Military aviation aircraft and its special equipment and facilities
- Category 8: Rockets, missiles, military satellites, and their auxiliary equipment
- Category 9: Military electronic products and fire control, ranging, optics, navigation, and control devices
- Category 10: Explosives, propellants, fuel agent, and related compounds
- Category 11: Military training equipment
- Category 12: Protective equipment and facilities against nuclear, biological, and chemical weapons
- Category 13: Logistic equipment, materials, and other auxiliary military equipment
- Category 14: Other products

(c) Classification of Technologies Prohibited or Restricted from Export

In addition to controlling dual use technologies, China also controls the export of certain non-dual-use technologies pursuant to the Regulations Concerning the Administration of Technologies Import and Export (RATIE). Under the RATIE, technologies are classified into three categories for the purpose of export administration, including prohibited technologies, restricted technologies, and nonrestricted technologies. The controlled purposes under the RATIE include national security, public morality, environmental protection, physical health, and so on. Prohibited technologies cannot be exported, while restricted technologies are subject to export licensing requirements, and nonrestricted technologies can be exported under a system of contract registration.

Under the RATIE, “export” means transfer of technologies from the territory of the PRC to outside of PRC through ways including patents transfer, technology transfer, transfer of patent application rights, grants of patent licenses, and so on. As long as technologies are transferred to outside of China, it will be viewed as technology cross-border transfer or technology export, and a license will be needed for those technologies listed under the restricted category. It is noteworthy that, unlike the control over dual-use technologies, for non-dual-use technologies

that fall under the prohibited or restricted category, the transfer or licensing of the patents are either prohibited or require an export approval and license, even if the patented technology information is already in the public domain.

Prohibited technologies and restricted technologies have separate lists. The control measures are administered by the Department of Trade in Service and Commercial Service (DTS) at MOFCOM. Technologies that fall under the Catalogues of Technologies Prohibited or Restricted from Export ("Technology Catalogues"), as amended in 2020, are controlled under RATIE. The current list was published in 2008,[13] and an amendment was issued in 2020.[14] The latest modification was introduced in 2022 for public comments.

To determine whether a technology is controlled under RATIE, the Technology Catalogues have provided the general description of technologies and specific "control points" to each listed technology. With respect to the "control points," it is similar to a "positive list," which means they are specific and exhaustive (not open ended). Nevertheless, from a technical point of view, such control points are still considered very broad.

In light of China's development and leading roles in certain computer and information technology sectors over the past years, MOFCOM adopted the recent 2020 amendment, and one of the main changes pertains to information-processing technologies, including artificial intelligence interactive interface technology, encryption security technology, and information defense technology. The technologies prohibited or restricted from export are classified under two main categories as the following:

- Technologies prohibited from export are divided into 20 categories, including nonferrous metal smelting, pharmaceutical manufacturing, transportation equipment manufacturing, telecommunications and other information transmission services, communications equipment, computers and other electronic equipment manufacturing, and so on. Here is one example of the prohibited technologies:
  Communications equipment, computers and other electronic equipment manufacturing
  Number: 054002J
  Technology Name: Robotic manufacturing technology
  Control Point: Robotic manufacturing technology of remote control and coring detection
- Technologies restricted from export are divided into 33 categories, including pharmaceutical manufacturing, general equipment manufacturing, computer service, software, electronic machine and equipment manufacturing, and so on. Here is one example:

Information Processing Technology
Number: 056101X
Technology Name: Information Processing Technology
Control Points:
{1-16, omitted}
[2020 additions] 17) Speech synthesis technology (including corpus design, recording and annotation technology; speech signal feature analysis and extraction technology; text feature analysis and prediction technology; speech feature probability statistics model construction technology, etc.); 18) Artificial intelligence interactive interface technology (including speech recognition technology, microphone array technology, voice wake-up technology, interactive understanding technology, etc.); 19) Voice evaluation technology (including automatic scoring technology for speaking, automatic scoring technology for oral expression, pronunciation detection technology, etc.); 20) Intelligent Marking Technology (including printing scan recognition technology, handwriting scan recognition technology, printing photo recognition technology, handwriting photo recognition technology, Chinese and English composition correction technology, etc.); 21) Personalized information push service technology based on data analysis.

Please refer to Section 15.7(d) for the licensing procedure.

15.6 General Prohibitions/Restrictions/Requirements

Regulations prior to the ECL prohibit (1) exports of controlled items without export licenses; and (2) exports of any items without export licenses when export operators know or should know the items are to be used for mass weapons of destruction or for terrorism purposes, or may jeopardize national security.

The new ECL further provides two additional general prohibitions: (1) export operators shall not deal in violation of relevant requirements with foreign importers and/or end users designated in the restricted parties list, who may be subject to prohibition or restriction measures; and (2) third-party service providers, including agency, transportation, mailing or express courier service providers, customs declaration brokers, and third party e-commerce trading platforms, as well as banking service providers, are prohibited from knowingly providing services to export operators who engage in unlawful exports.

With respect to economic sanctions, exporters should follow the UN resolutions adopted by China and shall not export subject products to the UN sanctioned countries, entities, and individuals. Also, if foreign entities are placed on the UEL or subject to the MFA sanctions, exports to those entities may be restricted or prohibited (also see Section 15.2(e) and (f)).

15.7 Licensing/Reasons for Control

The Foreign Trade Law authorizes export controls for the following reasons:

- Safeguarding national security, and public interests and ethics;
- Protecting human health or safety, the lives or health of animals and plants, or the environment;
- Implementing the measures related to the import and export of gold and silver;
- Short supply on domestic market or for effective conservation of exhaustible natural resources;

- Limited market capacity of the importing country or region;
- Serious disorder of exports;
- As required by laws and administrative regulations; or
- As provided for in any international treaty or agreement that China has concluded or acceded to.

Also, the National Security Law has provided legal authority for the State Council to take actions as necessary when there is a national security concern. Specifically, Article 37 provides that

> the State Council shall, in accordance with the Constitution of the People's Republic of China and other applicable laws, formulate administrative regulations related to national security, stipulate relevant administrative measures and issue relevant decisions and orders and it shall implement laws, regulations and policies related to national security.

The new ECL also includes a "catchall" clause, which provides that, for exports of items not on the Dual-Use Catalogue, when export operators know or should know, or upon notification by the authority that the items are to be used for (1) endangering national security and interest; (2) designing, developing, producing, or using weapons of mass destruction and their conveyances; or (3) terrorism purposes, export licenses are required.

For specific controlled items, the current export controls regulations provide the reasons for controls, including chemical weapon, biological weapon, WMD, and nuclear proliferation for those dual-use items.

(a) Types of Export Control Licenses and Permits for Dual-Use Items

Before export operators can proceed to apply for export control licenses for dual-use items, they need to first register with MOFCOM and obtain a Dual-Use Export Operation Registration Certificate. See Section 15.7(b) for the registration process. As to the dual-use items, there are three types of export control licenses:

- Single-use contract-specific license, which is good for each shipment or multiple shipments under the same contract. The license has a set expiry date, normally within one year.
- General or basket license, which is good for exporting one or multiple controlled items to one or multiple end users in one or multiple countries within the valid period of time (Type A), or good for exporting of a particular type of dual-use item made to specified end user(s) in a particular country (Type B). Such general/basket license is good for three years or less.
- Basket license for certain exports of civil aviation parts for repairing, temporary exports, bonded, leasing purpose can be used for unlimited shipments within the valid period.

(b) Export Control Licensing Procedure

(i) Registration

The Dual-Use Operation Registration Certificate application is submitted to the local department of commerce at the provincial level for pre-examination.[15] The application files should be submitted through an e-portal at https://ecomp.mofcom.gov.cn. Such application would be passed onto MOFCOM for final approval. The approval process takes ten working days. The registration is valid for three years and needs to be renewed one month prior to its expiration.

Changes in company names or corporate status (e.g., merge, spin-off, or deregistered) require a new application.

To be eligible for registration, export operators shall:

- Have a valid business license and have obtained the "Foreign Trade Operator Registration Certificate" (which is generally required for any exporter);
- Have passed annual review by the local offices of State Administration for Market Regulation and Ministry of Commerce;
- Have not been subject to criminal punishments, or administrative punishments relating to illegal operation, in the last three years;
- Have the knowledge regarding the performance, technical indices, and main usage of the subject items; and
- Have established internal functions responsible for export and aftersales follow-up services.

It is noted that in the draft Export Control Law, it was provided that export operators were required to establish an export control compliance program. Such a mandatory requirement is removed in the final ECL. Instead, when an export operator has established a compliance program and effectively implemented it, such factor would be taken into consideration by the licensing authority for extending convenience facilitation in license application, such as a general/basket license.

(ii) Single-Use Contract Specific Licensing

For contract-specific licenses, the application is first submitted to the local department of commerce at the provincial level for pre-examination. Once it is passed, the application would be further reviewed by MOFCOM for final approval. The application process is done through a MOFCOM Online Application Platform[16] and the physical copies of documents are submitted to the local department of commerce. The total processing time is 45 working days. The following documents are required for the application:

- Completed standard application form;[17]
- Foreign Trade Operator Registration Form and Dual-Use Operator Registration Certificate;
- Personal identification documents for the legal representative, and the personnel in charge for the application;
- Copies of export contract and sales documents;
- Statement providing the technical description of the subject controlled item;
- Statement providing the details of the end user;
- End user and end-use certification.[18]

The licensing authority considers the following factors in the approval process:

- International obligations and the state commitments,
- National security,
- Type of export,
- Sensitivity of the controlled item,
- Destination,
- End user and end use,
- Credit history of the export operator, and

- Other factors as prescribed in relevant laws and regulations.

During the drafting of the new Export Control Law, it was suggested that the licensing authority may require the end user and end-use certification to be provided by the concerned foreign government, depending on the sensitivity of the controlled item and the end user. Such language was removed in the final law and is now replaced with the wording that the end user and end-use certification may be issued by end users or the concerned foreign government agency.

In addition, the MOFCOM initial draft provided that the licensing authority may conduct on-site verification of end user and end use when necessary. Such on-site verification provision was removed in the later first draft submitted for NPC deliberation. However, in the final law, verification over end user and end use was added back, in the context that the state export control authority would establish a management system for controlled items end user and end use to enhance controls over end user and end use by conducting end user and end use evaluation and verification.

(iii) Licensing Convenience—General Licensing

To facilitate frequent applicants, companies that have been exporting dual-use items from China for two consecutive years are eligible to apply for general licenses.

- Type A (for exports of multiple types of dual-use items made to multiple end users in multiple countries). An eligible applicant must have successfully obtained no fewer than 40 export licenses for dual-use items in two consecutive years.
- Type B (for exports of a particular type of dual-use item made to specified end user(s) in a particular country). An eligible applicant must have successfully obtained no fewer than 30 export licenses for dual-use items and technology in two consecutive years.

Applications for both types of general licenses must be filed with MOFCOM through a MOFCOM Online Application Platform.[19] The following documents are required for the application:

- Completed standard application form;[20]
- Information and evidence in relation to the establishment and implementation of internal control system;
- Affidavit that the applicant has not been criminally penalized or punished by relevant government agencies;
- Foreign Trade Operator Registration Form or the Certificate of Approval for Foreign Invested Enterprise;
- Information concerning the export activities of dual-use items conducted by the applicant in the past two years;
- Descriptions of the dual-use item(s) for which the general license is sought;
- Guarantee that the applicant will request the end-user certification before the performance of each contract, pursuant to the applicable laws and regulations.

The current regulations provide that MOFCOM may engage independent expert consultants to evaluate the applicant's internal compliance program and the effectiveness thereof.

The new ECL provides that the licensing authority may extend convenience facilitation in license application by the means of general license for those export operators who have established and implemented a sound compliance control program.[21]

(c) Import and Export Licenses for Military Items

(i) Import of Military Items

Currently there is no specific regulation with regard to the import of military items. Since the Foreign Trade Law provides the legal authority, China may restrict or prohibit the import of military items when necessary for national security.

(ii) Export of Military Items

The export of military items can only be conducted by a limited number of authorized state-owned companies. Export of military items shall be reviewed and approved by the state military export authority itself or in conjunction with relevant departments of the State Council and the Central Military Commission. The export project needs to be reviewed first by the State Administration of Science, Technology and Industry for National Defense (SASTIND). After the project is approved, the export operator may sign an export contract with the foreign counterparty. After the export contract is signed, the export contract needs to be reviewed and approved by the state military export authority. The export contract can only become effective upon the approval. Military items trading companies shall apply to the State Munition Trade Bureau, which is the acting agency for the State Munition Trade Committee under the direction of the Central Military Commission, for export licenses for military items with the approval documents they received for the export contracts.[22]

(d) Export Licenses for Restricted Technologies

Pursuant to Regulations Concerning the Administration of Technologies Import and Export, an exporter (i.e., licensor or transferor) shall first submit an application to MOFCOM for project pre-approval. Upon approval, MOFCOM will issue a Letter of Intent for Technology Export License. Only after the Letter of Intent for Technology Export License is issued can the exporter negotiate and sign technology export contracts.

After entering into the contract, the exporter can then apply for a license for restricted technology export. The following are some basic documents that need to be submitted:

- Letter of Intent for Technology Export;
- Copy of the technology export contract;
- Materials related to the technology to be exported; and
- Incorporation certificates or business registration of the parties.

During the approval process, besides examining the commercial terms, MOFCOM evaluates the technologies in collaboration with the relevant authorities in charge of science and technology. The approval time is 45 working days. We note that, as the government has very limited experience in the review and approval of technologies restricted for export, the process could potentially be very long, up to several months.[23]

(e) Export Permits and Independent Expert Examination

Under the export control regulations prior to the ECL, the Regulations on Export Controls of Nuclear Dual-Use Items and Related Technologies provided that MOFCOM shall organize experts in relevant fields to form an Advisory Committee on Export Control of Dual-Use

Nuclear Items and Related Technologies, for consultation, evaluation, and examination of export controls of dual-use nuclear items and related technologies.

The new ECL also provides that the state export control administration departments shall coordinate with other relevant departments to establish an expert advisory mechanism for seeking consultation opinions. In addition, in reviewing application for basket licenses, the regulations provide that MOFCOM may engage independent expert consultants to evaluate the applicant's internal compliance program and the effectiveness thereof.

15.8 General Licenses/License Exceptions

Current export control regulations allow eligible exporters who have been exporting dual-use items for two consecutive years to apply for general licenses that allow multiple exports to multiple end users in multiple countries; please see Section 15.7(b) for a detailed discussion regarding general licenses.

There are no license exceptions under current Chinese export control regulations and the new ECL, but the newly published Draft Provision of Export Control Regulation of Dual-Use Items have provided license exceptions under limited circumstances; please see Section 15.11(g).

15.9 Penalties, Enforcement, and Voluntary Disclosures

(a) Penalties for Violations of Export Control

Exports of dual-use items without export licenses or beyond the scope of licenses are subject to administrative and/or criminal punishments. The new ECL provides that foreign entities and individuals could be subject to legal liabilities, if they violate the ECL, impede or obstruct the fulfillment of the PRC's nonproliferation obligation, or jeopardize PRC's national security and interests.

(i) Trading of Controlled Goods

As to administrative penalties, trading of controlled goods, exporting prohibited or restricted goods without a license, is a serious violation. The administrative liabilities provided under the Foreign Trade Law and the Customs Law include confiscation of the goods and illegal income, and a fine up to RMB 1,000,000; exclusion from holding an export license; and/or the limitation or revocation of export trading rights. In addition, under relevant export control regulations, MOFCOM can impose a fine in the amount of one to five times the amount of illegal income.

The new ECL substantially increases the monetary penalties as follows:

- In the case of exporting without proper registration or export licenses, or exporting beyond the scope of export licenses, or exporting of items prohibited for export, a fine in the amount of five to ten times of illegal income can be imposed when the illegal income is more than RMB 500,000, or a fine in the amount of RMB 500,000 to 5,000,000 can be imposed when the illegal income is less than RMB 500,000.
- In the case of obtaining export licenses through fraud, bribery, or other illicit manners, or unlawfully transferring export licenses, a fine can be imposed in the amount of five to ten

times of illegal income when the illegal income is more than RMB 200,000, or in the amount of RMB 200,000 to 2,000,000 when the illegal income is less than RMB 200,000.

- In the case of forging, falsifying, or trading of export licenses, a fine can be imposed in the amount of five to ten times of illegal income when the illegal income is more than RMB 50,000, or in the amount of RMB 50,000 to 500,000 when the illegal income is less than RMB 50,000.
- In the case of dealing in violation of export control prohibition measures with importers or end users who are designated onto the restricted parties list, a fine can be imposed in the amount of 10 to 20 times of illegal income when the illegal income is more than RMB 500,000, or in the amount of RMB 500,000 to 5,000,000 when the illegal income is less than RMB 500,000.
- For those third-party service providers, including agency, transportation, mailing or express courier, customs declaration broker, and third party e-commerce trading platform, as well as banking service provider, for knowingly providing services to export operators who engage in unlawful exports, a fine can be imposed in the amount of three to five times of illegal income when the illegal income is more than RMB 100,000, or in the amount of RMB 100,000 to 500,000 when the illegal income is less than RMB 100,000.
- In the case the exporter refuses or obstructs supervisory inspection, a warning and a fine can be imposed in the amount of RMB 100,000 to 300,000; and if the circumstances are serious, the exporter shall be ordered to cease business operation for an overhaul, and even be disqualified for the export of the relevant controlled items.

In addition, the ECL also provides that the violators would be excluded from licensing for five years. The supervisor and other personnel directly responsible for the violation may be disbarred for five years, or for a lifetime if criminal liability is imposed.

As to criminal penalties, in the case of trading of controlled goods, the indictment could be for the crimes of smuggling, illegal business operations, or leaking state secrets. The liabilities for a crime of smuggling could be imprisonment of up to 15 years or even life imprisonment, depending on the gravity of violation, as well as a fine and confiscation of assets. In case the organization/entity is penalized, the person in charge could be indicted and subject to imprisonment as well.

(ii) Trading of Controlled Technologies

As to administrative penalties, in the case of trading of controlled technologies, exporting prohibited or restricted technology could lead to severe administrative and criminal liabilities. The administrative liabilities could include confiscation of illegal income, and fine of one to five times of the illegal income, exclusion from holding an export license, and/or the limitation or revocation of export trading rights.

As to criminal penalties, in the case of trading of controlled technologies, the indictment could be for crimes of illegal business operation or leaking state secrets.

(b) Penalties for Violations of Economic Sanctions

(i) Administrative Penalties

Administrative penalties are provided in the administrative notices. Specific non-compliant activities can be an administrative violation of the relevant laws and regulations, for example:

A financial institution may be subject to administrative penalties if it violates the Anti-Money Laundering Law. Financial institutions may be subject to fines ranging from RMB 200,000 to 5,000,000, and suspension or revocation of their business license. Personnel directly in charge may be subject to fines ranging from RMB 10,000 to 500,000, and be sanctioned by a disciplinary warning, be deprived of qualifications, or be prohibited from engaging in relevant financial industry work.

In the case of the exporting of prohibited goods that violate relevant sanctions, an individual/entity in breach of the relevant laws relating to sanctions could be subject to one or several of the following penalties: (1) revocation of business license; (2) confiscation of the relevant goods and illegal proceedings; (3) fines of up to RMB 1 million; and/or (4) exclusion from obtaining export license and/or limitation or revocation of export trading rights.

(ii) Criminal Penalties

The Chinese government implements the UN economic sanctions through a series of administrative notices. While the notices themselves do not provide criminal penalties for violations, specific noncompliant activities nevertheless may constitute criminal violations under PRC Criminal Law.

- Money laundering. Financial transactions with sanctioned individuals/entities could be regarded as money laundering under certain circumstances. In the case of money laundering, financial institutions and other involved individuals/entities may be subject to criminal punishments under the Criminal Law, including the confiscation of illegal income and gain, fines, and imprisonment of up to ten years.
- Smuggling goods prohibited from import/export. In the case of trading of goods, importing or exporting of goods from or to sanctioned individuals/entities may be regarded as smuggling goods prohibited from import/export, which leads to severe criminal liabilities under the Criminal Law, including fines, criminal detention, and imprisonment of up to 15 years or even life imprisonment (for cases involving smuggling of weapons or nuclear materials).

In addition, individuals or entities criminally punished would be placed on a discredited names list, which would have a wide range of consequences. For example, there would be restrictions on excess spending, restrictions on assuming managerial roles in an entity, stricter scrutiny in import and export, and other practical difficulties such as in obtaining financing, and so on.

(c) Enforcement

(i) Export Control

For violations of export controls, enforcement actions are taken by MOFCOM and Customs. If violations have criminal implications, the criminal investigations would be initiated by the Anti-Smuggling Bureau of Customs then transferred to the Procuratorate office for indictment.

The Public Security Bureau is responsible for criminal investigation regarding crime of illegal business operations, which would be transferred to the Procuratorate office for indictment.

For cases related to state secrets, the Public Security Bureau and Ministry of State Security and its subordinate agencies are responsible for investigation. If the cases are related to the crime of leaking state secrets, the investigation and the indictment would be handled by the Procuratorate office.

(ii) Economic Sanctions

Administrative economic sanctions violations are investigated and enforced by relevant authorities such as MOFCOM, the General Customs of China, the People's Banks of China (the Central Bank), China Banking and Insurance Regulatory Commission, China Securities Regulatory Commission, the Ministry of Transport, and the Ministry of Public Security, in their respective authority.

Criminal violations are investigated by the relevant regulatory authorities, such as the People's Bank of China or Customs. If the authorities find that such violations constitute criminal offences, cases are further investigated by the public security organs and/or the anti-smuggling division of the Customs and prosecuted by the Procuratorates.

(d) Voluntary Disclosure

Under the current export control regime, there is no voluntary disclosure mechanism providing mitigation or leniency in punishments when export operators self-disclose violations. It is noted that during the drafting of the new Export Control Law, the 2017 MOFCOM draft provided that when export operators cease the violation proactively or immediately upon the notice by the government, or timely report possible risks after exports to the government and actively cooperate with the investigation, administrative penalties may be reduced or waived. However, that clause was removed from the final law.

As to economic sanctions, there is no voluntary disclosure mechanism by law either.

Meanwhile, although voluntary disclosure is not an established mechanism for seeking mitigation related to administrative penalties under the regulations, in practice, it is a strong mitigating factor taken into consideration by the authorities in enforcement actions. As to cases having criminal implications, the Criminal Law specifically provides that anyone who voluntarily discloses their criminal offences will receive lighter punishments. As such, in voluntary disclosure cases, while it does not exempt one from administrative or criminal liabilities, voluntary disclosure is a viable option to seek leniency with respect to administrative liabilities in practice and with respect to criminal liabilities by law.

15.10 Recent Export Enforcement Matters

Export enforcement is primarily taken by Customs at the border and their enforcement is active. Since 2021, the Customs started to cite the ECL as the authority for imposing administrative penalties. For example, in an enforcement action taken by Tianjin Xingang Customs, a company from Jiangsu Province declared to the Customs that it was exporting 60 tons of calcined petroleum coke, which is worth US$47,400. However, upon inspection, the Customs determined that the exported items were actually artificial graphite and the export of artificial graphite requires a dual-use export license. The Customs ruled that the company's action constituted a violation of Article 34 of the ECL (export without required license) and imposed a fine of RMB 36,000.

On the contrary, MOFCOM's enforcement has been weak, and it essentially plays the role of licensing authority in practice. Although Article 30 of the ECL provides that MOFCOM and relevant commerce departments at the provincial level could prevent export violations by calling in potential violators for enforcement discussion or issuing warning letters, these enforcement actions are usually not public.

The new ECL mandates that the state export control administration authorities (i.e., MOFCOM for dual use items and Central Military Commission for military items) supervise and inspect the export activities, and further authorizes the authorities to take actions as necessary when they conduct investigations, including:

- Access to the business facilities of the party being investigated or other relevant places;
- Interview the party being investigated, interested parties, and other relevant entities or individuals, and request explanation from such persons;
- Review and make copies of relevant documentation, agreements, accounting records, business correspondences, and so on, relating to the party being investigated, interested parties, and other relevant entities or individuals;
- Inspect the transportation vehicles for export, order to stop loading of items being exported when in suspicion, order to return unlawful exported items;
- Seal or seize anything relevant to the case; and
- Inquire for information related to bank accounts of the party being investigated.

Note that the export control administration authorities do not have the power to detain or take similar actions that may limit the freedom of any persons (the public security office or the anti-smuggling division of the Customs would have such power). As such, the new ECL provides that, during the process of supervision, inspection, and investigation, the authority may act alone or request support and assistance from other government agencies.

15.11 Special Topics and China Export Control Law

As noted earlier, in 2020, the National People's Congress passed the new Export Control Law. In order to complement the ECL and provide more details regarding its implementation, on April 22, 2022, MOFCOM released the Draft Provisions of Export Control Regulation of Dual Use Items (soliciting for public comment). This section describes in one place the key changes to Chinese law made by the new ECL and key points in the Draft Export Control Regulation.

(a) Re-export and In-country Transfer

The ECL expands the scope to "re-export," but the term is not defined. The term "re-export" is mentioned in the context together with transit, transshipment, pass-through, re-export and export from special customs supervision areas under Article 45. It is unclear what the purpose is and how the government intends to exert controls over re-exports, as the drafters offered no explanation in this regard. It is of lesser doubt that foreign-made items, after entering Chinese territory, could become subject to Chinese export controls if they fall under the Chinese Dual Use Catalogue, which would then require export licenses when they are re-exported out of China. As to the circumstance where foreign importers/end users intend to re-export the Chinese-controlled items to a third country, since the end user will change, prior approval/license from the Chinese government theoretically should be obtained. Similarly, while the term "in-country transfer" is not specified in the ECL, the change of end user would require prior approval from the Chinese government. Otherwise, the foreign importer and original end user would risk being placed on a restricted parties list. It is also a breach of the commitment as provided in the end-user certification "[w]e guarantee that we will not transfer the above-said . . . (commodity name) to any third party without the consent of the Chinese government."

(b) Intangible Transfer of Technology and "Deemed Export"

Under the current export control regimes, intangible technical information is regulated under both dual-use export controls and non-dual-use technology controls. The ECL also expands the scope to "deemed export" of dual use technologies. The term "deemed export" is not specified in the law, but is implied under the definition of "export control," which reads as "the provision of controlled items from PRC citizens and entities to foreign individuals and entities." Thus, the provision of controlled technologies to a foreign person within China is now regulated and would require an export license. This has created substantial challenges to multinational companies operating research and development in China.

Another issue often left unchecked is the export of non-dual-use technologies. Under the RATIE, non-dual-use technologies are classified into three categories: prohibited technologies, restricted technologies, and nonrestricted technologies. Prohibited technologies cannot be exported, while restricted technologies are subject to the export licensing requirements, and nonrestricted technologies can be exported under a system of contract registration. "Export" means transfer of technologies from the territory of the PRC to outside of PRC through ways including patents transfer, technology transfer, transfer of patent application rights, grants of patent licenses, and so on. It is noteworthy that, unlike the control over dual use technologies, for non-dual-use technologies that fall under the prohibited or restricted category, the transfer or licensing of the patents is either prohibited or requires export approval and license, even when the patented technology information is already in the public domain. Companies are advised to consult the Technologies Catalogue before the transfer or licensing of technologies. Please see detailed discussions at Section 15.5(c).

(c) Practical Issues Related to Export Control Clearance

As export controls are practically enforced by Customs at the border, and the China Dual Use Catalogue also provides HTS codes of dual-use items, although the HTS codes are only for reference purposes and the description in the Catalogue shall be dispositive, the first check item for Customs is the HTS codes. As such, it is very important to properly classify the items. When Customs sees the HTS code is listed in the Catalogue on a given export, it would expect to see the export license. If the exporter believes their products do not fit in the description of controlled items in the Catalogue, they can contact MOFCOM and request the authority to issue a noncontrolled opinion.

The new ECL further provides that, when an export license is not provided but Customs has evidence indicating the items being exported might be controlled items, Customs shall question the exporter, and can request the state export control administration authorities to verify and confirm. The export would be suspended during such questioning or verification.

(d) Recordkeeping

The recordkeeping period for export of controlled items is five years from the date of export.

(e) How to Be Compliant When Exporting to China

It should be noted that the dual use items controlled for importing into China are different than those controlled for exporting from China. In addition to encryption items (discussed separately in Section 15.12), there are three categories of import-controlled dual use items: (1) controlled

chemicals related to chemical weapons (same as Category 4 under the export-controlled items list), (2) controlled precursor chemicals related to drugs (same as Category 7 under the export-controlled items list), and (3) certain radioactive isotopes.

Besides the general compliance requirements on importation under the Customs laws and regulations, for import-controlled items, import licenses are required. As such, prior to exporting foreign items to China, the following steps are recommended:

- Determine whether the items are subject to import controls, and determine the correct HTS classification;
- Verify the end user and end use to make sure they are for civil purposes, and confirm whether the importer/end user has the right facility for using the controlled items for civil purposes and is capable of exerting sufficient control;
- Request the Chinese importer to secure the import license when applicable, and request a copy of such license;
- Confirm no red flags in terms of shipping routes, destination, and payment terms;
- Properly describe or characterize the item on all documents and labels or packaging to provide sufficient information for the authority to easily understand the nature of the item, and even indicate the wording “import controlled dual use item” on the paperwork;
- Maintain proper documentation and records;
- Do not deal with anyone who requests you to mischaracterize or describe the item in a vague or misleading manner, alter or disguise the labels or packaging, produce documents (contract, invoice, packing list etc.) containing false information.

(f) How to Be Compliant When Exporting Out of China

For exporting controlled items out of China, the exporter of record (or the consignor) is required to obtain a proper export license and abide by applicable export control regulations. The following steps are recommended:

- Determine whether the items are subject to export controls, and determine the correct HTS classification;
- Request an end user and end-use certification, and verify the end user and end use to make sure they are for civil purposes, and confirm whether the importer/end user has the right facility for using the controlled items for civil purposes and is capable of exerting sufficient control to determine no diversion risks;
- Secure export licenses when applicable;
- Confirm no red flags in terms of shipping routes, destination, and payment terms;
- Properly describe or characterize the item on all documents and labels or packaging to provide sufficient information for the authority to easily understand the nature of the item, and even indicate the wording “export controlled dual use item” on the paperwork;
- Maintain proper documentation and records;
- Do not deal with anyone who requests you to mischaracterize or describe the item in a vague or misleading manner, alter or disguise the labels or packaging, produce documents (contract, invoice, packing list etc.) containing false information;
- Implement effective internal trade compliance and control program;
- When in doubt, suspend the transaction or shipment, and consult an internal compliance officer or external experts;
- Once the sensitive areas and restricted parties lists are identified, exporter should perform the party screening and maintain the screening documentation.

(g) Key Points in the Draft Export Control Regulation of Dual-Use Items ("the Draft Regulation")

(i) Controlled Items

The Draft Regulation adopts a provision that authorizes the government to regulate the non-dual-use item (not currently included in the control lists) under the export control regime if the item is related to national security and interest. This provision provides an authorization for the Chinese government to further regulate items (such as high-tech items or emerging technology) other than items related to nuclear WSD under current export control regime.

(ii) Export Control Classification

The Draft Regulation stipulates that items included in the control list will be assigned a new control classification number. HS codes are currently used to identify dual-use items included in the current Dual Use Catalogue. The Draft Regulation does not specify how control classification numbers would be assigned. It might be similar to the ECCN under the U.S. and EU export control regimes.

(iii) Temporary Control

The Draft Regulation also clarifies the application of the Temporary Control System. Article 14 provides that before the expiration of each term of temporary control, MOFCOM and other relevant authorities should make an assessment and determine whether to terminate or extend the temporary control, or officially include the temporarily controlled item in the Dual Use Items Export Control List.

(iv) Country-based Risk Level

Article 8 of the ECL authorizes MOFCOM, together with MFA and other relevant departments, to conduct a risk assessment on the destination country/area that dual-use items are exported to and determine the different risk level accordingly. The export control restrictions will vary based on different risk level of destinations, which might be similar with the Commerce Country Chart under U.S. export controls. The following factors might be taken into account in the risk assessment: (1) the impact on national security and national interests, (2) the fulfillment of China's international obligations; (3) the needs of foreign policy, (4) China's cooperation with other countries in the area of export control, and others.

(v) Restrictions to Restricted Parties

Article 31 of the Draft Regulation provides restrictions that could apply to the restricted parties:

- Prohibition on the export of all or parts of controlled dual-use items;
- Denial of relevant export license applications;
- Retraction of export licenses issued prior to the designation;
- Suspension of export activities not yet completed;
- Other necessary measures.

(vi) Licensing

One notable change in the Draft Regulation is the abolition of the Dual Use Operation Registration System. If the Draft Regulation takes effect, exporters will no longer need to apply

for the Dual Use Operation Registration Certificate before they apply for an export license for dual-use items (exporters of nuclear items and munitions are still required to obtain a Registration Certificate before they apply for export licenses). With this change, the application process will be simplified for exporters of dual-use items to obtain the required export licenses.

The Draft Regulation also provides detailed rules regarding general license and license exceptions. For a general license, the Draft Regulation shortens its period of validity to two years and specifies the conditions an exporter should meet in order to be eligible for general licenses:

- The exporter must have an effective and operating export control compliance system;
- The exporter must have been in the business of exporting dual-use items for two or more years, and have successfully obtained multiple export licenses for dual-use items;
- The exporter must have steady sales and regular end users;
- Other conditions as imposed by MOFCOM and other relevant authorities.

After obtaining the general licenses, the exporter is required to report periodically to the MOFCOM and relevant authorities about how the licenses are used and accept checks and inspections from the authorities.

Other than general licenses, Article 25 of the Draft Regulation also stipulates four circumstances under which no license is required to export dual-use items:

- The export of items imported for inspection, repair, test, or examination within a reasonable period of time to the place of original exportation;
- The immediate export of items imported for participation in trade shows held in China to the place of original exportation, with their conditions intact;
- The export of components of civil aircraft for repair;
- Other circumstances as determined by MOFCOM and relevant authorities.

If an export of dual-use items falls under these circumstances, the exporter need only register with the authorities before export.

However, despite all these conveniences, certain exporters are not eligible for general license or license exceptions: (1) if they were subject to administrative or criminal penalties due to export violations within the last five years; or (2) if they were called in for an enforcement discussion or in receipt of a warning letter in the past year because their activities or actions pose a risk of export violations; or (3) for other reasons as determined by MOFCOM and relevant authorities.

(vii)End-Use and End-User Control

Article 10 of the Draft Regulation proposes the promulgation of an Administrative Regulation for End-Use and End-User Certification, which could potentially include the circumstances under which MOFCOM and other relevant authorities are authorized to issue an “End-Use and End-User Certification” to the government of other countries and regions upon request. Reciprocally, MOFCOM could also request such certification to be issued by the government agencies of other countries in which the end-user is located.

In the certification, end-users are required to certify and undertake that it is the end user of the exported item and will only use the item for the end uses described in the certification. Meanwhile, it should be noted that not only the end user but also the exporter is required to abide by these certifications and undertakings. In case of any violations, the exporter and the end user could be subject to forfeiture and be fined for more than five to ten times the illegal income

if their income exceeds RMB 200,000, and for RMB 200,000 to two million, if their income is less than RMB 200,000.

(viii)Reporting Obligations

The Draft Regulation sets forth four reporting obligations for exporters and third-party service providers. For exporters, they are required to report to relevant authorities in the following three situations:

- Within three years of exportation, the exporter finds that the exported items might pose the risk of (1) endangering national security and interests; (2) being used for the design, development, production, and use of weapons of mass destruction and their means of delivery; or (3) being used for terrorism purposes.
- The exporter finds that the documents proving the end user or end use of the exported items are forged, outdated, or obtained with illicit methods such as fraud or bribery.
- The exporter finds that the end use or end user of the exported item might change or have already changed.

For third-party service providers, they are required to report if they come to be aware of export violations committed by the exporters they serve. If the relevant parties fail to fulfill their reporting obligations, they could be subject to warnings or fines between RMB 100,000 and 300,000 if their violations are deemed to be egregious.

(ix) Voluntary Disclosure and Internal Compliance System

Article 52 of the Draft Regulation provides that exporters and third-party service providers could be eligible for a lighter or mitigated penalty if they meet any of the following conditions:

- Taking actions to proactively reduce or eliminate negative consequences resulting from their violations;
- Being forced or cajoled into committing the violations;
- Voluntarily disclosing violations that are not discovered by the relevant authorities;
- Having made contributions in their cooperation with relevant authorities to combat export violations;
- Establishing and maintaining an effective internal compliance system that prevented the spread of negative consequences.

15.12 Encryption Controls

(a) General Comments and Legislation Summary

(i) Encryption Law

On October 26, 2019, China passed the Encryption Law, which went into effect on January 1, 2020. Before the enactment of the Encryption Law, the relevant regulation regarding the commercial encryption was Regulations for the Administration of Commercial Encryption (hereinafter “Regulation”). According to the Regulation, restrictions on foreign commercial encryption products were primarily as follows:

- Encryption products imported from overseas are only allowed for foreign invested companies for internal use purpose and cannot be sold in China.

- Import of encryption products or equipment containing encryption technology requires an import license.

The release of the Encryption Law officially eases these restrictions on commercial encryption products. The most noteworthy change is the deregulation of commercial encryption, specifically defined under Article 28 of the Encryption Law:

- "Mass consumer products" exception. Commercial encryption used in mass consumer products is not subject to import/export licensing systems.
- Export/import licensing control. For products that involve national security and public interest and provide encryption protection functions, an import approval is required. For export of products that involve national security and public interest or are required by China's international responsibility, an export approval is required.

(ii) Encryption Catalogue: (January 1, 2021 to Now)

The list of commercial cryptography subject to import licensing and export controls ("Encryption Catalogue") was published by MOFCOM, Customs, and the State Cryptography Administration (SCA) on November 26, 2020. Items listed in the Encryption Catalogue require licenses during importation and exportation. If items are not listed in the Encryption Catalogue, there is no need to apply for an import/export license. See detailed discussions at Section 15.12(c).

(b) Classification and Definition for Encryption Products

(i) "Cryptography"

According to Article 2 of the Encryption Law, the "cryptography" refers to technology, products, and services using methods such as a specific transformation for encrypted information protection and security authentication.

(ii) Three Types of Encryption Control

The Encryption Law provides a new classification system of encryption: core encryption, ordinary encryption, and commercial encryption. Core encryption and ordinary encryption are regarded as "state secret" and are strictly regulated, while commercial encryption is deregulated, and development of commercial encryption is encouraged.

The Encryption Law itself does not provide a definition for a "commercial encryption" product. However, the definition from the Regulation is still effective and can be a reference. According to the Regulation, "commercial encryption" means encryption technology and encryption products used to protect by encryption, or to carry out security certification for, information that does not involve state secrets.

(iii) "Mass Consumer Encryption Products"

Another tricky issue is what exactly "mass consumer products" refer to as commercial encryption used in mass consumption products is not subject to import/export licensing systems based on Article 28 of the Encryption Law.

The term "mass consumer products" has not been defined in the Encryption Law or other regulations. The only official reference can be found in a Q&A published on SCA website on April 2, 2020,[24] which provides a definition that "commercial encryption employed in mass

consumer products refers to those products or technologies that are available for the public to acquire from regular retail channels without restrictions, and for their personal use, and the encryption function of which cannot be easily modified." It is the SCA's position that "as the commercial encryption in mass consumer products has relatively low risk to national security and public interests and controllable, no licensing requirements can largely reduce the impact over trade. This is conformed to the common practice in international community as well as the practice in the administration in China." Such interpretation can be taken as SCA's official interpretation with legal binding effect, although not written in the form of regulations.

In practice, the absence of a clear definition of "mass consumer encryption products" seems not to be a prominent issue. Based on our experience, we understand from our consultation with relevant authorities that the only criteria for determining whether an import or export license is required is the listing in the Encryption Catalogue. If items are not listed in the Encryption Catalogue (described in detail in Section 15.12(c)), there is no need to apply for an import/export license. The logic behind this practice is that the authorities have considered the technical parameters of mass consumer products, based on which the authorities have excluded any mass consumer products from the lists. In case exporters/importers believe any products fall in the Catalogue might fit the definition of mass consumer product, they should consult with the authorities for their determination.

(c) Encryption Licensing Requirements

(i) Import/Export License Requirement

According to the Encryption Law, commercial encryption used in "mass consumer products" and components and software that do not have the technical parameters in the Encryption Catalogue are not subject to import/export licensing systems. For products that involve national security and public interest and provide encryption protection functions, an import approval is still required. For export of products that involve national security and public interest or is required by China's international responsibility, an export approval is required. It is noted that the export of encryption items is now covered under the new ECL. The table that follows includes the items listed in the Encryption Catalogue.

(A) Export Control List of Commercial Encryption

1. System, equipment, and parts			
No.	**Item**	**Description (Dispositive Factor)**	**HS code (Reference Only)**
1	Security chips	The integrated circuit chips that partially or fully realize the functions of cryptographic calculation, key management, random number generation, etc., and has one of the following characteristics: (1) Includes symmetric cryptographic algorithms with key lengths of 64 bits or more, asymmetric cryptographic algorithms based on integer factorization with key lengths of 768 bits or more, or asymmetric cryptographic algorithms based on elliptic curves with key lengths of 128 bits or more, that are all specially applying to the area of electric power, taxation, public security, finance, etc. (2) Includes symmetric cryptographic algorithms with key lengths of 64 bits or more, asymmetric cryptographic algorithms based on integer factorization with key lengths of 768 bits or more, or asymmetric cryptographic algorithms based on elliptic curves with key lengths of 128 bits or more, and the encryption and decryption rate of symmetric cryptographic algorithms is 10	8542311910 8542319010

		Gbps or more, or the signature rate of asymmetric cryptographic algorithms is 50,000 times per second or more.	
2	Cryptography machine (cryptography card)	The equipment (including cryptography card) whose primary function is to realize cryptographic calculation, and which has both of the following characteristics: (1) Includes symmetric cryptographic algorithms with key lengths of 64 bits or more, asymmetric cryptographic algorithms based on integer factorization with key lengths of 768 bits or more, or asymmetric cryptographic algorithms based on elliptic curves with key lengths of 128 bits or more; (2) Encryption and decryption rate of symmetric cryptographic algorithm is 10 Gbps or more, or the signature rate of asymmetric cryptographic algorithms is 50,000 times per second or more.	8543709950
3	Encrypted VPN equipment	The equipment that has IPSec/SSL VPN as its primary function and has both of the following characteristics: (1) Includes symmetric cryptographic algorithms with key lengths of 64 bits or more, asymmetric cryptographic algorithms based on integer factorization with key lengths of 768 bits or more, or asymmetric cryptographic algorithms based on elliptic curves with key lengths of 128 bits or more; (2) Communication rate under encryption is 10 Gbps or more.	8517622920 8517623920
4	Products of key management	A server-side equipment used for management functions such as generation, distribution, storage, etc., of symmetric or asymmetric keys, and having both of the following characteristics: (1) Includes symmetric cryptographic algorithms with key lengths of 64 bits or more, asymmetric cryptographic algorithms based on integer factorization with key lengths of 768 bits or more, or asymmetric cryptographic algorithms based on elliptic curves with key lengths of 128 bits or more; (2) Supports managing 10,000 objects or more.	8543709950
5	Special-purpose equipment	Includes symmetric cryptographic algorithms with key lengths of 64 bits or more, asymmetric cryptographic algorithms based on integer factorization with key lengths of 768 bits or more, or asymmetric cryptographic algorithms based on elliptic curves with key lengths of 128 bits or more , that are all specially applying to the area of electric power, taxation, public security, finance, etc.	
6	Quantum cryptography equipment	The equipment that use quantum technology to realize cryptographic functions based on quantum mechanics and cryptography.	
7	Cryptography analysis equipment	Analysis equipment used to hack, weaken, or evade cryptography technology, products, or systems.	

2. Equipment for test, inspection, and production			
No.	**Item**	**Description (Definitive Factor)**	**HS code (Reference Only)**
8	Equipment for cryptography development or production	Specially designed for the development or production of items 1 to 7.	
9	Equipment for test and verification of cryptography	Equipment specially designed to measure, test, evaluate, and verify items 1 to 7.	
3. Software			
No.	**Item**	**Description (Dispositive Factor)**	**HS code (Reference Only)**
10	Software		

	specifically designed or modified for the development, production, or use of items 1 to 9.		
4. Technology			
No.	**Item**	**Description (Dispositive Factor)**	**HS code (Reference Only)**
11	Technology specially designed or modified for the development, production, or use of items 1 to 10.		

(B) Import License List of Commercial Encryption

No.	Item	Description (Dispositive Factor)	HS code (Reference Only)
1	Encrypted telephone	Landline telephones or mobile phones that use cryptography technology to realize the protection of data transmission and other functions, including symmetric cryptographic algorithms with key lengths of 64 bits or more, asymmetric cryptographic algorithms based on integer factorization with key lengths of 768 bits or more, or asymmetric cryptographic algorithms based on elliptic curves with key lengths of 128 bits or more.	8517110010 8517180010
2	Encrypted fax machine	Fax machines that use cryptography technology to realize the protection of data transmission and other functions, including symmetric cryptographic algorithms with key lengths of 64 bits or more, asymmetric cryptographic algorithms based on integer factorization with key lengths of 768 bits or more, or asymmetric cryptographic algorithms based on elliptic curves with key lengths of 128 bits or more.	8443311010 8443319020 8443329010
3	Cryptography machine (cryptography card)	The equipment (including cryptography card) whose primary function is to realize cryptographic calculation, and which has both of the following characteristics: (1) Includes symmetric cryptographic algorithms with key lengths of 64 bits or more, asymmetric cryptographic algorithms based on integer factorization with key lengths of 768 bits or more, or asymmetric cryptographic algorithms based on elliptic curves with key lengths of 128 bits or more; (2) Encryption and decryption rate of symmetric cryptographic algorithm is 10 Gbps or more.	8543709950
4	Encrypted VPN equipment	The equipment that has IPSec/SSL VPN as its primary function and has both of the following characteristics: (1) Includes symmetric cryptographic algorithms with key lengths of 64 bits or more, asymmetric cryptographic algorithms based on integer factorization with key lengths of 768 bits or more, or asymmetric cryptographic algorithms based on elliptic curves with key lengths of 128 bits or more; (2) communication rate under encryption is 10 Gbps or more.	8517622920 8517623920

(d) Export/Import Licensing Procedure

Once the imported/exported items are determined to be controlled by the Encryption Catalogue, importers/exporters shall follow the same license application procedure for dual-use items.[25]

The import/export license application is to be filed to MOFCOM through the provincial commerce department; the following documents shall be submitted along with the application:

- Identification of legal representative, manager and agent of the applicant
- Copy of the contracts or agreements
- Technical notes of the commercial encryption
- End-user and end-use certificates
- Other materials required by MOFCOM

MOFCOM shall review these listed application documents in conjunction with the SCA and other relevant departments, and within the statutory period issue a decision to permit or deny the application. Import and export licenses for dual-use items and technology will be issued, if the permit has been granted by MOFCOM.

While the restrictions on import, sales, and use of foreign encryption products are removed, the Encryption Law imposes mandatory testing or certification requirements on those commercial encryption products that may affect "national security, national welfare or public interests." Such products would be included in the Catalogue of Critical Network Equipment and Dedicated Cybersecurity Products ("Catalogue"), and should pass the testing and certification conducted by a qualified agency according to the Cybersecurity Law. However, the description in the Catalogue is broad and vague.

(e) Penalties for Violation of Encryption Regulations

The Encryption Law provides the penalties for violations relating to import and export as follows:

- When an operator of critical information infrastructure imports or exports commercial cryptography in violation of relevant import licensing or export control measures, such violation would be subject to administrative penalties by MOFCOM or the Customs in accordance with relevant laws and regulations (i.e., the Export Control Law, please see Section 15.9).
- For anyone who sells or provides commercial cryptography products or services that have not undergone security certification or that have failed to pass security certification, such violation may be subject to administrative penalties, ranging from a warning, an order to rectify, to cease the illegal act, confiscation of illegal products and forfeiture of illegal income, as well as a fine (in the amount of one to three times of the illegal income when the illegal income exceeds RMB 100,000; or in the amount of RMB 30,000 to 100,000 when there is no illegal income or the illegal income is less than RMB 100,000).
- Any violation of the law that constitutes a crime shall be criminally penalized in accordance with the Criminal Law.

15.13 Unreliable Entity List

MOFCOM issued an order promulgating the Provisions on the Unreliable Entity List (the Provisions) on September 19, 2020, effective immediately. The idea of designating foreign entities onto some blacklists was first introduced on May 31, 2019, right after the Chinese technology company Huawei was designated onto the Entity List by the U.S. government.

The Unreliable Entity List (UEL) creates new and unique challenges and dilemmas for some multinational companies doing business with and in China, particularly when foreign companies

have to comply with economic sanctions and export controls under foreign jurisdictions in their dealings with Chinese entities. The UEL is a powerful tool for the government and will have a profound impact on foreign trade and investment. It even has the potential to have some extraterritorial effect, as this UEL mechanism is designed to protect Chinese companies' interests.

On Feb. 16, 2023, Lockheed Martin Corporation and Raytheon Missiles & Defense were designated to the UEL for endangering the national sovereignty, security, and development interest of China.

(a) Why This?

It's all about Huawei, and MANY OTHERS.

This idea was first introduced on May 31, 2019, after Huawei was placed on the BIS Entity List on May 15, 2019, one of the many restricted party lists administered by the U.S. government, and was thus barred from obtaining certain items and technologies subject to U.S. export control regulations. Over the past decade, in the course of the trade war and now the technology war between the United States and China, several hundred Chinese entities have been put onto these restricted party lists, such as Specially Designated Nationals and Blocked Persons (SDNs), and they have been subject to economic sanctions and export control measures imposed by the U.S. government. As the U.S. government is stepping into more sensitive areas like Hong Kong, Xinjiang, and the South China Sea, and has put some Chinese senior government officials and many large state-owned enterprises onto the list, sentiment in China has grown to the point where the government needs to take countermeasures against the United States.

(b) How Effective Could It Be?

When the UEL idea was first rolled out, the international community appeared worried yet skeptical. The government said it will "take any necessary legal and administrative measures against the designated unreliable entities; and the public will be alerted to be cautious to do business with those entities."[26] No more specific measures were laid out and nothing happened for a few months. It was thought to be a "tiger without teeth."

However, with the enactment of the Provisions, it seems to have real "teeth." The Provisions set out a menu of measures the government can choose from, such as:

- Restricting or prohibiting the foreign entity from engaging in China-related *import or export* activities;
- Restricting or prohibiting the foreign entity from *investing in China*;
- Restricting or prohibiting the foreign entity's relevant personnel or means of transportation from *entering into China*;
- Restricting or revoking the relevant personnel's *work permit*, status of stay, or residence in China;
- Imposing a *fine* of the corresponding amount according to the severity of the circumstances; and
- *Other* necessary measures.

The Provisions state that when making a designation, the authority may also issue "an alert about the risks of conducting transactions with the said foreign entity." Be mindful that the

phrase "*other necessary measures*" may be more severe than it sounds. It provides the authorities with wide discretion.

As the Provisions explain, the UEL mechanism is "a working mechanism composed of relevant central departments to take charge of the organization and implementation of the Unreliable Entity List System." The relevant central departments are unspecified but would very likely include the Ministry of Finance and the People's Bank of China. The Provisions also state that "the measures provided . . . shall be implemented according to the law by the relevant departments in light of their respective duties and functions." So, it would not be surprising if the designated UEL is faced with other unspecified measures, or even "extra efforts" at a different level of authority.

Many questions remain unanswered since its enactment two years ago. Such as, does "investing in China" mean new investments, or could it cover existing investments in China? By one interpretation, "invest*ing*" may mean an investment being contemplated, so it could mean a new investment rather than an existing investment.

Another issue that is unclear is whether the measures would be applied to affiliated companies. Under the U.S. sanction, OFAC has a 50 percent rule under which subsidiaries that are directly or indirectly owned 50 percent or more by one or more SDNs are also blocked entities. If a foreign entity is designated, would its affiliates/subsidiaries in other countries, or even in China, also be subject to such measures? Would a subsidiary in China be allowed to continue its business with the designated foreign owner? Would a new acquisition or investment by an existing FIE be deemed as an investment by the ultimate foreign owner? There are no clear answers for now. It is hoped that the government will add some clarity over time, or at least be more specific in their designation decisions.

(c) What Could Trigger the UEL, and How Far Can It Reach?

From the outset, the Provisions set forth that:

> The State shall establish the Unreliable Entity List System, and adopt measures in response to the following *actions taken by a foreign entity in international economic, trade and other relevant activities*:
>
> (1) *endangering* the national sovereignty, security or development interests of China;
>
> (2) *suspending normal transactions* with an enterprise, other organization, or individual of China or *applying discriminatory measures* against an enterprise, other organization, or individual of China, which violates normal market transaction principles and causes serious damage to the legitimate rights and interests of the enterprise, other organization, or individual of China.

It is noteworthy that such actions are not limited to activities in China. So, the government can exert long-arm jurisdiction over actions taken outside of China.

Any activities that are viewed as endangering the national sovereignty, national security, or development interests of China could invoke the UEL designation. It is worth recalling that the MFA made several announcements in July 2019 and July 2020 that the government would impose sanctions over certain U.S. companies involved in arms sales to Taiwan. It now seems that the UEL designation could be one of the measures the government may opt to take, as such actions may well be viewed as endangering the national sovereignty of China.

Similar to the International Economic Emergency Power Act (IEEPA) in the United States, which grants the U.S. President wide authority to impose sanctions and trade control measures in order to "deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of

the United States," the Provisions provide legal authorization for the government to impose measures on anyone that acts contrary to the interests of China.

Putting aside the long-arm jurisdiction and broad authorizations, the Provisions specifically address scenarios wherein foreign entities are *suspending normal transactions* or *applying discriminatory measures* against a [Chinese person], which violates normal market transaction principles and causes serious damage to the legitimate rights and interests of the [Chinese person]. This clearly relates to the Huawei situation and other Chinese persons (entities or individuals) who have been placed on the Entity List or the SDN list by the U.S. government, and thus are subject to U.S. economic sanctions and/or export control restrictions, or other restrictions (such as the U.S. CBP's Withhold Release Order). Such Chinese persons are essentially cut off from the supply chain, for example, unable to obtain U.S. items (e.g. Huawei), not able to access the U.S. market (such as fabrics/clothing containing Xinjiang cotton), or cannot deal with non-U.S. companies (with secondary sanction exposure) or in U.S. dollars (when they are designated as an SDN). This UEL mechanism has been made to retaliate and deter to help protect the interests of Chinese companies in those situations. It would place multinational companies (not just U.S. companies) in a very difficult situation.

In a case where someone is sanctioned by the U.S government (either under sanction programs or export controls) by being placed on the Entity List, items subject to the U.S. Export Administration Regulations (EAR) cannot be supplied to such a person without a license from the U.S. government. Otherwise, it is a violation of U.S. law. In the case of fabrics/clothing containing cotton from Xinjiang, the products could be subject to detention under a Withhold Release Order issued by U.S. Customs. For these reasons, foreign counterparties would have to comply with U.S. law when the items are subject to the EAR or are entering the U.S. market. Such compliance would require them to discontinue the supply or the purchase from a Chinese entity sanctioned by the U.S. government if no license can be obtained. With this UEL mechanism, complying with U.S. law in such a situation could possibly trigger a UEL designation. Once designated, foreign companies could be cut off from Chinese supply chains, meaning that sourcing from China or supplying into the Chinese market would be impossible.

(d) How to Navigate the Dilemma

There is no perfect solution.

In making the decision of UEL designation, the authority would look into factors including (1) the degree of danger to the national sovereignty, security, or development interests of China; (2) the degree of damage to the legitimate rights and interests of [Chinese persons]; (3) *whether being in compliance with internationally accepted economic and trade rules*; and (4) other factors that shall be considered.

If "suspending normal transactions" is a must-do under U.S. law, then the only possible argument is "being in compliance with internationally accepted economic and trade rules." Arguments such as the fact that "designation" would do more harm to other Chinese interests (e.g., other Chinese companies still need American chips) could be helpful in negotiating with the government to impose as few restrictions as possible.

The third factor, "*whether being in compliance with internationally accepted economic and trade rules*" is vague. The previous factor "whether the actions of the entity are not for commercial purposes and are in violation of market principles and contractual obligations," as explained by MOFCOM officials in May 2019 when the UEL concept was first introduced, is

also vague, but it is at least easier to comprehend. In any event, being obliged to comply with U.S. laws is definitely not among the "internationally accepted economic and trade rules."

So the burden is for the foreign entity to demonstrate if there is any cause existing under any "*internationally accepted economic and trade rules*" (such as WTO rules, UN Convention on Contracts of International Sales of Goods, INCOTERMs, or perhaps the multilateral control regimes in which China is a member state, such as the Nuclear Suppliers Group) that could serve as justifiable grounds to suspend the transaction. A few things may be worth considering:

- Carefully examine the compliance requirements. Try not to over-comply.
- Contract terms. Sanctions or trade control clauses are very common in contracts drafted by sophisticated multinational companies. One suggestion would be to think it through twice. Indicating that the items are subject to EAR and requesting representations and warranties with respect to the end user/end use, and non-diversion would be unlikely to become an issue. It could be problematic to directly state the events, such as the buyer becomes an SDN or is placed on the Entity List by the U.S. government as a ground for terminating the contract. No-obligation to supply at discretion would be a good clause to include in the contract. Revisit the governing laws and the dispute resolution clauses for better protection in case of being sued for commercial losses.
- Establish affirmative defenses. Building up a case of a breach of contract by the counterparty or citing some other cause (such as an inability to obtain a supply of materials) when deciding to terminate the contract. In addition, demonstrating efforts to seek licenses from the U.S. government could be helpful.
- Consider a Plan B, especially for major deals. Both sides of the deal should carefully review the MAC (Material Adverse Change) or MAE (Material Adverse Effect) clause, as well as exit plans, to accommodate this UEL situation.
- Maintain a low profile when the business relationship is suspended. Developing a crisis management protocol is recommended.

(e) What's the Designation Procedure? What Needs to Be Prepared for Investigations?

Unlike the U.S. government SDN and Entity List designation procedures, which typically do not allow the non-U.S. party to comment, the Chinese designation process provides such an opportunity to the foreign entity to comment on their proposed designation:

- The Provisions state that the authority will make an announcement when it opens an investigation.
- During the course of the investigation, the foreign entity can present its arguments.
- The Provisions further provide that the authority may suspend or terminate the investigation based on the actual circumstances, and resume when the facts warranting the suspension change materially. This seems to suggest that there might be an opportunity to negotiate and reach a settlement.

According to the Provisions, the authority can self-initiate the investigation process, or initiate the investigation "upon suggestions and reports from relevant parties." So, counterparties may exploit this as leverage if the parties are in dispute.

During the course of the investigation, the authority can "inquire the relevant parties, consult or copy the relevant documents and materials, and take other necessary means."

Note that an investigation is not always a must-do procedure before the designation. The Provisions also provide that, "[w]here the facts about the actions taken by the relevant foreign entity are clear, the working mechanism may, by taking into overall consideration the factors specified in Article 7 of these Provisions, directly make a decision on whether to include the relevant foreign entity in the Unreliable Entity List; if a decision is made to include in the Unreliable Entity List, an announcement shall be made."

15.14 Blocking Rules

MOFCOM recently enacted the Chinese "Blocking Statute"—The Rules on Counteracting Unjustified Extra-territorial Application of Foreign Legislation and Other Measures (the "Blocking Rules"), which became effective on January 9, 2021. These Blocking Rules have raised questions and concerns among various industries in China and around the globe. The Blocking Rules are drafted in a vague and confusing way, and could be interpreted broadly. They therefore have the potential to be used as a powerful tool for the government to intervene in international business.

(a) What Could Be Blocked?

The Blocking Rules do not specify any particular foreign laws and measures as the EU blocking statute does. Instead, the Blocking Rules essentially adopt a two-prong test: (1) whether the foreign laws and measures have unjustified extraterritorial application, and (2) whether such foreign laws and measures unjustifiably prohibit or restrict transactions between Chinese persons with third-country persons.

As to the first prong, under Article 6, the Blocking Rules set forth subjective criteria for determining whether any foreign law and measures have unjustified extraterritorial application, such as the law and measures are not in line with international law and norms; have a potential impact over Chinese sovereignty, security, and interests; or have a potential impact over Chinese persons' lawful rights and interests. These subjective criteria leave a lot to the government's discretion.

As to the second prong, such foreign laws and measures should have the effect to "prohibit or restrict transactions between Chinese persons with third country persons." This test would exclude those foreign laws and measures that would impose prohibitions only to certain nationals, for example, the U.S. Executive Order 13959, which prohibits U.S. persons from transacting publicly traded securities of certain Chinese companies. EO 13959 does not "prohibit or restrict transactions between Chinese persons with third country person," and therefore should not be blocked.

U.S. secondary sanctions appear to be a target of the Blocking Rules. For example, U.S. secondary sanctions on Iran, Russia, North Korea, and Venezuela can be imposed with extraterritorial effect even when no part of the conduct has any U.S. nexus. However, given the vagueness and flexibility of the Blocking Rules, they could also be interpreted in a broader way to cover certain "primary sanction" scenarios where transactions in question were between non-U.S. persons but there was U.S. nexus (such as involving U.S. dollars or U.S. banking system, or U.S. items), as well as export controls scenarios where transactions involving re-exports or in-country transfer in a non-U.S. country or involving items made outside of the United States but containing U.S. controlled content above the de minimis amount or items developed or produced by utilizing certain U.S. technologies (the U.S. foreign direct product rules).

(b) What Transactions Are Covered?

The phrase "prohibit or restrict transactions between Chinese persons with third country persons" under Article 2 raises many questions as to whether the Blocking Rules only apply to transactions between Chinese persons with third-country persons. One narrow interpretation is that it only covers transactions between Chinese persons and third-country persons. A broader interpretation, which makes more sense, is that transactions between Chinese persons and Chinese persons are also covered (and indeed it is the primary concern of the Chinese government). In reality, many Chinese persons have to terminate business with another Chinese persons subject to sanctions or export controls restrictions. If that is left out of the scope, the purpose of the Blocking Rules would be defeated.

In addition, at one point MOFCOM had clarified that under Article 9, a Chinese person can sue another Chinese person. This clarification (although later removed from its published Q&As) indicates that the government intends to apply the Blocking Rules to transactions between Chinese persons. As such, these broader applications could be very likely.

(c) Obligation of Reporting and Penalties for Failing to Report

Chinese citizens, legal entities, and other organizations ("Chinese Persons") should abide by the Blocking Rules. The Blocking Rules cover all types of entities in China, such as incorporated companies, partnerships, foreign invested companies in China (including joint ventures of foreign companies with Chinese companies, or wholly owned subsidiaries of foreign companies), branches or offices of foreign entities. Meanwhile, although it has not been officially clarified, Hong Kong persons are not regarded as Chinese Persons for the purpose of the Blocking Rules.

Chinese Persons are obligated under Article 5 to report to MOFCOM within 30 days of encountering prohibitions or restrictions by such foreign laws and measures as defined under Article 2. Failure to report could lead to certain administrative punishments, such as warnings, orders to rectify, and fines (the range is not specified by the Blocking Rules itself, but under the Administrative Punishment Law the maximum monetary penalty is RMB 30,000). However, it is unclear which party has the obligation to report. A broader interpretation is that both transacting parties have the reporting obligation.

Please also note that such reporting obligation is not contingent on whether there is any MOFCOM prohibition order in place. The threshold for one to file a report is effectively very low if one wishes to report, as the Blocking Rules have not defined, or provided illustrative factors to determine, the situation "encountering prohibitions or restrictions." It leaves it to the parties to interpret based on their own situation and position, and the authority again would have its own discretion in such determination.

A tricky question is when exactly the reporting obligation is triggered. MOFCOM has not offered any further explanations so far. Terminating or suspending existing customers or contracts more likely would fall in that situation. Meanwhile, whether declining new customers or new deals rises to the level of "encountering prohibitions or restrictions" is debatable. MOFCOM would have their own views on finding that the parties have "encountered prohibitions or restrictions." When there is an existing contractual commitment, it would be more likely for MOFCOM to determine the parties have "encountered prohibitions or restrictions"; while it would be less likely when there is no existing contractual commitment.

Once MOFCOM issues prohibition orders, Chinese Persons that intend to comply with the requirements under the blocked foreign laws should seek exemptions from MOFCOM before

they can proceed (Article 8). Chinese Persons' acting in complying with the blocked foreign laws without such exemption is a violation, which could lead to certain administrative punishments (same as the above).

(d) Litigation Risks

The Blocking Rules authorize two judicial remedies for Chinese Persons:

- Article 9(a). Chinese Person whose legitimate rights and benefits are damaged as a result of "a party's compliance with the blocked foreign laws [without MOFCOM's exemption]" can bring a lawsuit at court against such "a party" and seek for compensation;
- Article 9(b). If a judgment or award made based upon the blocked foreign laws results in losses to Chinese Persons, such Chinese Persons can bring a lawsuit at court and seek compensation from the "party" that benefited from such judgment or award. In case the "party" refuse to honor Chinese court's judgment, the complainant Chinese Persons can seek to enforce such judgment.

The Blocking Rules do not define the key term "party." One of MOFCOM's published Q&As clarified that the "party" in the Article 9(a) is limited to Chinese persons only, and "party" in the Article 9(b) may include foreign persons. However, this clarification has been removed, which leaves ambiguity on whether foreign persons may face litigation risks under Article 9(a). These judicial remedies theoretically could cover any party to a transaction, such as Chinese, third-country persons, and even U.S. persons. Whether MOFCOM or Chinese courts would implement this judicial remedy remains to be seen.

15.15 Anti-Foreign Sanctions Law

(a) Brief Summary

The Anti-Foreign Sanctions Law was adopted by the Standing Committee of the National People's Congress (NPC) and signed into law by the Chairman of the PRC on June 10, 2021, and became effective immediately.

While this law has sent chills throughout the business community over the past year, and has created irreconcilable compliance issues, this new law is of a nature of reactive and defensive response. It is designed more toward countering foreign sanctions by imposing sanctions over members of foreign government/administration, NGOs, or anyone who acts contrary to Chinese national security or interests, rather than targeting foreign companies in the private sector (although litigation exposures could exist between private parties).

In a nutshell, it is a groundbreaking law that (1) provides an overarching legal authorization for the government to take measures to counter foreign "discriminatory restrictive measures"; and (2) prohibits anyone to implement such "foreign discriminatory restrictive measures (otherwise facing civil litigation risks)." This new law is short and basic and, yet, could be very powerful when fully implemented. As it is intended to be a basic law that lays out high-level principles and provides comprehensive authorizations to the government, how it may be implemented remains to be seen.

(b) What Foreign Measures Are to Be Countered?

The term “foreign sanctions” as included in the title of the law is referred to as “foreign discriminatory restrictive measures” in the main text of the law, which is defined very broadly under Article 3 as “If a foreign country violates international law and the basic norms of international relations, uses various pretexts or according to its own laws to contain and suppress China, takes discriminatory and restrictive measures against its citizens and organizations, and interferes in its internal affairs. . . .”

While the law does not define “foreign discriminatory restrictive measures,”, statements by a senior official of the Legislative Affairs Commission of the Standing Committee of NPC during the Q&A session provide guidance as to the purpose of the law, making it likely that such “foreign discriminatory restrictive measures” would cover:

- Unilateral sanctions on Chinese government agencies and officials and other persons in connection with matters related to Xinjiang, Tibet, Hong Kong, South China Sea, Covid-19, human rights; and
- Other forms that deviate from the basic norms of international law and international relations. It could extend to the long-arm reach of foreign export controls measures. This is also echoed in the China Export Control Law, which at Article 48 provides “If any country or region abuses export control measures to endanger the national security and interests of China, China may take countermeasures.”

(c) Who Is Likely to Be Designated?

The new law primarily targets those foreign persons/organizations that are actively pursuing or involved in enacting the “discriminatory restrictive measures” against China:

- Article 4. Any individuals or organizations that directly or indirectly participate in the formulation, the decision-making, or the implementation of the “discriminatory restrictive measures”;
- Article 5. In addition to the listing under Article 4, the government may also impose countermeasures against (1) spouse and immediate family members of the designated individuals; (2) senior managers of or persons controlling the designated organizations; (3) organizations in which the designated individuals are serving in senior management; (4) organizations subject to the actual control by those designated individuals and organizations, or organizations in which the designated individuals or organizations participate in the establishment or operation.

Besides the preceding primarily targeted persons, the new law does provide a broad authorization under Article 15, which authorizes the government to take countermeasures against any foreign nations, organizations, or individuals that commit, assist, or support acts that endanger the sovereignty, security, and development interests of China. Although it is a broad authorization, it is believed that it is less likely that the government would aggressively take actions under Article 15 against foreign entities or individuals in the private sector. As of February 2023, the counter-sanction list includes two individuals participating in “discriminatory restrictive measures”, who are subject to asset freeze, transaction prohibition and visa ban.

(d) What Could Be the Countermeasures?

Article 6 of the law lists a menu of restrictive measures that the government can choose from, including:

- Visa and entry denial or deportation;
- Sealing, seizing, or freezing assets in China (note that, unlike the assets freezing requirement of OFAC, this does not extend to assets within the control of Chinese persons, e.g., assets at a Chinese overseas banks);
- Prohibiting or restricting transactions or other activities with organizations and individuals in China (note that "in China" is to define the organizations and individuals, but not to limit the transactions in China);
- Other measures as necessary (Be mindful that this type of unspecified restriction could be even more severe. It gives the authority wide discretion.)

These measures are limited to the territory of China, and only entities and individuals within China are required to comply with these countermeasures imposed on the sanctioned persons.

(e) Which of These Measures Is Currently Effective?

It is unclear when the "countermeasures" under this new law might take effect. Specifically,

- **Counter-sanction list.** There have been a number of sanctions announced by the MFA prior to this new law. It is understood that those sanction measures should be implemented immediately when announced. MFA did not cite any legal authorizations when they announced such sanctions; those announcements did not turn into a form of law (e.g., an order or regulations). No formal list of persons subject to such sanctions was published. This new law now eliminates any doubts as to whether it is mandatory to comply with those sanction measures. As the new law now authorizes relevant government agencies to take countermeasures by establishing a list of persons subject to Chinese countermeasures/sanctions, it is anticipated that MFA or other relevant government agencies would reintroduce such sanction measures and publish a formal list of sanctioned foreign persons in the near future in a formal legislative manner. That said, in the absence of such formal list, it would be advisable to follow those sanctions that were already announced. See Section 15.2(f).
- **Article 12.** This new law prohibits anyone from implementing "foreign discriminatory restrictive measures" against Chinese persons under Article 12. Since the law took effect immediately on June 10, 2021, technically, such prohibitions must be followed after June 10, 2021. Article 12 also authorizes Chinese persons to bring a lawsuit in Chinese courts to seek compensation or require the defending party to cease and desist implementing the foreign discriminatory measure. By reading through the law, the term "Anyone" under Article 12 could cover both Chinese and foreign persons. This has created concerns among different sectors, such as, whether the refusal by companies (either Chinese or foreign) to transact with or the decision to terminate contracts with Chinese counterparties designated by U.S. government (such as Entity List, or SDN list) could be viewed as "implementing such foreign discriminatory restrictive measures" and therefore expose companies to potential litigation. It is also important to note that the new law does not authorize any administrative or criminal punishments on anyone who fails to follow this Article 12.

(f) How Does It Interact with the Unreliable Entities List and the MOFCOM Measures?

This new law is enacted by the NPC, which is the highest legislative authority. It has higher authority than MOFCOM's Unreliable Entity List Provision and Blocking Rules, which are departmental administrative regulations.

The UEL Rules and the Blocking Rules are not superseded or nullified by this new law. The new law has specifically provided under Article 13 that: "For conducts endangering our nation's sovereignty, security, or development interests, other necessary countermeasures in addition to those provided for in this Law may be provided for by related laws, administrative regulations, and departmental rules."

While these MOFCOM rules, the UEL Rules, and the Blocking Rules have different purposes and goals, and are tools that can be applied depending on specific circumstances, they could be combined in some scenarios. Meanwhile, note that there might be conflicts as well; for example, it is unclear whether the exemptions under the Blocking Rules would still work under the Anti-Foreign Sanctions Law.

---

1. This chapter is written based on Chinese laws and regulations that are in effect as of July 2022.
2. https://flk.npc.gov.cn/index.html.
3. http://aqygzj.mofcom.gov.cn/article/zcgz/. The new ECL is available at http://aqygzj.mofcom.gov.cn/article/zcgz/fl/202010/20201003008925.shtml.
4. https://www.fmprc.gov.cn.
5. http://www.npc.gov.cn/npc/c30834/202106/d4a714d5813c4ad2ac54a5f0f78a5270.shtml.
6. http://english.mofcom.gov.cn/article/policyrelease/announcement/202101/20210103029708.shtml.
7. http://english.mofcom.gov.cn/article/policyrelease/announcement/202009/20200903002580.shtml.
8. For an example, a recent sanction over two military industrial enterprises can be found at https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202202/t20220221_10644075.html.
9. http://aqygzj.mofcom.gov.cn/.
10. This announcement can be found at https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/t1894670.shtml.
11. The relevant announcements can be found at https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/.
12. http://www.mofcom.gov.cn/article/zwgk/gkzcfb/202212/20221203376668.shtml.
13. http://fms.mofcom.gov.cn/article/a/ae/201911/20191102909472.shtml.
14. http://fms.mofcom.gov.cn/article/a/ae/202008/20200802996641.shtml.
15. The relevant MOFCOM webpages can be found at http://egov.mofcom.gov.cn/xzxksx/18017/.
16. https://ecomp.mofcom.gov.cn/.
17. http://egov.mofcom.gov.cn/xzxksx/18017/minganwuxiang.xls.
18. https://zzyhzm.mofcom.gov.cn.
19. https://ecomp.mofcom.gov.cn/.
20. http://egov.mofcom.gov.cn/xzxksx/18017/minganwuxiang.xls.
21. The relevant MOFCOM webpages can be found at http://egov.mofcom.gov.cn/xzxksx/18017/ and https://ecomp.mofcom.gov.cn.
22. The relevant government webpages can be found at http://www.sastind.gov.cn/n6195634/n6195706/n6195716/n6427863/n6428033/c6429000/content.html.
23. The relevant MOFCOM webpage can be found at http://fms.mofcom.gov.cn/article/b/ah/201508/20150801085455.shtml.
24. http://www.sca.gov.cn/sca/xxgk/2020-04/02/content_1060694.shtml.
25. http://egov.mofcom.gov.cn/xzxksx/18017/.
26. http://www.mofcom.gov.cn/article/zhengcejd/bl/201912/20191202918575.shtml.

16

Export Controls and Economic Sanctions in France

Raphael Barazza - Avocat au barreau de Paris Julien Nava - Sorbonne Law School lecturer

16.1 Overview

What Is Regulated: French export control regulations have been built in parallel in accordance with European laws, with the contribution of international treaties and European management of flows aimed at protecting the European market, combating terrorism and the proliferation of weapons of mass destruction. French regulations are constantly evolving in order to respond to the international trends and standards to which France subscribes.

Thus, there are important rules applicable to dual-use goods as well as military goods. These two lists of controlled goods include the results of intellectual activities (intangible) as well as the export and brokering of real goods and software and certain services. An important issue is to distinguish between the transfer of the technologies and goods within the EU and the actual export, which concerns trade with countries outside the EU.

Where to Find the Regulations: In general, all French laws and regulations are available on the official French-language legal information website.[1] It is important to take into account the more detailed legislation at

the European level on the European Commission's website (in particular regarding dual-use goods and Regulation 2021/821).[2]

Who Is the Regulator: The main export control bodies are the National Agency for the Security of Information Systems (hereafter referred to as ANSSI) for cryptology; the dual-use goods service (Service des Biens Double Usage, or SBDU) of the Ministry of the Economy, Industry and Digitalization for dual-use goods and technology; and the Ministry of Defense (Direction Générale de l'Armement, or DGA) for military goods.

The most sensitive applications are examined by an Interministerial Commission for Dual-Use Goods (CIBDU), chaired by the Ministry of Europe and Foreign Affairs. The French Ministry of Foreign Affairs cooperates with a number of other bodies to provide the necessary support and assistance in the field of export controls.

Foreign trade in arms and military items falls within the competence of the Ministry of Defense, as well as of the Prime Minister and the Interministerial Commission for the Study of War Material Exports (CIEEMG).

The Directorate General of Customs and Indirect Duties (DGDDI) is responsible for customs clearance and customs control of items controlled at the border, including post-clearance customs control and customs audits.

How to Get a License: Exporters wanting to obtain a license need to identify within an internet portal called EGIDE (Interministerial Registration and Management of Export Files).[3] The EGIDE portal allows exporters to file applications for export licenses for dual-use items and technologies. EGIDE enables exporters to securely enter, transmit, and monitor the processing of their license applications and associated documents. Since June 18, 2018, EGIDE has been interconnected with customs online services (DELTA) via said "GUN" (Guichet Unique National) to allow the automated and dematerialized management of exports of dual-use goods subject to export licenses. You will find detailed technical documentation on the GUN page of the prodouane website.[4]

Companies can also submit questions to the SBDU regarding the regime applicable to their goods (the procedure is called *Dossier hors license*—DHL—that is, non-license application).

Key Websites: The site of the French customs is particularly helpful for companies in describing French export control laws: https://www.douane.gouv.fr/. The GUN page of the prodouane website can be found at https://www.douane.gouv.fr/le-guichet-unique-national-du-dedouanement-gun-generalites. Concerning dual-use goods, the portal of the dual-use goods service is more specific: https://sbdu.entreprises.gouv.fr/fr.Concerning goods and technologies related to cryptology, the portal of the National Agency for Information Systems Security is specifically dedicated: https://www.ssi.gouv.fr. Concerning military goods, information can be found at http://www.ixarm.com.

16.2 Structure of the Laws and Regulations

(a) International Treaties

France participates in a number of international treaties on export controls, and its national regulations are based on such treaties. The chief international agreement is the Wassenaar Arrangement (discussed in detail next), but France is also a member of the Missile Technology Control Regime, the Australia Group, and the Nuclear Suppliers Group.—The Wassenaar Arrangement

The Wassenaar Arrangement is a comprehensive multilateral arrangement for the control of exports of conventional arms and dual-use goods and technologies used in their manufacture. It was concluded in July 1996 by 33 states and takes its name from the city of Wassenaar, in the Netherlands. It now includes 42 states.

The Wassenaar Arrangement aims primarily to promote “transparency and greater responsibility in the transfer of arms and dual-use goods in order to prevent destabilizing accumulations.”[5] It complements and strengthens existing regimes for the nonproliferation of weapons of mass destruction. States parties to the Arrangement must ensure that their transfers of conventional arms and dual-use goods and technologies do not contribute to the development or strengthening of military capabilities that could undermine regional and international security and stability.

The legally informal nature of the Wassenaar Arrangement is based on a political commitment expressed in initial elements and additional texts or declarations unanimously adopted by the participating states. All decisions within the Wassenaar Arrangement are taken by consensus.

At the political level, the states have committed themselves to follow the “guidelines,” “elements,” and “best practices” adopted by the Wassenaar Arrangement; control under their national legislation the export of goods on the Wassenaar Arrangement’s Military List and Dual-Use List; to report, in the interests of transparency, on transfers of conventional arms and dual-use items deemed to be highly sensitive, as well as on denials of transfers of dual-use items in general; and exchange information on exports of highly sensitive dual-use items and technologies.

The permanent secretariat of the Wassenaar Arrangement is located in Vienna and has a staff of about a dozen. The Plenary Assembly meets once a year, and its subordinate bodies meet regularly.

Depending on technological developments, the expert group updates the checklists annually. The Wassenaar Arrangement’s military list is included in the European Common Military List of Military Equipment and the list of dual-use items is transposed into the Community Regulation on the Control of Exports of Dual-Use Items and Technology (Regulation (EU) 2021/821). Export controls remain the sovereignty of each participating state.

(b) France National Laws and Regulations on Export Controls

In the area of arms exports, France is committed to transparency vis-à-vis the international community and civil society. In addition to providing information on its national system for controlling the production and trade of arms (regulations and administrative procedures), it also provides data on its arms transfers.

France thus participates in the United Nations Register of Conventional Arms, established in 1992, by submitting annually information on exports, imports, holdings of its armed forces, and purchases related to national production. France also transmits information to its partners in the Wassenaar Arrangement (export of military equipment and certain dual-use items) and the Organization for Security and Cooperation in Europe (import, export, and destruction of small arms and light weapons; reports on

national control procedures). Lastly, France participates fully in the information exchange mechanisms set up within the European Union (COARM, denial notification system, national contribution to the European Union's annual report).

At the national level, since 1998, information on France's arms exports has been illustrated by the publication of the annual report to Parliament, presented by the Minister of Defense to the members of the Defense and Armed Forces Committees of the National Assembly and Senate. The report is widely distributed, and an electronic version is available online on the Ministry of Defense website. Similarly, the Ministries of Foreign Affairs and Defense maintain a regular, high-quality dialogue with all civil society actors concerned by arms export issues, either directly or indirectly through national representation via parliamentary questions.

The "ICT Directive" maintains the principle of authorizing transfers to EU member states of the equipment listed in its annex, which it refers to as "defense-related products." France has decided to add satellites, launchers, and their components to the scope of the directive, which are treated according to the same procedure. The directive decisively simplifies controls in several respects:

- European Union member states can no longer, barring exceptions, require a War Material Import Authorization (WMIA) for "incoming intra-community transfers" as was the case prior to the adoption of the directive.
- General transfer licenses (GLT) are introduced, four of which are provided for in the Directive, in order to allow community suppliers (companies, government departments, etc.) meeting certain conditions to transfer, without prior authorization, defense-related products listed by the GLT to community recipients in accordance with the criteria laid down in the directive.
- Global and individual licensing mechanisms granted by the national authority to an identified supplier, allowing the transfer to the territory of one of the member states of the European Union.
- Certification of undertakings receiving transfers: issued for a limited period by the national authorities of each member state for undertakings established on its territory, the certification attests, depending on compliance with general criteria defined by the Directive and adopted by the member states, the general capacity of

the undertaking to comply with restrictions on the end use or export of defense-related products received under a transfer license from another member state, and thus compliance with the requirements attached to licenses, as a guarantee of mutual trust between member states.

- A control mechanism for export restrictions (outside the European Union) that obliges companies to comply strictly with the conditions imposed on their equipment during previous transfer(s) and to certify to the exporting state that they are in compliance with these obligations.
- An a posteriori control process has been introduced to ensure that the greater fluidity of transfers within the European Union, permitted by the Directive, does not undermine the effectiveness of the control.

(c) European Common Position

On December 8, 2008, the Council of the European Union adopted Common Position 2008/944/CFSP "defining common rules governing the control of exports of military technology and equipment." This document, published in the *Official Journal of the European Union*, sets out a list of criteria to be taken into account by member states when considering export applications submitted to them by their companies. By adopting this position, the Council gives the export control policy a legally binding character.

The common position serves two purposes:

- To promote the principles of transparency and responsibility on the part of arms exporting countries with regard to transfers to third countries: The notification to partners of refused transactions and the resulting consultations meet this requirement. The annual report on arms exports is a direct consequence of the implementation of the Common Position. In addition, member states are required to transmit annually to the General Secretariat of the Council of the EU very precise data on their arms exports.
- To facilitate the convergence of member states' war material export policies.

Trade under the CFSP is all the more fruitful, as European states often have to control similar export projects. The Common Position takes up and

clarifies the eight criteria of the Code of Conduct that the national control authorities must respect when examining applications for authorizations submitted by industrialists.

The decision to accept or refuse an export remains the sole responsibility of each state. However, the Common Position exposes a member state that fails to comply with these guidelines, for example by failing to comply with the transparency procedures, or by failing to respect the criteria set out in the Common Position (and in particular the criterion of respect for human rights) to political and diplomatic sanctions decided by the European Union.

The export control regime for war materiel and similar equipment was thoroughly overhauled in 2012 and 2013 under Law No. 2011-702 of June 22, 2012, which came into force on June 30, 2012, in application of the European directive on intra-community transfers (Directive 2009/43/EC of 6 May 2009, known as the ICT Directive;. France has taken advantage of this transposition work to also conduct a broad reflection on its processes for controlling exports of war materiel and similar items outside the European Union, which do not fall within the scope of the directive and therefore remain entirely within its jurisdiction. Its provisions, as well as those of one of its implementing decrees, are codified in the Defense Code, which they amend (in particular in Title III of Book III of Part 2 of the Legislative Part).

This act introduces two new concepts into our regulations. On the one hand, it now distinguishes between intra-community transfers (ICTs) governed by the provisions of the “ICT Directive,” which it transposes, and exports outside the European Union (EU) for which states remain free to define the principles of control and which France has chosen to reform in depth.

On the other hand, it creates three types of export or intra-community transfer licenses: general licenses, and individual or global licenses. They may be subject to conditions. Intra-community transfers of equipment mentioned in Article L.2335-18 of the Defense Code (defense satellites and their components) are subject to “prior transfer authorizations.” Despite a different legal basis, the licenses used for this equipment are the same. It does not, of course, abolish controls on imports from countries outside the European Union.

The evolution of the control regime should make it possible to meet the expectations of economic operators by introducing a license system that is easier to use while ensuring equal robustness in terms of control. In addition, the operation of the Interministerial Commission for the Study of War Materiel Exports has been adapted to the new regulations and optimized to ensure more efficient examination of applications for export and intra-community transfer licenses.

(d) France and the UN Export Control

In its resolution 1540 (2004), the United Nations Security Council decided that all states shall refrain from providing any form of support to non-state actors that attempt to develop, acquire, manufacture, possess, transport, transfer, or use nuclear, chemical, or biological weapons and their means of delivery, in particular for terrorist purposes. The Council also decided that all states shall adopt and enforce appropriate legislation and other effective measures to prevent the proliferation of such weapons and their means of delivery in order to prevent access by non-state actors, in particular for terrorist purposes.

Furthermore, on April 2, 2013, the United Nations General Assembly adopted, by a very large majority, the Arms Trade Treaty, the first universal legally binding instrument to regulate the trade in conventional arms and to combat illicit arms trafficking in a comprehensive manner, thereby preventing the dramatic consequences for civilian populations.

The Arms Trade Treaty applies to all conventional weapons as defined by the United Nations Register, including small arms and light weapons. It requires states parties to establish the legal tools and practical arrangements to control the flow of military equipment and associated parts and components.

It also requires states to prohibit any transfer that would result in the violation of a UN Security Council resolution, the noncompliance of a state with its international obligations, the commission of international crimes (including war crimes and crimes against humanity), grave breaches of the Geneva Conventions, or attacks against civilian populations or protected civilian objects as defined by international agreements. States should also make the export of arms subject to prior authorization. In particular, export applications will be refused if there is an overriding risk that the arms will

be used to commit serious violations of international human rights and humanitarian law.

France signed the treaty on June 3, 2013 in New York with 66 other states, including 24 member states of the European Union. France, which has a rigorous system for controlling its arms transfers, is already complying with all these provisions.

(e) France National Licensing Process

Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021, lists the various general export authorizations of the Union in Annex II (see Annexes IIa to IIh).

The export authorizations include the following:

(i) Individual License, Valid for Two Years

This individual license is valid throughout the European Union for one or more identified goods of the same nature with a named consignee within the limit of a given quantity and value. It may be granted for all dual-use items subject to authorization and for all destinations (article 12 of Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021).

(ii) Global License (LIGLO), Valid for Two Years

This global license allows the export without limitation of a quantity or value of one or more identified goods to one or more consignees or states of destination named on the license. The company must set up an internal audit program with a commitment to internal control procedures. The consignees are either the end users or the distributors applying the control procedures specified by the exporter and allowing the latter to know the distributed products and their end users.

Excluded are the goods listed in Annex IV of the regulation Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021as well as certain goods designated by decrees. Invoices and documents accompanying the goods must be marked “dual-use goods subject to export control, taken out of France under a general license . . . No. issued on . . . .”

The exporter must inform the foreign buyer of the status of the exported goods. He must notify the administration of any change of final destination if he is informed of it and set up a filing system enabling information on exports made in this context to be communicated to customs.

(iii) International Import (CII) and Delivery Verification (CVL) Certificates

In order to enable his foreign supplier to obtain an authorization from his national authorities to export the goods, the importer of goods (listed in Annex I to Regulation 2021/821 as amended) from a third country outside the European Union may apply for an International Import Certificate, or a Delivery Verification Certificate, proving that the goods have arrived at their destination.

(iv) Information to Be Entered on the Export Declaration

Exporters must specify in box 44 of the customs declaration (Single Administrative Document) the reference number of the license used and the document code X002 (or document code 2410 for exports of civil helicopters and their spare parts, tear gas or riot control agents to third countries).

(v) Brokerage Authorizations

They shall be granted by the competent authorities of the Member State where the broker resides or is established for a fixed quantity of given goods moving between two or more third countries (see EGIDE portal).[6]

Brokers must indicate the location of the goods in the third country of origin, a clear description of the goods, the quantity involved and the third parties involved in the operation, the country of destination, the end user in that country, and its exact location. The authorizations are valid throughout the European Union.

(f) France Sanctioned Parties Lists

The national register of frozen assets is operated by the Treasury Department. It lists all the persons, entities, and vessels subject to asset

freezing measures in force on French territory, in application of national, European, and international (UN) provisions.

France applies the UN and EU sanctions, but it also enacts sanctions of its own as per national law. French law currently includes more than 2,000 asset-freezing measures, designed to combat the financing of terrorism, proliferation and serious and illegal violations of human rights and international peace and security. In this way, it contributes to guaranteeing the full implementation of asset-freezing measures without delay by all concerned parties.

A new system has been implemented as of March 16, 2021. Now the interaction between the user's systems and the data is easier via an APP.[7]

The registry is offered in interoperable formats (xml and json), available via an APP, in order to facilitate the automation of filtering. The registry is also delivered in the form of filterable data that can be exported in PDF version. Each person, entity, vessel has a unique number on the register (id), even if the person is designated in several sanctions regimes.

New fields have also been added to optimize filtering: passport, identity documents, title, cryptocurrency, EU reference, UN reference. The register can be consulted at https://gels-avoirs.dgtresor.gouv.fr/.

Last but not least, in order to keep up to date on the evolution of sanctions, operators are strongly advised to subscribe to the Treasury newsletter.[8]

16.3 What Is Regulated: Scope of the Regulations

The export control laws of course regulate exports. But the definition adopted by the law is broad: export control therefore also covers

- Temporary exports (e.g., under cover of an ATA carnet);
- Standard exchange of parts;
- Secondhand goods;
- Samples;
- Re-exports of non-community goods following the following customs procedures: free zone, customs warehouse, inward processing, temporary importation;
- Goods that are merely in transit (transport of non-community dual-use items entering the customs territory of the community and

passing through it to a destination outside the community) through the territory of the European Union: the authorities of the member states have the option of prohibiting or subjecting to authorization on a case-by-case basis the transit of non-community dual-use items;

- The provision of brokering services (negotiating or arranging transactions for the purchase, sale, or supply of dual-use items from one third country to another third country or for the sale or purchase of dual-use items that are located in third countries with a view to their transfer to another third country) where the broker knows or has been informed by the competent national authorities that such provision could lead to the production or supply of weapons of mass destruction in a third country.

Exports of dual-use items and technology, listed in Annex 1 of Council Regulation (EC) No. 2021/821, are subject to an export license regardless of the third country to which they are exported or re-exported.

On May 20, 2021, the European Union adopted a new regulation 2021/821, which takes into account the numerous and substantial changes made to regulation (EC) 428/2009.

It came fully into force on September 9, 2021.

An export license issued in one member state is valid throughout the European Union. It is issued by the competent authorities of the member state where the exporter is established. This member state may be different from the one from which the customs export formalities are completed. In this case, the export declaration to French customs must be accompanied by the original of the foreign license (which must first be requested in several copies) and its translation into French. The references and number of the license must appear on the SAD (box 44).

If the French exporter plans to export his products from a member state other than France, he will have to apply to the SBDU for an export license in paper and not dematerialized format. Exporters must inform the competent authorities of the member state in which they are established at the time of first export.

16.4 Who Is Regulated?

The main responsible person for managing export controls is the exporter, that is, the person who holds the contract leading to the actual export of the item outside of France. In case there is no contract or such contractor is located outside of the European Union, you have to consider the person in charge of deciding that the goods are to be shipped outside of the EU.

Nevertheless, in French law, other persons can be held accountable in case of violations, such as the customs declarant and the natural person who is the legal director of the company.

For the specific case of encryption, a distinction has to be made between national formalities, which are the responsibility of the manufacturer or author of the encryption, and the export license as per the EU regime, which has to be applied for by the exporter.

16.5 Classification

(a) Classification of Dual-Use Items

A “dual-use item” is a product or service “capable of having both civilian and military use,” that is, generally intended for civilian use, for example, in industry, but which can also be used to develop military weapons or equipment. As such, its export is not prohibited a priori but is subject to control, generally in the form of a licensing requirement. Some dual-use goods or technologies are likely to have a conventional military use, while others can be used to manufacture weapons of mass destruction: nuclear, chemical, or biological weapons or missiles capable of carrying such weapons.

The 2021 reform established the definition of dual-use goods in article 2 of the regulation:

> Products, including software and technology (including the transmission of software or technology by electronic means, facsimile or telephone to a destination outside the Community) outside the Community) which may have both civilian and military uses

The 2021 reform broadens the scope by including cyber-surveillance technologies that are now subject to export controls.

The Regulations aim to further prevent the misuse of dual-use items in connection with acts of terrorism or human rights violations. The prevention of human rights violations becomes, first of all, a criterion for

assessing the need to include an item or technology in the list in Annex 1 of the Regulation and in the “National Control List” of the member states.

Also, the notion of exporter has finally been identified: “the exporter is the person (natural or legal) entitled to decide on the export of the product.”

With the 2021 reform, the notion of exporter is extended to include operators re-exporting European products. Natural persons are explicitly included in the definition of exporter. They can therefore be held responsible for the transmission or provision of goods. The communication in electronic or oral format of these goods is also included in the scope of the Regulation.

Moreover, technical assistance is now defined in point 9 of Article 2 of Chapter I and is therefore subject to authorization.

With the exception of certain very sensitive goods included in a specific list annexed to the Regulation (Annex IV), transfers within Union territory are not subject to these controls.

Dual-use goods are classified into ten categories

- Category 0: nuclear materials, facilities and equipment
- Category 1: special materials and related equipment
- Category 2: materials processing
- Category 3: electronics
- Category 4: calculators
- Category 5: telecommunications and “information security”
- Category 6: sensors and lasers
- Category 7: navigation and aero-electronics
- Category 8: marine
- Category 9: aerospace and propulsion

Each product concerned is classified and identified by an alphanumeric reference.

The first digit of the product reference corresponds to the category (0 to 9), the letter to the type of goods (A for equipment, assembly, components; B for test, inspection, control, production equipment; C for material; D for software; and E for technology). The second digit refers to the international control regime, and the remaining two digits to the serial number of the good. For example, the reference OD001 corresponds to software containing information on uranium production.

Article 4 of Regulation 2021/821 maintains the application of the catchall clause for goods that are not on the regulation's lists but may be subject to control if they are likely to contribute to the proliferation of chemical, biological, or nuclear weapons.

In France, implementation is done through a notice to exporters, or on a case-by-case basis.

The new regulation provides for the creation by each member state of a "national control list" comprising goods not listed in Annex 1 of the regulation for which the state in question has nevertheless considered that their export requires an authorization. This innovation makes it possible to harmonize "catchall" practices and to limit any "shopping" in terms of export controls within the EU.

(b) Classification of Military Items

The regime that applies to war equipment is a prohibition regime. All operations concerning war equipment themselves are prohibited (design, manufacture, trade, import, transit, export), unless authorized. The category of "related material" is subject to authorization only for export.

Goods whose transfer or export is subject to authorization are defined in order of 27 June 2012, as amended (Order of June 27, 2012, relating to the list of war materiel and similar materials subject to prior export authorization and defense-related products subject to prior transfer authorization). This list is common to all European countries (except Annex II) and member countries of the Wassenaar Arrangement. The first act of internal control shall be the classification of the item or technology that the company manufactures or plans to manufacture to export, as goods may be covered by several different regulations.

It is primarily related to the "designed" character or "modified for military use." The classification of the item is the responsibility of the exporter (on the basis of the decree of 27 June 2012). If there is a doubt, the French general directorate of armament (named DGA in French) can provide assistance, in particular through advice or a request for classification filing. A form filing application[9] allows one to question the DGA and obtain a classification decision. The request for classification must include technical documentation of the concerned equipment.

Authorizations are in the form of licenses; import licenses (from a country outside the EU), export licenses (to a country outside the EU), and transfer licenses (to an EU country) are different in their scope. A license is required for the transmission of information, the temporary export or transfer of materials for demonstration or evaluation, the signing of contracts or the formal acceptance of orders, and finally to the export or physical transfer of materials.

16.6 Licensing/Reasons for Control

(a) Types of Export Control Licenses for Dual-Use Items

The control of exports of dual-use goods and technologies is legally based, in France as in the other member States of the European Union, on a Community regulation (Regulation 2021/821, as amended). This regulation defines in particular the various types of export licenses and sets out the list of goods concerned. The controls apply to all exports to territories outside the European Union. With the exception of certain very sensitive goods included in a specific list annexed to the Regulation, transfers within European Union territory are not subject to these controls.

The list of dual-use items and technologies subject to controls is the first annex to the regulation, which can be accessed at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32021R0821. It is regularly updated to take account of technological developments and their availability on the international market. The list includes dual-use items covered by the Wassenaar Arrangement, the NSG (Nuclear Suppliers Group), the MTCR (Missile Technology Control Regime), the Australia Group (against biological and chemical proliferation), and the Chemical Weapons Convention.

It is noted that some countries are subject to import or export restrictions. The list of restrictive measures in this area is available on the Customs website at https://www.douane.gouv.fr/demarche/consulter-la-carte-interactive-des-mesures-de-restrictions-commerciales. In France, the dual-use goods service (SBDU) of the Ministry of the Economy, Industry and Digitalization is the authority responsible for issuing export licenses for dual-use goods. The most sensitive applications are examined by an

Interministerial Commission for Dual-Use Goods (CIBDU), chaired by the Ministry of Europe and Foreign Affairs.

(i) The Australia Group

Established in 1985, the Australia Group comprises the 41 leading exporters of chemical and biological dual-use goods and technology, including all European Union member states and the European Commission.

The Australia Group brings together States that are parties to both the 1972 Biological and Toxin Weapons Convention (BWC) and the 1993 Chemical Weapons Convention (CWC) and are actively engaged in their work and compliance with their implementation.

The Australia Group agrees on chemical and biological dual-use export control lists and guidelines in the chemical and biological fields that harmonize the control practices of member states, while not impeding economic exchanges or work for peaceful purposes.

The European Union has made these lists legally binding on its member states through a Union regulation, the latest version of which is Regulation 2021/821.

France actively participates in the work of the Australia Group, in line with its commitment to the universalization and implementation of the CWC and the BTWC, as well as the 1925 Geneva Protocol prohibiting the use in war of asphyxiating, poisonous, or other gases and bacteriological methods of warfare, of which it is the depositary.

(ii) The Nuclear Suppliers Group (NSG)

The Nuclear Suppliers Group (NSG), established in 1974, comprises 48 participating states. It is a group of nuclear supplier countries that seeks to contribute to the nonproliferation of nuclear weapons through the implementation of two guidelines.

The guidelines define sets of supply conditions applicable to transfers of nuclear items for peaceful purposes to ensure that they do not result in diversion to unsafeguarded nuclear activities or nuclear explosive activities. They are supplemented by lists of sensitive items that must be subject to export controls by national authorities.

Participating governments undertake to implement the guidelines within the framework of their national legislation.

(iii) Control of Missile Technology

In order to combat the proliferation of means of delivery likely to carry weapons of mass destruction and to develop common principles to govern exports of ballistic equipment and technology, France participated with the rest of the G7 in the creation of the Missile Technology Control Regime (MTCR) in April 1987. The MTCR has gradually expanded and now has 35 members.

The MTCR is based on compliance by each of the member states—in their national export policies—with common guidelines for the transfer of goods and technologies which could contribute to the manufacture of delivery systems for weapons of mass destruction. These guidelines are based on a common list of equipment, software, and technology subject to control (MTCR Technical Annex).

France has supported efforts to adapt the MTCR to new threats, in particular the terrorist threat. Moreover, continuing to make effective export control a priority, the member countries decided in 2003 to include a catchall clause in the Regime's guidelines, which makes it possible to control the export of items not on the MTCR control list but which could contribute to the development of delivery systems for weapons of mass destruction.

France provides the permanent secretariat of the Regime as the "Point of Contact." It facilitates the smooth flow of information and documentation among partners, assists the Chair of the Regime in its activities and organizes regular meetings.

(b) Export Control Licensing Procedure

See preceding Section 16.6(a).

(c) Import and Export Licenses for Military Items

(i) General Principles

French arms export controls are defined by a rigorous legislative and regulatory framework, which takes into account the national imperatives of sovereignty and security as well as France's international and European commitments in the areas of arms control, disarmament, and nonproliferation.

The French system for controlling war materiel is based on a general principle of prohibition, unless authorized by the state and under its control, which means that the entire defense sector and its flows are subject to state control. Applications for export licenses are subject to Interministerial evaluation within the framework of the Interministerial Commission for the Export of War Materiel (CIEEMG). Chaired by the Secretary General for Defense and National Security, it includes representatives of the Ministries of Foreign Affairs, Defense and Economy.

France exercises strict, transparent, and responsible control over its war materiel exports.

France is a member of all international instruments that organize consultations on arms export issues. In this respect, the control exercised by France is one of the most comprehensive in the world. It bases its export decisions on criteria determined within the framework of the international treaties, conventions, instruments, or forums to which it adheres, in particular Council Decision (CFSP) 2019/1560 of September 16, 2019, amending Common Position 2008/944/CFSP, defining common rules governing control of exports of military technology and equipment and the Arms Trade Treaty. France implements the international embargoes established by the United Nations and the European Union.

All data on French exports is accessible online and updated annually as part of the report to parliament and France’s report to the Arms Trade Treaty. These data cover the strategic context, the regulatory framework, and statistical elements.

The Arms Trade Treaty (ATT), adopted on April 2, 2013, by the UN General Assembly and entered into force on December 24, 2014, is the first legally binding instrument to regulate the international trade in conventional arms. At the beginning of December 2019, it had 105 states parties.

The objective of the Treaty, while recognizing the legitimate interest of members in the export, import, or transfer of conventional arms, is to encourage members to adopt responsible, transparent, and proportionate rules of conduct in this area in order to contribute to international peace and stability and to avoid violations of international humanitarian law and human rights law. To this end, the treaty provides, inter alia, for the establishment of national export control regimes for war materiel, the adoption of measures to prevent their diversion, and the submission of reports on the implementation of the treaty.

France attaches the utmost importance to this treaty, which it has supported since the launch, in 2006, of the negotiation process that led to its adoption. It deposited its instrument of ratification on April 2, 2014, at a joint ceremony with Germany, and remains committed to the universalization of the ATT. To be fully effective, the treaty must be signed and ratified by the largest possible number of states, in particular the main arms exporters and importers.

France maintains a regular dialogue with civil society on issues relating to the implementation of the ATT. On the occasion of the fifth Conference of States Parties, which took place in Geneva from August 26 to 30, 2019, France committed to the proper implementation of the treaty and also organized a side event on the contribution of the private sector to the implementation of the treaty, in parallel with the fifth Conference of States Parties.

France is also taking part in assistance and communication activities to support certain countries, particularly African countries, in acceding to the Treaty or in its effective implementation. The Expertise France agency is mandated by CFSP Decision 2017/915 to implement, in partnership with the German Federal Office of Economics and Export Control (BAFA), the European Union project to support the application of the ATT (EU ATT Outreach Project II). This project aims both to contribute to the strengthening of the national control systems of the beneficiary countries, through assistance in the development of the regulatory framework or the training of officials, and to promote the universalization of the ATT among states that have not yet ratified it.

(ii) In Practice

The first step for companies seeking licenses for operations in relation with military goods is to register with the “SIGALE” portal.[10] In order to register, the following information about an organization must be provided: company name, EORI number and addresses of all company branches, list and contact details of persons in charge, and persons having authority to engage the company. Operators will also have to provide a certificate of incorporation (named “k-bis extract”) dated less than three months. Once the registration is validated, the operator will receive by mail the ID, access and validation codes, and individual card (token).

The second step is to identify the concerned items within the General Directorate of Armament "catalogue." To carry out this online declaration, operators must have completed the identification process and therefore be in possession of an ID. Information to be provided includes the category of the equipment according to the decree of June 27, 2012, and its technical reference, together with a description of the equipment and a technical documentation. Depending on how sensitive such documentation is, it can be either transmitted on the SIGALE online platform, sent by mail, or hand delivered.

Having performed these two steps, the operator is now allowed to submit an application for an individual or global license, modify a current application, file a request to modify a notified license, and declare the intention to use a general license (first registration). Again, the more or less sensitive nature of the required documentation will change the way it is made available to the authority.

16.7 General Licenses/License Exceptions

The European Union provides for general licenses no. EU001 to EU006: they facilitate without limitation of quantity and duration exports for certain types of goods (EU005 for telecommunications; EU006 for chemicals). Most dual-use items can be concerned but for certain destinations only (EU001 and EU002), and/or certain types of operations (EU003 for export after repair/replacement or EU004 for temporary export for an exhibition or fair). Two new general export authorizations have been created (EU007 and EU008), notably for encrypted data, shipments below a certain value, and intra-group transmission of software and technology.

In France, there are seven types of national general licenses: industrial goods, chemical products, biological products and graphite, trade fairs and exhibitions, dual-use goods for the French armed forces, and aeronautical equipment. Attention shall be brought on the fact that these general licenses or license exceptions do require some steps to be taken from the exporter prior to the export (filing for the EU or national general license) and after the export (reporting).

16.8 Penalties, Enforcement, and Voluntary Disclosures

An unauthorized export of goods covered by Regulation 2021/821 constitutes an infringement under Article 38 of the Customs Code.

Exporting prohibited goods without a license is a first class customs offence punishable under Article 414 of the Customs Code. It is punishable by a maximum of three years imprisonment, confiscation of the object of the fraud and the means of transport, and a fine of between one and two times the value of the goods. Penalties are higher if it is established that the export was carried out with a view to promoting proliferation (see the following subsections).

(a) Administrative Penalties

No administrative penalties are available in France for export control or sanctions violations.

(b) Criminal Penalties

Penalties are of a criminal nature, but settlements are often available with the administration.

Under French law, both the signatory of the export declaration and the exporter can be held criminally responsible. Export control violations are regarded as criminal offences, which can be brought before criminal courts. Penalties in place for export control violations were already among the toughest under the French Customs Code (up to two times the value of the goods and three years in prison). In accordance with the reform of customs legislation (Article 14 of law 2011-266 of 14 March 2011), Article 414 of the French National Customs Code has been amended to include a specific provision that applies to export control violations. For exporting without declaration or smuggling a dual-use item, the applicable maximum penalty is now equal to three times the value of the goods concerned in addition to confiscation of the goods; the potential prison sentence has been raised to a maximum of five years.

In practice, bringing a criminal case against a legitimate company can be counterproductive, and for many companies, paying a penalty amounting to the value of the goods exported—not to mention three times their value, as provided by Article 414 of the French Customs Code—could result in bankruptcy. Therefore, most customs cases end with a settlement proposal. Customs proposes a reduced fine to the exporter, instead of bringing the

case before the criminal courts. The company itself may also request the benefit of a settlement if customs does not spontaneously propose it, although customs is solely in charge of evaluating and proposing an actual penalty. If customs and the exporter agree upon the settlement conditions, a transaction is signed between them, and when the penalty is paid by the exporter and the final settlement approved by customs, the case is closed. The transaction signed between customs and the exporter is then regarded as valid and definitive, and the relevant infringement may not be prosecuted again by customs.

(c) Voluntary Disclosures

No voluntary disclosure process is available in the law for export control violations.

16.9 Recent Export Enforcement Matters

The French administration is entrusted with extensive powers to investigate export control infringements. As an example, upon the authorization of a judge, they can decide to search the company offices, computers, cars, and so on. Once authorized, the search can be very extensive and difficult to challenge. This was the case for Cour d'appel de Paris—Pôle 05 ch. 15, May 20th 2020/no. 19/13830, when customs suspected that the company XX had proceeded to export without authorization of goods subject to the regulations on dual-use goods, the National Directorate of Intelligence and Customs Investigations filed a request before the judge for authorization to carry out a home inspection of the head office of XX company, the head office of YY company, the vehicles of XX company and the vehicle of Mr. D, the manager of YY company.

Indeed, the investigators suspected that the company XX had exported in 2016, to the company Invap located in Argentina, goods classified in Annex I of the European Regulation No. 2021/821 without having the necessary license for the export of this type of goods. The investigators also suspected XX company of having circumvented two refusals of license in 2017 and 2018 imposed by the Dual-Use Service concerning a project to export leaded glass armored portholes to India, by exporting materials subject to license to a company in Argentina but in reality on behalf of a

final consignee located in India, the company WW. The defendants appealed the measure but the court of Paris rejected the claim.

The French administration can also act further to a request from a foreign authority for extradition purposes.

Cour de Cassation, March 11th 2020: Mr. C., an Iranian national, was arrested upon his arrival at Nice airport on February 2, 2019, pursuant to a request for provisional arrest with a view to extradition sent by the authorities of the United States of America, and placed under extradition detention.

He was accused of having attempted to export equipment manufactured in the United States, finally seized in the port customs zone, whose uses can be both civil and military, and therefore subject to export authorization, after having acquired them using front companies, assumed names and fraudulent interbank transfers, by informing them on an electronic medium with false information instead of the real recipient country, Iran.

Mr. C.'s extradition was sought pursuant to two arrest warrants issued on January 17 and February 22, 2019, by the federal judge in Washington, D.C. The Cour de Cassation rejected Mr. C's claim.

16.10 Special Topics

Although industrial groups have a broad understanding of the regulatory regimes for import and export controls, the operational translation of these regimes remains a challenge for them. This is particularly true since they must integrate into their compliance programs the rapid changes in the economic sanctions regimes that are intrinsically linked to it.

However, the scope of application of export control rules goes far beyond the industrial domain and places heavy constraints on the financial institutions and insurance companies that accompany exporters, without their having fully appreciated the nature of the constraints and due diligence that export control requires. Their current apprehension is to some extent comparable to the treatment they gave to due diligence relating to the fight against money laundering and the financing of terrorism (LCB/FT) in the early 2000s.

Long neglected by both foreign and domestic regulators, export control is now at the heart of their preoccupations; sectoral economic sanctions against Russia and the gradual opening up of the Iranian market after years

of almost total embargoes have increased the vigilance of regulators, who are now showing increasing activism in this area. It is therefore becoming urgent for industrial groups—the primary targets of these complex and evolving regulations—as well as for financial institutions and insurance companies to integrate their export control obligations into their compliance programs in order to better prevent this hitherto poorly appreciated regulatory risk.

At first glance, the link between export control rules and economic sanctions regimes is not easy to grasp. The two sets of regulations are intrinsically linked, which is not without creating a form of confusion for industrial groups and the financial institutions and insurance companies that accompany them. However, these two regimes exist independently of each other; to consider that export control issues would only apply to exports to countries under embargoes would not only be simplistic but above all dangerous for the exporter and his banker/insurer, who could then find themselves in a situation of noncompliance.

Broadly speaking, the export control rules identify certain types of goods, technologies, and services whose import (in certain specific cases) or export requires prior authorization from a control authority—in France, the SBDU and the CIEEMG—which will decide on the basis of the background information provided by the importer or exporter. These rules apply irrespective of the country of origin of the import or destination of the export.

Economic sanctions regimes add to this “general” regime prohibitions for certain countries or geographical areas. For example, the export of dual-use items to Russia has always been subject to prior authorization by the SBDU. The sectoral economic sanctions in force since the summer of 2014 have prohibited the export of these goods to certain populations in Russia (the army in particular see ahead).

A misunderstanding of the relationship between these different regimes is not without risks: some financial institutions, for example, consider—wrongly—that they are only obliged to carry out controls on the goods financed in the context of exports to countries under sanctions.

Export control compliance programs must also take account of the extraterritorial scope of these rules: for example, U.S. rules apply outside the United States if, among others, the exported good contains a certain percentage of U.S. components. These are all risks to which industrial

groups, bankers, and insurers must provide satisfactory operational responses.

While industrial groups are beginning to integrate export control mechanisms into their compliance programs, the same cannot be said for banks and insurance companies. Before granting financing, few of them ensure that the exporting company has complied with its export control obligations. And if they do, it is often only in the case of exports to countries under sanctions. However, financial institutions and insurance companies are also subject to export control rules and their liability may, at a minimum, be engaged on the basis of complicity and/or LCB/FT regulations.

(a) Re-exports/Extraterritorial Application of Laws

French export control laws do not have extraterritorial effect. Even though an end-user certificate is required in many instances, and such end user commits not to re-export the goods, controls do not follow the goods, and the re-export could be take place, subject to the authorization of the concerned authority locally.

(b) Intangible Transfer of Technical Information

France controls the transfer of controlled technology and information, but does not implement deemed exports and deemed re-exports controls.

(c) Practical Issues Related to Export Control Clearance

Even in a fairly compliant company, export control violations can happen due to negligence, lack of communication, or lack of training for the most part. It is important to design systems to flag articles that have to require special permits. Of course, the sophistication of such systems depends on the size of the relevant company.

As an example, staff in charge of logistics use an express carrier or postal service because the delivery date is short, but with no consideration of the applicable license. Vendors will accept orders with short deadlines without considering the sensitive nature of the goods and the applicable procedures to obtain the license.

Service providers are keen on getting export formalities done quickly. They tend to use the relevant codes where the goods are not controlled, unless the exporter explicitly instructs otherwise. Should they raise the possibility of a license being required for each and every client, they would not be able to do business, so remember it is up to the exporter to instruct properly.

Also in the case of returns or exchanges of merchandise for warranty reasons, it is frequent that personnel from after-sale service department will not be aware of the existence of a license requirement.

The general idea is to encourage the rise of awareness and internal communication when it comes to export controls.

Also, a lot of applicants lose a lot of time and effort in their application because of inconsistencies that could have been identified before: the quantity, consignee, pricing, and so on, from the documentation do not match with the application and cause automatic rejection.

(d) Recordkeeping

Due to statute of limitation rules, potential ongoing investigations for infringement, which an exporter might not be aware of but still may be their concern, it is advisable that all sensitive export documentation is kept in a secure manner for as long as a ten-year period. That includes a copy of any license, export declaration, shipping documents, invoices, and packing list.

In the case where the exporter thought about applying for a license, but finally decided against it, it is recommended to keep track of the decision, such as a classification advice from an inside officer or outside counsel for ten years.

16.11 Encryption Controls

(a) General Comments

Encryption consists of cryptography techniques applied to convert data into an “encrypted” form in order safeguard sensitive information. Encryption responds to different needs:

- Confidentiality. Making information unreadable to anyone who intercepts the message inadvertently;
- Access control. Limits access to sensitive data or servers to selected authorized users (Unix password, for example);
- Data integrity. Guaranteeing that the encrypted data is not tampered with fraudulently;
- Identification. Ensures the authentication of partners and the authenticity of the message.

Large hi-tech companies quickly realized that encryption, the same way as the internet, was to become a flourishing business and heavily invested into it.

(b) Encryption Export Licensing Requirements

In 1997 (March 27), the Organization for Economic Co-operation and Development (referred to as OECD) provided guidelines for cryptography policy. These guidelines advocate the liberalization of cryptographic means to promote the emergence of electronic business. The development of encryption greatly contributes to electronic commerce, notably, by ensuring that confidential bank account information does not fall into the hands of ill-intentioned people.

In the European Union, most products incorporating encryption functions are classified as dual-use goods or war material and are subject to export control. They are treated as such since the technology surrounding encryption and cryptology maybe employed both for military and civilian use.

The means of cryptology fall under the category of “dual-use” goods; they are recognized under Category 5, Part II “Information Security” of Annex I of amended Council Regulation (EU) No. 2021/821.

Cryptology programs used for cryptanalysis are subject to stricter regulations and are included in the list of “very sensitive” items in Annex IV of Regulation 2021/821.

Although the European Union sets the regulations, it is the duty of the member states to enforce these rules.

Unlike imports and intra-EU transfers, which are subject to declaration made by the manufacturer/author as described later in the chapter, exports on the other hand are subject to a different regime. Depending on the

destination of the export, the export permit requirements differ. On one hand, exports to “ally countries” (Australia, Canada, USA, etc.) benefit from a general authorization of export from within the Union granted by Council Regulation (EC) No. 2021/821. These products only need to be declared, and the exporters of such equipment may ask for a general EU 001 license delivered by the Service for dual-use goods (referred to as SBDU) in France. However, exporters who ask for such general authorization are subject to extra formalities; indeed, they have an obligation of self-assessment and must report the details of their operations on a regular basis to the ANSSI.

On the other hand, exports to third countries are subject to the full force of administrative formalities. The manufacturer of the encryption must file for an authorization of the concerned product before ANSSI. Authorizations shall be filed at least four months before the export. The ANSSI shall deliver an affidavit to justify that the process is ongoing. The exporter (which can be a different party than the manufacturer) can use such affidavit to initiate a filing for a license at the SBDU. In exceptional cases, an exporter that is not the manufacturer of the encryption can proceed directly with ANSSI, for example if the manufacturer fails to cooperate.

(c) Import and Other Encryption Clearance Requirements

France yet implements another layer of controls for encryption that goes beyond the export controls set forth by the EU. Indeed, whereas the use of encryption media in France is unrestricted, the supply, import, intra-EU transfer, and export of cryptology are however regulated and subject to various administrative steps.

Under French law (art. 29 of law 2004-575 of 21 June 2004—Law regarding Confidence in the Digital Economy (LCEN)), the means of cryptology are defined as “any hardware or software designed or modified to transform data, whether it is information or signals, using secret conventions or to perform the opposite operation with or without a secret convention. These cryptological means are primarily intended to ensure the security of storage or data transmission, allowing to ensure their confidentiality, authentication or control of their integrity.”

The means of cryptology are subject to a specific control by French authorities, which requires that such means of encryption should be

declared or authorized before they are subject to intra-community transfers, import, or export from or to France. These steps are the responsibility of the manufacturer/author of the cryptology means and are to be taken alongside the National Agency for the Security of Information Systems (hereafter referred to as ANSSI). This Prime Minister Agency, created by Decree No. 2009-834 of July 7, 2009, records declarations and investigates requests for authorization of cryptology equipment.

Moreover, the requirements may vary depending on the technical functionalities of the means and the planned commercial operation (supply, import, export, etc.). It should be noted that the concepts of supply, import, and export cover any intangible transfers. In order to import cryptology equipment or software in France, including from another EU member country unless specifically exonerated, a declaration must be filed at the ANSSI at least one month before the operation. The transfers from France to other EU member states or from such member states to France are also subject to prior declaration. Applications are made in French, using the applicable form.[11] The information shall contain:

- Administrative information about the company such as a certificate of incorporation
- A description of the encryption functionalities
- A commercial documentation
- A technical documentation
- A letter of context

A mass market exception is also available but only applicable upon the confirmation of French authorities. In other words, mass market declared by a foreign country does not preclude the French authorities to declare it controlled and vice versa.

(d) Penalties for Violation of Encryption Regulations

Last but not least, for failing to comply with the aforementioned formalities, the concerned operators expose themselves to hefty fines up to 30,000 euro per infringement[12] and even prison sentences, without prejudice to the implementation of the customs code's sanctions (please see Section 16.8).

16.12 Blocking Laws/Penalties for Compliance with Sanction Imposed by Other Countries

As a member of the European Union, France implements the blocking statute decided by the EU authorities.[13]

The news of the war in Ukraine has seen the EU implement several "packages" of sanctions against Russia set out in Council Regulations 833/2014 and 269/2014. These sanctions apply to conduct in the EU and to all EU nationals and EU-incorporated entities anywhere in the world.

The European Commission has published frequently asked questions on several aspects of the new sanctions related to Russia and Belarus. In addition to separate FAQs on individual topics, the European Commission has also published a consolidated version of all FAQs published to date. These FAQs continue to be updated on an almost daily basis. In its FAQs, the European Commission confirms, among other things, that EU sanctions do not apply to non-EU companies or individuals operating entirely outside the EU. However, the European Commission says that, for example, if a non-EU entity "imports products through the Union or makes payments in the Union, it must comply with EU sanctions because it is entering the EU's internal market."[14] Council Regulation 269/2014 (as amended) imposes an asset freeze on a number of individuals and entities.

By Council Regulation (EU) No. 2022/2476 of December 16, 2022, the EU extended existing restrictions on dual-use items and technology. The new sanctions include a ban on the sale, supply, transfer, or export of any dual-use goods and technology to any natural or legal person, entity or body in Russia or for use in Russia, regardless of whether such goods and technology are intended for military use or for military end users. The prohibition also applies to the provision of technical assistance, brokering and other services, and financing or financial assistance related to the listed goods and technology.

Certain exemptions apply in the case of nonmilitary use and nonmilitary end users, including sales, exports, and so on, for humanitarian or medical purposes, software upgrades, or use as consumer communication devices. In addition, the competent authorities of the EU member states may, for example, grant authorizations, including for nonmilitary use and nonmilitary end users, if the operation relates to electronic communications networks.

1. https://www.legifrance.gouv.fr.
2. https://eur-lex.europa.eu/
3. https://sbdu.entreprises.gouv.fr/fr/demandes-ligne/portail-egide-avec-authentification-forte.
4. https://www.douane.gouv.fr/le-guichet-unique-national-du-dedouanement-gun-generalites.
5. https://www.armscontrol.org/factsheets/wassenaar.
6. https://sbdu.entreprises.gouv.fr/fr/demandes-ligne/portail-egide-avec-authentification-forte.
7. https://www.tresor.economie.gouv.fr/Articles/2021/03/18/le-registre-national-des-gels-se-transforme-pour-faciliter-la-mise-en-oeuvre-des-mesures-de-gel-d-avoirs.
8. Send request to info-gel-subscribe@listes.finances.gouv.fr (subject matter: “Abonnement à la liste Info-Gel”).
9. www.ixarm.com.
10. https://www.ixarm.com/fr/sigale.
11. https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/cryptographie/.
12. See Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique, art. 35.
13. https://finance.ec.europa.eu/eu-and-world/open-strategic-autonomy/extraterritoriality-blocking-statute_en.
14. https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine/frequently-asked-questions-sanctions-against-russia_en.

17

Export Controls and Economic Sanctions in Germany

Bärbel Sachs

17.1 Overview

German trade law is multilayered, complex, and—compared to other jurisdictions—rather restrictive. It is important to understand that most of its complexity results from the division of competences between the European Union (EU)[1] and its member states. This leads to different levels of lawmaking and enforcement in the concerned areas of law.

As the Treaty on the Functioning of the European Union (TFEU) contains an exception for the protection of essential security interests and the trade in military goods,[2] the export controls laws of the EU are divided into (1) controls of war weapons and military goods, which are subject to national law and (2) controls of dual-use goods, which are subject to EU regulation.

Within the EU, enforcement is generally a matter of the member states. As a consequence, national authorities enforce both export controls of military and of dual-use goods. In Germany, the Federal Office for Economic Affairs and Export Controls (*Bundesamt* für *Wirtschaft und Ausfuhrkontrolle*, BAFA) is responsible for most of the enforcement actions.

With regard to economic sanctions law it should be noted that under German law, United Nations Security Council Regulations are directly applicable.[3] Economic sanctions laws within the European Union are

adopted as decisions of the Council within the framework of the Common Foreign and Security Policy and as Council Regulations under Article 215 TFEU. The latter are directly applicable in all EU member states, are binding in their entirety, and take precedence over conflicting measures of a member state. As military goods are subject to national regulations, arms embargos are implemented on a national level in Germany, pursuant to sections 74 *et seq*. German Foreign Trade and Payments Ordinance (*Außenwirtschaftsverordnung*, AWV). The EU member states can adopt national measures going beyond EU sanctions. Germany has currently not made use of this possibility.

In Germany, BAFA is competent to enforce goods-related economic sanctions. However, the German Central Bank (*Deutsche Bundesbank*) is competent to enforce financial sanctions such as asset freezes, the prohibition to make available funds to listed entities, license requirements for financial assistance, as well as payment notifications and authorizations.

What Is Regulated: The following goods are subject to controls: (1) war weapons pursuant to the War Weapons Control Act (*Kriegswaffenkontrollgesetz*, KWKG); (2) military items pursuant to the German Foreign Trade and Payments Act (*Außenwirtschaftsgesetz*, AWG) and its implementing ordinance, AWV; (3) dual-use goods pursuant to the EU Dual-Use Regulation[4] and further national controls laid down in the AWV; (4) goods that can be used for torture;[5] and (5) firearms pursuant to the EU Firearms Regulation.[6]

In addition to controls of listed items, the provisions inter alia also provide controls for the following: exports of nonlisted items for further specified end uses, technical assistance, trafficking and brokering transactions, foreign investments, cross-border payments, and movements of capital.

Where to Find the Regulations:

EU Regulations

- http://eur-lex.europa.eu/homepage.html
- https://www.sanctionsmap.eu/#/main

German Regulations

- https://www.bafa.de/EN/Foreign_Trade/Export_Control/export_control_node.html

Who Is the Regulator: German national laws, as for example, AWG and KWKG, are adopted by the German Bundestag. AWV is adopted by the federal government and the German Federal Ministry for Economic Affairs and Climate Action (BMWK). BAFA, as the licensing authority, adopts general and individual licenses. The German customs authorities are responsible for administering any export procedures.

How to Get a License: In order to receive an export license, an application must be submitted with BAFA. This may be done in writing or via the ELAN K2 online portal. The online portal enables the exporter to process a high number of applications at the same time and create templates for applications of repeating business transactions. The exporter must enter the customs number (EORI) and branch number in the application form. The exporter must submit an End-Use Certificate unless the export is only of temporary nature or in case the export value is below certain thresholds. Any company applying for licenses with BAFA must identify a "person responsible for export." This person must be a member of the top management and will be held personally liable for all breaches of the company for violations of export laws. The only defense available is to demonstrate that adequate procedures to prevent the breach were in place.

Please note that the following types of licenses are available in Germany: individual export licenses, maximum amount licenses, global export license, and general licenses. An individual license permits the shipment of one or several items to one consignee and is based on one order. A maximum amount license is a special type of individual license permitting the shipment to one consignee up to the authorized maximum amount (expected annual sales) on the basis of several orders, for example, in connection with a general contract. Certain exporters may, in accordance with certain conditions, apply for a global export license (*Sammelgenehmigung*, SAG) instead of applying for several individual licenses. The SAG is a privileged procedure for reliable exporters with a high number of foreign trade transactions. A global export license permits the export of a group of items to several consignees. Please further note that

export licenses may be subject to terms and conditions as, for example, time limitations, notification requirements, and so on.[7]

Key Websites:

- BAFA: https://www.bafa.de/EN/Home/home_node.html
- Customs administration: http://www.zoll.de/EN/Home/home_node.html
- EU trade and financial sanctions: https://www.sanctionsmap.eu/#/main

17.2 Structure of the Laws and Regulations

The German Foreign Trade and Payments Act (AWG) is divided into three parts: Part 1 Legal Transactions and Actions; Part 2 Supplementary Provisions; and Part 3 Provisions on Penalties, Fines and Surveillance.

The German Trade and Payments Ordinance (AWV) includes the following chapters: Chapter 1 General Provisions; Chapter 2 Export and Transfer from Germany; Chapter 3 Import; Chapter 4 Other Movements of Goods; Chapter 5 Movement of Services; Chapter 6 Restrictions on Movements of Capital; Chapter 7 Reporting Requirements for Movements of Capital and Payments; Chapter 8 Restrictions against Certain Countries and Persons; Chapter 9 Criminal and Administrative Offences; Chapter 10 Transitional Arrangements, Evaluation and Entry into Force, Expiry.

The AWV currently has 19 annexes, of which Annex 1 AL is particularly noteworthy. This annex contains the list of military goods and nationally listed dual-use items.

17.3 What Is Regulated: Scope of the Regulations

(a) Special Regime for War Weapons

First, it should be mentioned that Germany has adopted very strict rules concerning the control of so-called war weapons. These are listed as an Annex to the KWKG and include nuclear, biological, and chemical weapons; combat aircraft; military helicopters; and barrelled weapons. In Germany, it is prohibited to import, export, or transit nuclear, biological,

and chemical weapons; cluster munitions; and anti-personnel mines. Regarding all other war weapons, the KWKG sets up very restrictive rules with regard to their handling, including production, sale, transport, and so on. In the following, we have set out the export controls regime for regular military goods only.[8]

(b) Exports

Under the German Foreign Trade and Payments Ordinance, the export of listed items is subject to a license. Part I section A of the Export List[9] contains the German Military List; it is based on the Control List under the Wassenaar Arrangement and largely adopts the Common Military List of the European Union. Part I section B of the Export List supplements the EU Dual-Use List, containing goods such as flow-forming machines destined for Syria or trucks with a payload of over 1,000 kg destined for the DPRK. Transfers from Germany to another EU member state also require a transfer license. Further, and in addition to provisions of the EU Dual-Use Regulation, the export of nonlisted goods may also be subject to a license requirement, in case these goods are or can be wholly or partly destined for the construction or the operation of a facility for nuclear purposes or for installation in such a facility and the country of destination is Algeria, Iran, Iraq, Israel, Jordan, Libya, the Democratic People's Republic of Korea, Pakistan, or Syria.

(c) Technical Assistance

With the recast of the EU's Dual-Use Regulation, the scope of the prohibitions was extended to the provision of technical assistance services.[10] Germany has enacted a number of additional restrictions. These cover technical support related to (1) the development, manufacture, handling, operation, maintenance, storage, detection, identification, or spread of (a) chemical or biological weapons or (b) nuclear weapons or other nuclear explosive devices or (c) for the development, manufacture, maintenance, or storage of missiles suited to the launching of such weapons,[11] (2) a military end use being provided in a country subject to a weapons embargo,[12] and (3) the construction or operation of facilities for nuclear purposes in the following countries: Algeria, Iran, Iraq, Israel,

Jordan, Libya, the Democratic People's Republic of Korea, Pakistan, or Syria.[13] Similar restrictions apply for technical support in connection with goods used for communication surveillance.[14]

(d) Brokering Services

It must be emphasized that exports from one third (non-EU) country to another may also require a trafficking and brokering license under the rules for trafficking and brokering transactions. According to section 46 AWV, any trafficking and brokering transaction relating to listed military items that is at least partially carried out in Germany is subject to a license requirement. Trafficking and brokering transactions are quite broadly defined as "(i) the brokering of a contract on the acquisition or release of goods, (ii) the documentation of an opportunity to conclude such a contract or (iii) the conclusion of a contract on the release of goods." In practice, these provisions frequently lead to requirements for the inter-company business of multinational companies. Please note that in special cases section 46 also applies to trafficking and brokering transactions carried out in a third country by German nationals with a residence or habitual abode in Germany. This includes in particular trafficking and brokering transactions with regard to specifically mentioned war weapons and ammunition or goods used for communication surveillance.[15]

(e) Sanctions and Embargoes

As previously stated, Germany has not passed any sanctions going beyond the sanctions and embargoes adopted by the European Union. However, due to the division of competences, sections 74 *et seq*. AWV currently implement arms embargoes against the following countries: Belarus, Burma/Myanmar, Central African Republic, Democratic Republic of the Congo, Democratic People's Republic of Korea, Iraq, Iran, Lebanon, Libya, Russia, Somalia, Sudan, South Sudan, Syria, Venezuela, and Zimbabwe.

(f) Re-exports

The legal provisions do not contain any rules relating to re-exports. Re-exports are controlled by way of end-use certificates: The initial export from Germany will only be licensed based on an end-use certificate

provided by the recipient of the items. The language of these end-use certificates differs according to the goods or technology to be exported. The end user of the goods certifies not to re-export the goods to a third country without prior approval of BAFA. In some cases, the export to certain third countries is exempted from this rule.[16] The only way to sanction violations of these end-use undertakings is to question the end user's reliability. Further exports to an unreliable end user will not be licensed.

17.4 Who Is Regulated?

In essence, German foreign trade and payments law may be applicable to (1) German citizens, (2) residents, and (3) with respect to any business at least partly carried out with the Federal Republic of Germany. Residents include (1) natural persons resident or habitually resident in Germany, (2) legal persons and partnerships based or headquartered in Germany, (3) branches of foreign legal persons or partnerships if the headquarters of the branch are in Germany and separate accounts are kept for them, and (4) permanent establishments of foreign legal persons or partnerships in Germany if the permanent establishments are administered in Germany.[17]

When looking at the scope of application of individual provisions, German foreign trade and payments law is more complex. In general, German law adopts a territorial scope of application.[18] This means that German law is applicable with regard to any business that is carried out at least partially on the territory of the Federal Republic of Germany. However, German foreign trade and payments law has an even wider scope of application: The rules on trafficking and brokering transactions are in part applicable not only in Germany but also in non-EU countries for persons with (1) German citizenship and (2) habitual abode in Germany. Further, the rules on technical assistance are applicable to German citizens and residents for services carried out in (1) Germany,[19] (2) in third (i.e. non-EU) states,[20] or (3) irrespective of the location.[21] In accordance with these rules, section 18 paragraph 10 AWG extends criminal liability to acts carried out outside of Germany irrespective of whether the act constitutes a crime under local law.

17.5 Classification

A reliable classification process is the heart of any internal trade compliance program. An incorrect classification of goods can, in the worst case, trigger a high number of exports control law violations. In practice, the correct classification requires thorough legal knowledge of the relevant lists as well as an accurate technical knowledge of the items concerned and their intended end-use.

The German Military List follows the model of the Common Military List of the European Union[22] for most numbers. This list follows the model of the Munitions List agreed upon within the framework of the Wassenaar Arrangement.[23] It contains items ranging from "Smooth-bore weapons with a calibre of less than 20 mm" (No. 0001) to Cryogenic and "superconductive" equipment (No. 0020) as well as software (No. 0021) and technology (No. 0022). Specially designed components as well as accessories for controlled items are very often also controlled. Please note that many terms used in the list are legally defined. Definitions of terms between 'single quotation marks' are laid down in a Technical Note to the relevant item; definitions of terms between "double quotation marks" are laid down in the general notes preceding the list of items.

Many of the items on the military list are only controlled if specially designed for military purposes. As in any other jurisdiction, the concept of specially designed has been debated controversially. According to case law, not the producer's subjective intention at the time of the production needs to be taken into account, but the objective characteristic of construction of the final goods, at the point in time of the particular export.[24]

The German authorities have developed a conversion table as a tool to identify items subject to export controls.[25] It provides some indication on those items (as classified according to the Combined Nomenclature[26] for tariff classification purposes) falling under specific numbers of the Military and EU Dual-Use Lists. However, this table is not legally binding and does not exempt an exporter from the duty to carefully check each item against the lists.

17.6 General Prohibitions/Restrictions/Requirements

German export control law does not have general prohibitions similar to the ones contained in the EAR. However, certain provisions under the European Union embargo and sanctions law have a similar effect; certain exports are prohibited and it is not possible to obtain a license.[27] Please note that some of the export restrictions under EU sanctions law are subject to exceptions, for example, grandfathering clauses for contracts that have been concluded prior to the adoption of the sanctions.[28]

17.7 Licensing/Reasons for Control

BAFA will take into account the following considerations when deciding on whether to grant an export license: considerations of foreign policy, national security interests, intended end use, the exporter's and the end user's reliability, and so on. The duration of the licensing procedure largely depends on the facts and circumstances of the individual case and may take more than a month, in particular in case of exports to countries that are not NATO member states or states of equivalent status.[29] In these cases, more thorough investigation and, if necessary, the participation of the competent federal ministries is required.

17.8 General Licenses/License Exceptions

(a) General Licenses

BAFA makes frequent use of general licenses. They are published by BAFA in the Federal Gazette (*Bundesanzeiger*) and are subject to registration and notification requirements. A general license's scope is usually limited to specific items and specific destinations. Currently there are 29 general licenses available, eight of which have been provided for in EU Regulations (EU001-EU008), for example, for dual-use and military goods to certain states or temporary exports for trade fairs.[30]

In addition to the general licenses of the EU, national general licenses exist that only apply in case the EU general licenses are not applicable. Those national general licenses apply to the export of goods below the threshold of EUR 5,000 (No. 12); special cases of export such as the import of goods or technology into the EU and unmodified re-export to the country

of consignment without customs clearance or if re-exported within six months (No. 13); certain valves and pumps (No. 14); certain dual-use exports to the UK (No. 15); the export of telecommunication and information security goods (No. 16); frequency converters (No. 17); clothing and equipment with signature suppression (No. 18); the export/transfer of cross-country vehicles (No. 19); trafficking and brokering transactions concerning armaments (*Rüstungsgüter*) (No. 20); the export/transfer of protective equipment (No. 21); the transfer of explosives (No. 22); the re-export of armaments (No. 23); the temporary transfer of armaments (No. 24); the export/transfer of armaments in certain cases (No. 25); the transfer to EU member states (No. 26); the transfer of armaments to certified companies pursuant to No. 9 of the Regulation (EC) No. 2009/43/EG[31] (No. 27); exports of certain military goods to France and Spain (No. 28); to certain nonsensitive business with Iran (No. 30); to public contracts or concessions made in accordance with Article 5k (2) Reg (EU) 833/2014[32] (No. 31); and to exports of protective equipment to Ukraine (No. 32).

If the requirements of one of the general licenses of the EU Nos. EU 001 to 008 are fulfilled, those will apply regardless of the national general licenses. In this case, the exporter may not export/transfer goods in accordance to national general licenses or file a license with the BAFA. If no general license of the EU applies, the exporter may check if the requirements of any of the national general licenses are met. The exporter may decide which general license shall apply if the transaction falls within the scope of more than one general license.

The use of each general license requires a unique registration with the BAFA using the ELAN K2 portal. The one-time registration does not need to be repeated in cases of amendments or extensions of the respective general license. Some general licenses require a semi-yearly notification to the BAFA declaring the number of exports/transfers carried out and the general license that applied to each export/transfer.

(b) License Exceptions

Regarding controls of listed items, the German legislator decided to refrain from license exceptions and rather makes use of general licenses. The

statutory provisions on license requirements regarding exports of military items or technical support contain only very limited exceptions.

17.9 Penalties, Enforcement, and Voluntary Disclosures

There are graded penalty levels for different kinds of trade law violations. There are two types of penalties for the breach of foreign trade law, including export controls and sanctions law: (1) criminal penalties and (2) administrative penalties. Violations of export prohibitions, license requirements, or asset freezes committed with intent may entail a prison sentence ranging from three months to five years. Negligent violations and other trade law breaches may entail administrative fines capped at EUR 500,000 or EUR 30,000 per breach depending on the kind of prohibition. Further, the turnover arising from trade law violations can be subject to criminal or administrative asset forfeiture provisions.

Voluntary disclosure of breaches of export prohibitions or license requirements will not automatically entail (partial) relief from penalties. This effect is only available for other, less severe breaches of foreign trade law. In practice, courts and prosecution bodies afford some mitigation credit to a party that submits a voluntary disclosure when assessing the penalties. There are no formal procedures for self-disclosure.

It should be noted that many foreign trade law violations are discovered by the authorities when carrying out foreign trade audits at a company. The main customs offices conduct foreign trade audits on a regular basis and look into the companies' books and records in order to review trade compliance.

17.10 Recent Export Enforcement Matters

Please note that few enforcement matters get published in Germany. The Customs Administration is authorized to enforce minor violations of export controls and sanctions law and conduct fine procedures. In case criminal sanctions are at stake, the cases need to be passed on to the public prosecutor. Very often, procedures will be discontinued in exchange for the acceptance of a sanction. Unless the case goes to court—for example, because a criminal sanction is at stake, or because the concerned company

individual does not accept a fine, no information on these cases will be publicly available.

In 2019, the BGH confirmed a decision of the District Court in Stuttgart, which decided on a prison sentence of two years for the unauthorized export of rifles. It decided that the defendant could not rely on an error about the classification as a war weapon. Particularly where a case poses complex factual and recognizably difficult legal questions, a detailed, written expert opinion is regularly required in order to establish an unavoidable error.[33]

In 2021, the BGH upheld a judgment by the Kiel District Court sentencing three defendants to prison sentences ranging from ten months to one year and six months and ordering the forfeiture of around EUR 11,000,000. In this case, the company had exported pistols to the United States, knowing they would be reexported to Colombia, while relying on an End-Use Certificate stating the items would remain in the United States.[34]

A recent judgment by the Dresden Appellate Court resulted in a prison sentence of three years and three months for the defendant. He was found guilty of exporting unlisted dual-use goods to recipients based in the Russian Federation in violation of Article 4 (1) Regulation (EC) 428/2009. Additionally, proceeds of almost EUR 1,000,000 were forfeited.[35]

17.11 Further Restrictions

Three kinds of further restrictions of international trade are worth mentioning: (1) Germany has passed a blocking law that prohibits to declare compliance with foreign sanctions laws. (2) As does an increasing number of other nations, Germany controls foreign investments in German companies. (3) Finally, German foreign trade and payments law also sets up notification requirements for cross-border payments and capital movements.

(a) Blocking Laws

Germany has imposed a blocking law that prohibits declaring compliance with foreign boycott laws. Section 7 sentence 1 AWV reads as follows: “The issuing of a declaration in foreign trade and payments transactions whereby a resident participates in a boycott against another country

(boycott declaration) shall be prohibited." The scope of application exempts declarations made to satisfy the requirements of an economic sanctions measure adopted by a third state against another if the latter is also subject to sanctions imposed by the United Nations Security Council under Chapter VII of the Charter of the United Nations (No. 1), by the Council of the European Union under Chapter 2 of the Treaty on European Union (No. 2), or by the Federal Republic of Germany (No. 3).

The German blocking law stands next to the EU Blocking Regulation,[36] whose Article 5 prohibits compliance by persons listed in Article 11 with third states' laws listed in the annex.[37]

Violations of section 7 AWV as well as the EU Blocking Regulation constitute administrative offences that may entail an administrative fine of up to EUR 500,000 per breach. Under German contract law, clauses in violation of this prohibition are null and void.[38]

(b) Foreign Investments

As does an increasing number of countries, Germany controls foreign investments in domestic companies. The Federal Ministry for Economic Affairs and Climate Action (*Bundesministerium* für *Wirtschaft und Klimaschutz*, BMWK) has powers to review and prohibit or restrict certain transactions for reasons of public order or security. Generally, the BMWK can review investments in all sectors (cross-sectoral investment screening). Special rules apply for investments in the defense and cryptology-related sectors (sector-specific investment screening).

The cross-sectoral investment screening applies to investors not resident in an EU member or EFTA state. The rules also cover indirect investments in which a domestic entity owned by a non-EU/EFTA-company acquires a German company. The sector-specific investment screening applies to any foreigner, including cases where the investor has its seat or residence in a EU member or EFTA state.

Cross-sectoral investment screening applies to acquisitions of assets or shares at different thresholds depending on the activity of the acquired company: investments in any company may be screened at a threshold of 25 percent.[39] Target companies in a group of sectors enumerated in section 55a paragraph 1 Nos 8-27 AWV, for example, emerging technologies, health technology, or large agricultural businesses, are subject to a 20 percent

threshold.[40] A 10 percent threshold applies to investments in companies active in the critical infrastructure of certain sectors[41] and to further case groups listed by section 55a paragraph 1 Nos 2-7 AWV.[42] Investments subject to the 10 percent or 20 percent thresholds entail mandatory notification of the BMWK and a closing prohibition;[43] the BMWK may initiate an ex officio screening for any other acquisition subject to the 25 percent threshold. If the BMWK concludes that an acquisition has a *likely effect on the public order or security of the Federal Republic of Germany, of another Member State of the European Union or in relation to projects or programmes of Union interest*, it can either prohibit or restrict the investment, provided it has informed the investor of the review within three months after conclusion of the acquisition contract.[44]

Sector-specific investment screening applies only to the defense and encryption sectors. Foreign investors must notify to the BMWK any acquisitions of 10 percent or more of the shares of enterprises that produce or develop (1) goods subject to the German war weapons control laws; (2) certain IT-security products; (3) specifically designed motors or gears for combat tanks and other armored military vehicles, (4) certain items listed on the German Military List, and (5) items listed on the German Military List if they are intended for the production of goods listed under (4).[45] Such investments are also subject to a notification requirement and a closing prohibition.[46] In the sector-specific investment screening procedure, BMWK can prohibit or restrict acquistions *in order to uphold essential security interests of the Federal Republic of Germany*.[47]

(c) Notification Requirements for Cross-Border Payments and Capital Movements

Finally, it should be noted that German foreign trade and payments law provides for a number of reporting obligations with regard to certain cross-border (1) capital movements, (2) shareholdings, and (3) claims and liabilities. In particular, the following reports need to be made to Deutsche Bundesbank:

(i) Cross border incoming and outgoing payments, except for payments (a) not exceeding EUR 12,500; (b) payments for the import, export, or transfer of goods; or (c) payments for the granting, receipt, or

repayment of loans with an originally agreed term of not more than 12 months.[48]

(ii) Assets of a domestic company if (a) at least 10 percent of the shares or voting rights in the domestic company are to be attributed to a foreigner, and (b) the total balance sheet exceeds EUR 3 million.[49] Likewise, German residents need to file reports for similar assets held abroad.[50]

(iii) Claims and liabilities with regard to foreigners must be reported if the aggregate sums of these claims or liabilities total more than EUR 5 million at the end of a month.[51]

---

1. *See* Chapter 7, Export Controls and Economic Sanctions in the European Union.
2. Article 346(1) TFEU.
3. Alain Pellet & Alina Miron, *Sanctions*, *in* MAX PLANCK ENCYCLOPEDIA of PUBLIC INTERNATIONAL LAW 45.
4. Regulation (EU) 2021/821 of the European Parliament and of the Council of May 20, 2021, setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) (OJ L 206 11.6.2021, p. 1) as amended.
5. Regulation (EU) 2019/125 of the European Parliament and of the Council of January 16, 2019, concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment (OJ L 030, 31.1.2019, p. 1).
6. Regulation (EU) No. 258/2012 of the European Parliament and of the Council of March 14, 2012, implementing Article 10 of the United Nations' Protocol against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition, supplementing the United Nations Convention against Transnational Organised Crime (UN Firearms Protocol), and establishing export authorization, and import and transit measures for firearms, their parts and components and ammunition (OJ L 94, 30.3.2012, p. 1).
7. *See* Article 6(2) Dual-Use Regulation, section 14(1) AWG.
8. For the European Union regulations on dual-use goods, please see Chapter 7, Export Controls and Economic Sanctions in the European Union.
9. Annex I, part I A, AWV.
10. *See* Articles 6(1) and 8(1) Dual-Use Regulation.
11. Section 49 para. 1 AWV.
12. Section 50 para. 1 AWV.
13. Section 52 para. 1 AWV.
14. See sections 52a and 52b AWV.
15. *See* Section 17.1 in this chapter, and Sections 52a and 52b AWV.
16. https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_eve_ausfuellanleitung_eng_ruestungsgueter.pdf?__blob=publicationFile&v=12.
17. Section 2 para. 15 AWG.
18. *Compare, e.g.*, Section 3 German Criminal Code and Section 30 para. 1 German Social Code I.
19. Section 51 AWV.
20. Sections 49, 50, 52a, 52b AWV.
21. Section 52 AWG.

22. Common Military List of the European Union adopted by the Council on February 17, 2020 (equipment covered by Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment) (updating and replacing the Common Military List of the European Union adopted by the Council on February 18, 2019) (CFSP), OJ C 85, 13.3.2020, p. 1.

23. https://www.wassenaar.org/control-lists/.

24. VG Frankfurt, Judgment dated May 23, 1996, upheld by the Higher Administrative Court of Kassel, Decision dated January 10, 2000—8UE 5098/96.

25. https://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Gueterlisten/gueterlisten.html.

26. Regulation (EEC) No. 2658/87 as amended latest by Commission Regulation (EU) 2020/1369 dated September 29, 2020 (OJ L 319, 2.10.2020, p. 2).

27. For current weapons embargoes and EU sanctions law, please see Chapter 7, Export Controls and Economic Sanctions in the European Union.

28. *See, e.g.* Article 2 para. 5 Council Regulation (EU) No 833/2014 of July 31, 2014, concerning restrictive measures in view of Russia's actions destabilizing the situation in Ukraine (OJ L 229, 31.07.2014, p. 1).

29. Australia, New Zealand, Japan, and Switzerland.

30. *See* Chapter 7, Export Controls and Economic Sanctions in the European Union.

31. *See* http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02009L0043-20150105&qid=1460557883313&from=DE.

32. *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0833-20220604.

33. BGH, decision of July 23, 2019 – 1 StR 433/18.

34. BGH, decision ofJuly 1, 2021 – 3 StR 518/19.

35. OLG Dresden, decision of July 15, 2022 – 4 St 1/22.

36. Regulation (EC) No. 2271/96 of November 22, 1996, protecting against the effects of the extraterritorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom (OJ L 309, 29.11.1996, p. 1) as amended.

37. *See* Chapter 9.

38. Section 134 German Civil Code.

39. Section 56 para. 1 Nr. 3 AWV.

40. Section 56 para. 1 Nr. 2 in connection with section 55a para. 1 Nos 8-27 AWV.

41. Energy, information technology and telecommunications, transport and haulage, health, water, nutrition, finance and insurance, and municipal waste management; see section 2 para. 10 Nr. 1 Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, BSI Act).

42. Section 56 para. 1 Nr. 1 in connection with section 55a para. 1 Nos 1-7 AWV.

43. Section 15 para. 4 AWG.

44. Sections 55 para. 1, 59 para. 1 AWV.

45. Section 60 para. 1 AWV.

46. Section 15 para. 4 AWG.

47. Sections 60 para. 1, 62 para. 1 AWV.

48. *See* section 67 AWV.

49. *See* section 65 AWV.

50. *See* section 64 AWV.

51. *See* section 66 AWV.

18

Export Controls and Economic Sanctions in Hong Kong

Michael Cheung[1]

18.1 Overview

What Is Regulated: Hong Kong is a free port. Under the "One Country, Two Systems" principle, Hong Kong is a special administrative region of the People's Republic of China, and under its current laws, Hong Kong will be a separate legal jurisdiction and customs territory from the People's Republic of China for 50 years until 30 June 2047. The enactment of the Law of the People's Republic of China on Safeguarding National Security in Hong Kong by the Standing Committee of the National People's Congress in Beijing on June 30, 2020, bypassing the legislature in Hong Kong, has raised international concerns about Hong Kong's autonomy. As a result, the United States ended certain license exceptions for export/re-export to or transfer within Hong Kong with effect from June 30, 2020, and as of December 23, 2020, treats Hong Kong virtually in the same manner as the People's Republic of China. The European Union and a few other countries have followed suit to implement new export restrictions to Hong Kong.

However, so far there is no change to Hong Kong's import and export licensing control and economic sanctions laws. The Hong Kong government encourages the free flow of goods. Traders are advised to liaise with the exporters/manufacturers to obtain the necessary export authorization according to the latest requirements. It is yet to be seen if

Hong Kong will make any change to its laws in response to these new developments. Therefore, it is advisable to monitor the situation and seek Hong Kong counsel's assistance to ensure compliance with the conditions imposed in the export authorization in moving controlled items into, within, or out of Hong Kong.

In respect of the trade of dual-use and military products and technologies, Hong Kong's control lists of strategic commodities set out what items are regulated, and includes the following categories:

- Munitions list
- Dual-use goods list
  - Category 0: Nuclear Materials, Facilities and Equipment
  - Category 1: Special Materials and Related Equipment
  - Category 2: Materials Processing
  - Category 3: Electronics
  - Category 4: Computers
  - Category 5 (Part 1): Telecommunications
  - Category 5 (Part 2): Information Security
  - Category 6: Sensors and Lasers
  - Category 7: Navigation and Avionics
  - Category 8: Marine
  - Category 9: Aerospace and Propulsion
- Other items that are intended for use in the production, development, or use of weapons of mass destruction.

Hong Kong's control lists are updated from time to time to reflect the changes adopted by international nonproliferation regimes such as the Wassenaar Arrangement, the Australia Group, the Missile Technology Control Regime, and the Nuclear Supplies Group. Hong Kong is not technically a member of these regimes but follows their controls. The last few updates were made in 2017, 2015, 2013, 2011, and 2021. By closely following the control thresholds adopted by the international nonproliferation regimes, Hong Kong upholds controls consistent with the international standards while relieving traders from licensing requirements when the international standards are relaxed. The policy goals of Hong Kong's licensing control is to maintain the confidence of technology-supplying countries so as to ensure Hong Kong's continued access to high technology.

Where to Find the Regulations: The Import and Export Ordinance (Chapter 60 of the Laws of Hong Kong) and its subsidiary legislation, the Import and Export (Strategic Commodities) Regulations (Chapter 60G of the Laws of Hong Kong) are the legal basis for the control in Hong Kong. The full texts are available in both English and Chinese, which are the two official languages in Hong Kong, at the Hong Kong e-legislation website.[2] In addition, the website of the Strategic Commodities Control System of the Trade and Industry Department of the Hong Kong government contains hyperlinks to the regulations.[3]

Who Is the Regulator: Hong Kong's strategic commodities import and export licensing system is administered by the Trade and Industry Department and enforced by the Customs and Excise Department of the Hong Kong government.

How to Get a License: Under the Import and Export Ordinance (Chapter 60 of the Laws of Hong Kong), subject to certain exceptions, a person who imports or exports an article specified in the control lists except under and in accordance with an import or export license issued by the Trade and Industry Department commits an offence. Applications for the import or export licenses should be made by the importer or exporter of record, who must hold a Hong Kong business registration certificate or be an individual living in Hong Kong. The signed application form, together with a set of supporting documents such as datasheet and foreign exporting country's export authorization, may be submitted in paper form or through the electronic service offered by the Trade and Industry Department.[4] Applications are free of charge. Typically a license may be issued in around two weeks after all required documents have been submitted. For license applications in respect of an item for which a license was previously issued by the Trade and Industry Department, a new license under a repeat application may be granted as quickly as in three working days, provided the classification under the previous license is provided in the application form. In practice, if the application for a repeat import/export does not provide the classification in the previous license, it will be processed as a fresh item and the processing time will still be around two weeks after all required documents have been submitted.

Key Websites: The strategic commodities control system website of the Trade and Industry Department at https://www.stc.tid.gov.hk provides a comprehensive overview of Hong Kong's control regime, links to the legal basis of control, application forms and circulars.

The website of the Hong Kong Customs and Excise Department contains a page on the control on strategic commodities at https://www.customs.gov.hk/en/trade_controls/control/index.html, which provides information about recent enforcement actions.

The business registration number of the applicant can be searched at the Hong Kong government's business registration number inquiry website at https://www.gov.hk/en/residents/taxes/etax/services/brn_enquiry.htm.

The link to the license application electronic service can be found at https://www.stc.tid.gov.hk/english/eaccount/e-account_content.html.

18.2 Structure of the Laws and Regulations

(a) International Treaties

At present, since China is not a member state of the Wassenaar Arrangement, the Australia Group, the Missile Technology Control Regime, or the Nuclear Supplies Group, neither is Hong Kong. On the other hand, since China is a signatory to the Chemical Weapons Convention, this convention applies to Hong Kong pursuant to the Hong Kong Basic Law and this convention has been incorporated into Hong Kong's local legislation. Nevertheless, the control regimes in Hong Kong and China are two different systems. Licenses are required from the exporting of controlled items between Hong Kong and China.

(b) Hong Kong Laws and Regulations on Export Controls

The Import and Export Ordinance (Chapter 60 of the Laws of Hong Kong) and its subsidiary legislation, the Import and Export (Strategic Commodities) Regulations (Chapter 60G of the Laws of Hong Kong), are the legal basis for the control in Hong Kong. The Import and Export Ordinance establishes the licensing control and the offences. The Import and Export (Strategic Commodities) Regulations contain the control lists,

which are updated from time to time to reflect the changes adopted by international nonproliferation regimes.

Other laws and regulations relevant to Hong Kong's control regime include:

- United Nations Sanctions Ordinance (Chapter 537 of the Laws of Hong Kong) and its subsidiary regulations, which provide for the imposition of sanctions against persons and against places outside the People's Republic of China as resolved by the UN Security Council.
- Chemical Weapons (Convention) Ordinance (Chapter 578 of the Laws of Hong Kong), which implements the Chemical Weapons Convention in Hong Kong to control chemical weapons and certain chemicals capable of being used as chemical weapons.
- Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Chapter 526 of the Laws of Hong Kong), which controls the provision of services that will or may assist the development, production, acquisition, or stockpiling of weapons capable of causing mass destruction or that will or may assist the means of delivery of such weapons.
- Firearms and Ammunition Ordinance (Chapter 238 of the Laws of Hong Kong), which provides the licensing requirement for the possession and dealing of arms and ammunition in Hong Kong. A license for possession or dealer's license issued by the Hong Kong Police Force is required for an import or export license involving arms and ammunition to be valid.

(c) Controlled Lists

The Import and Export (Strategic Commodities) Regulations (Chapter 60G of the Laws of Hong Kong) set out Hong Kong's control lists. See https://www.customs.gov.hk/en/trade_controls/control/index.html. There are four schedules in the Import and Export (Strategic Commodities) Regulations:

- Schedule 1 comprises the munitions list and the dual-use goods list.
  - The munitions list covers firearms, ammunition, explosives, bombs and rockets, tanks and toxicological agents, etc., and equipment and technology for the production of these weapons, etc.

    - The dual-use goods list covers ten categories of dual-use goods as outlined earlier in Section 18.1.
- Schedule 2 sets out the more sensitive items in Schedule 1 to which the licensing exceptions of articles in transit and articles of air transshipment cargo do not apply.
- Schedules 3 and 4 bring end use under control. Items not included in Schedules 1 or 2 are still subject to the licensing control if they are intended for use in the production, development, or use of weapons of mass destruction. Schedule 3 sets out the relevant items. Schedule 4 sets out the activities related to the items listed in Schedule 3 that are subject to control.

(d) Hong Kong and UN Security Council Sanctions

Under the United Nations Sanctions Ordinance (Chapter 537 of the Laws of Hong Kong), sanctions include complete or partial economic and trade embargoes, arms embargoes, and other mandatory measures decided by the UN Security Council, implemented against a person or against a place outside the People's Republic of China. The countries and persons subject to such sanctions are posted and updated at the website of the Commerce and Economic Development Bureau of the Hong Kong government.[5]

18.3 What Is Regulated: Scope of the Regulations

Items covered by the munitions list and the dual-use goods list as set out in Schedule 1 of the Import and Export (Strategic Commodities) Regulations are regulated. An import or export license is required before any of these items are imported into or exported from Hong Kong. Please see Section 18.8 for license exceptions.

Items not included in Schedules 1 or 2 of the Import and Export (Strategic Commodities) Regulations are still subject to the licensing control if they fall under Schedule 3 and are intended for the activities set out in Schedule 4, which relate to the production, development, or use of weapons of mass destruction. The end-use control applies not only to the items falling under Schedule 3 but also to technological documents containing information relating to them. The end use must be declared in the application form for the import or export license. It is one of the

conditions for the issue of an import or export license that the goods covered by the license shall not be used in relation to nuclear, biological, or chemical weapons or missiles capable of delivering these weapons.

18.4 Who Is Regulated?

Under the Import and Export Ordinance, “import” means to bring, or cause to be brought, into Hong Kong any article, and “export” means to take, or cause to be taken, out of Hong Kong any article. Persons subject to the licensing control include the importer of record, the exporter of record, the freight forwarders, and individuals who hand carry the controlled items.

18.5 Classification

(a) Classification of Dual-Use Items

The ten categories of dual-use items under Schedule 1 of the Import and Export (Strategic Commodities) Regulations are set out earlier in the chapter in Section 18.1. Categories 1 to 9 generally follow the dual-use goods list of the Wassenaar Arrangment with some differences in the details because Hong Kong’s dual-use list has incorporated various international nonproliferation regimes. Category 0 is nuclear materials, facilities, and equipment. In each category, the controlled items are further divided into five subcategories: (1) systems, equipment and components; (2) test, inspection, and production equipment; (3) materials; (4) software; and (5) technology. There is no reference to HS codes in Hong Kong’s dual-use goods list.

(b) Classification of Military Items

Hong Kong’s munitions list generally follows the munitions list of the Wassenaar Arrangment with 22 sub-categories, from ML1 to ML22.

(c) Pre-Classification Service

An item’s control status is known if an export authorization has been obtained in the exporting country or the product’s originating country, or if

an import authorization has been obtained from the final destination. If the control status is unknown or uncertain before exporting to Hong Kong, anyone in Hong Kong (which does not have to be the importer or exporter of record) may submit a pre-classification application to the Trade and Industry Department to determine whether an item is subject to Hong Kong's import/export licensing requirement and the category number if it is a controlled item. Pre-classification applications may be submitted in paper form or through the electronic service offered by the Trade and Industry Department.[6] Pre-classification is free of charge. The result of pre-classification is an official document and a useful tool to reduce compliance risk. For products classified as not controlled, they can be imported or exported without a license. For products classified as controlled, a pre-classification reference number will be assigned, which will help with the speedy issue of the requisite import or export license.

18.6 General Prohibitions/Restrictions/Requirements

The issue of a Hong Kong import/export license is subject to a few conditions as stated on the import/export license, including the following:

- The goods covered by the license are not to be used in relation to nuclear, biological, or chemical weapons or missiles capable of delivering these weapons.
- Prior approval from the Trade and Industry Department is required if the goods covered by the license are not for civil end use.
- For Hong Kong import license:
  - Re-export of the goods imported under an import license must be covered by an export license if the goods are controlled at the time of export.
  - Part shipments are allowed, in which case the importer must notify the Trade and Industry Department. When the balance of the consignment covered by the import license is imported, the original of the import license (carrier's copy) must be given to the shipping, airline, or transportation company.
  - Any further re-export, resale, or transfer of the goods for the use by a government end user requires prior approval from the Trade and Industry Department.

- For Hong Kong export license:
  - Exporters should check with the manufacturer/foreign exporter of the goods to ensure that there is no re-export control by the government of the products' foreign exporting country or originating country, or a valid re-export authorization has been obtained.
  - The export license only authorizes export to the stated consignee for civil end use. Any change of end user or end use, or further re-export, resale, transfer, or disposal of the goods is subject to the authorization of the original exporting government.

18.7 Licensing/Reasons for Control

(a) Types of Export Control Licenses and Permits for Dual-Use Item

An import license must be obtained before the import of controlled items into Hong Kong. The arrival date and the vessel/flight/vehicle number can be stated on the application for an import license if they are known. It is acceptable to state that the arrival date is to be determined. An import license is generally valid for six months from the date of issue. A new import license must be applied for if it is not used upon the expiry.

An export license must be obtained before the export of controlled items from Hong Kong. The departure date and the vessel/flight/vehicle number can be stated on the application for an export license if they are known. It is acceptable to state that the departure date is to be determined. An export license is generally valid for three months from the date of issue. An export license is consignment based and no part-shipment is allowed.

(b) Export Control Licensing Procedure

The application for an import or export license can be submitted in paper form to the Trade and Industry Department or submitted online if the importer/exporter of record has opened an E-Account with the Trade and Industry Department.[7] The application package includes:

- An application form in the prescribed form that has been signed and chopped by the importer/exporter of record. Some of the information to be declared on the application form includes:
  - End use and the contact information of the end user;
  - Export authorization of the foreign exporting country or the product's originating country;
  - Details of the goods, including the brand name, part number, description, number of units, CIF value in Hong Kong dollars.
- A copy of the applicant's business registration certificate if it is a business, or the applicant's Hong Kong identity card or passport if the applicant is an individual;
- Datasheet;
- A copy of the export authorization of the foreign exporting country or the product's originating country;
- A cryptography questionnaire completed and signed by the brand owner/manufacturer for classification of cryptography products;
- Other supporting documents as required by the Trade and Industry Department such as an end-user statement.

Upon receiving an application, the Trade and Industry Department will issue an application receipt with a receipt number, which can be used to check the application status. The Trade and Industry Department will return the application package if amendments or additional supporting documents are required. With appropriate amendments and additional supporting documents as required, the application is resubmitted. In practice, amendments may be written by hand on the application form with the applicant's company chop stamped next to each amendment. Import or export licenses will be issued in duplicate, with one original being the importer/exporter's copy and the other original being the carrier's copy. Hard copies of the original license are collected at the Trade and Industry Department by handing in the original application receipt.

(c) Import and Export Licenses for Military Items

It is a general requirement that goods covered under an import or export license will only be used by or transferred to civil end users for civil end uses. Any reexport, resale, or transfer of the goods for use by government end users requires prior approval by the Trade and Industry Department. If

the military items are arms and ammunition under the control of the Firearms and Ammunition Ordinance (Chapter 238 of the Laws of Hong Kong), the validity of the import or export license is subject to the issuance of a valid license for possession or dealer's license by the Hong Kong Police Force.

(d) Export Permits and Independent Expert Examination

There is no self-classification or independent expert examination under Hong Kong's control regime. The Trade and Industry Department maintains a database of items that have been classified through past license or pre-classification applications and the database may be shared with the Hong Kong Customs and Excise Department. In enforcing Hong Kong's control requirements, the Hong Kong Customs and Excise Department will seek the opinion of the Trade and Industry Department to determine if any goods imported into or exported from Hong Kong are subject to the licensing requirement.

18.8 General Licenses/License Exceptions

(a) General Licenses

As a trade facilitation measure, the Trade and Industry Department selects[8] frequent users of strategic commodities licenses for items in Category 3 or Category 5 with a good compliance record to participate in its approval-in-principle arrangement for bulk users of strategic commodities licensing service to streamline the licensing procedure. The approval-in-principle arrangement is applicable to companies that frequently import a less-sensitive product from the same supplier or frequently export a less-sensitive product to the same consignee. The approval in principle is valid normally for one year and may be reapplied for before its expiry. Each approved participant must have an e-account with the Trade and Industry Department. Within the scope of the approval-in-principle, an import or export license application can be filed online before each shipment without the supporting documents normally required for an application. The application will be processed automatically, and once approved, the license will be issued electronically.

(b) License Exceptions

There are exceptions to the licensing requirement for articles in transit and articles of air transshipment cargo:

- An article in transit means an article that is brought in to Hong Kong solely for the purpose of taking it out of Hong Kong and remains at all times in or on the vessel or aircraft in or on which it is brought into Hong Kong. However, the articles in transit do not apply for the more sensitive items set out in Schedule 2 of the Import and Export (Strategic Commodities) Regulations.
- Air transshipment cargo means transshipment cargo that is both imported and consigned for export in an aircraft and which, during the period between its import and export, remains within the cargo transshipment area of the Hong Kong International Airport. However, the articles in air transshipment cargo do not apply for the more sensitive items set out in Schedule 2 of the Import and Export (Strategic Commodities) Regulations.

Certain exceptions such as personal use and mass market products are provided in Schedule 1 the Import and Export (Strategic Commodities) Regulations. In practice, claims for such exceptions need to be approved by the Trade and Industry Department with supporting evidence. There are no license exceptions for temporary import or export.

18.9 Penalties, Enforcement, and Voluntary Disclosures

(a) Administrative Penalties

The Trade and Industry Department has no administrative power to impose any fines. It may cancel, revoke, or suspend a license if any of the conditions of the license are breached.

(b) Criminal Penalties

The export or import of any strategic commodities without a requisite license is a strict liability offence in Hong Kong, punishable (1) on summary conviction to a fine not exceeding HK$500,000 and to

imprisonment for a term not exceeding two years; and (2) on conviction on indictment to an unlimited fine and to imprisonment for a term not exceeding seven years. Criminal penalties may be imposed only by a court in Hong Kong. The case will be prosecuted in the Hong Kong court and the sentence is decided by the judge. A party unsatisfied with the decision has the right to appeal before the decision is finalized. The controlled items will be seized and forfeited by the Hong Kong Customs and Excise Department under the Import and Export Ordinance if they have entered into Hong Kong but have not been cleared with the customs.

(c) Enforcement

Criminal investigations are initiated by the Hong Kong Customs and Excise Department. Generally the investigations are friendly, involving prearranged interviews and voluntary provision of records. It is normally not disputed whether a requisite license has been obtained or whether the items are controlled. During the investigation, the value of the controlled items and the amount of profits (if any) will be determined, which will be relevant to sentencing.

(d) Voluntary Disclosures

There is no legal requirement in Hong Kong for voluntary disclosure of any violation of the law. There are no penalties for nondisclosure or failure to report under Hong Kong law. There is no rule that any legal liability could be exempted by voluntary disclosure.

18.10 Recent Export Enforcement Matters

Recent enforcement statics are published by the Trade and Industry Department and the Customs and Excise Department on their websites. Based on their latest information, the Trade and Industry Department reported that total fines of HK$415,800 were imposed from July to December 2019, and the Customs and Excise Department reported that it prosecuted 57 cases with a total fine of HK$660,000 in 2019. One of the cases prosecuted in 2019 was a high-profile case involving nine armored cars and other military items that belonged to the Singapore government. It

was reported that these military items were used for drills by Singaporean soldiers in Taiwan and were in transit through Hong Kong on their return to Singapore. The items were released and returned to Singapore through diplomatic resolutions. The carrier company was fined for HK$90,000 and the captain of the vessel was fined HK$9,000 and received a suspended prison sentence.

18.11 Special Topics

(a) Re-exports/Extraterritorial Application of Laws

Re-export of the goods imported into Hong Kong under an import license must be covered by an export license if the goods are controlled at the time of export. On the application form for an export license, the applicant must declare that the goods will only be used by or be transferred to civil end users for civil end use. The standard conditions stated on an export license include that the exporter should inform the recipient of all conditions of the export license, prior approval from the Trade and Industry Department is required if the goods covered by the export license are not for civil end use, and that exporters should check with the manufacturer/foreign exporter of the goods to ensure that there is a valid re-export authorization issued by the government(s) of the products' foreign exporting/originating country. Except that any subsequent re-exports should not be for non-civil end use, the Hong Kong export license generally does not impose any condition in relation to subsequent re-exports after the items have been exported from Hong Kong.

(b) Intangible Transfer of Technical Information

Intangible transmission of technical information does not require any import or export license under the current control regime in Hong Kong. At present, Hong Kong's licensing control applies to import and export of specified strategic commodities and their technology in physical and tangible forms (e.g., those recorded on media such as paper, disks, tapes, etc). However, if the technical information relates to the development, production, acquisition, or stockpiling of weapons of mass destruction, intangible transfer through Hong Kong is prohibited under the Weapons of

Mass Destruction (Control of Provision of Services) Ordinance (Chapter 526 of the Laws of Hong Kong). Traders are advised to confirm that there is no prohibition by the authorities of the originating country for any intangible transfer of the technology.

(c) Practical Issues Related to Export Control Clearance

Trade compliance teams are advised to screen the end use, the end user, and the products to ensure compliance. Generally, an internal database can be built for the products that the company has dealt with and know the control status. For new products, the control status may be confirmed with the manufacturer or through the pre-classification service of the Trade and Industry Department. Due diligence should be performed on the customers who seek to purchase controlled items. Nonaffiliated customers should be requested to sign an end-user statement in the Trade and Industry Department's format. In addition, the company should also ensure that there is no UN sanction or prohibition for re-export by the originating country against the customer or the destination.

(d) Recordkeeping

Companies in Hong Kong are required to maintain all documents generated that are related to the import or export of controlled items, including invoices, bills of lading, air waybills, and applications for and copies of import or export licenses. The records may be stored in paper form or electronically as the company deems efficient. Business records shall be retained for a period of not less than seven years from the date of the documents.

(e) How to Be Compliant When Exporting to Hong Kong

A Hong Kong import license is required before a controlled item is exported to Hong Kong. A Hong Kong import license may be required even if the goods are in transit through Hong Kong. It is advisable for the foreign exporter to follow the following steps to be compliant when exporting to Hong Kong:

1. Determine if any item in the shipment is controlled by the exporting country or the originating country and has obtained an export

authorization.
   - Confirm with the manufacturer about the control status and export authorization;
   - For items in the shipment whose control status is uncertain, forward the datasheet to the Hong Kong importer of record for arranging a pre-classification application with the Hong Kong Trade and Industry Department;
   - Do not ship the goods until the requisite Hong Kong import license has been obtained.
2. Ascertain that all items in the shipment will be for civil end use by civil end users.
3. Forward copies of the export authorization and datasheet to the Hong Kong importer of record to apply for a Hong Kong import license.
4. If the result of pre-classification application shows that an import license is required, arrange for the Hong Kong importer of record to apply for a Hong Kong import license.
5. Review the conditions stated on the import license and ensure all of the conditions are complied with during shipment, customs clearance, and transfer in Hong Kong.
6. Inform the Hong Kong importer of record of any re-export restrictions by the authorities of the exporting or originating country.
7. Keep all documents generated during the process.

(f) How to Be Compliant When Exporting from Hong Kong

A Hong Kong export license is required before a controlled item is exported from Hong Kong. It is advisable for the Hong Kong exporter of record to follow the following steps to be compliant when exporting from Hong Kong:

1. Determine if any item in the shipment is controlled under Hong Kong's licensing requirement, for example, if a Hong Kong import license has been obtained when the goods entered into Hong Kong.
   - For items in the shipment whose control status is uncertain, submit a pre-classification application with the Hong Kong Trade and Industry Department;

- Do not ship the goods until the requisite Hong Kong export license has been obtained.

2. Ascertain that all items in the shipment will be for civil end use by civil end users.
3. If the result of pre-classification shows that an export license is required, submit an application for a Hong Kong export license.
4. Review the conditions stated on the export license and ensure all of the conditions are complied with during the exporting process.
5. Inform the foreign consignee of all conditions of the Hong Kong export license.
6. Keep all documents generated during the process.

18.12 Encryption Controls

(a) General Comments

Hong Kong generally follows the Wassenaar Arrangement in controlling encryption products with the current control threshold at a symmetric key length of 56 bits. Encryption products falling under "Category 5 (Part 2)—Information Security" are not included in the more sensitive items in Schedule 2 of the Import and Export (Strategic Commodities) Regulations, and, therefore, can enjoy the articles in transit licensing exception as long as they are brought in to Hong Kong solely for the purpose of taking them out of Hong Kong and remain at all times in or on the vessel or aircraft in or on which they are brought into Hong Kong.

(b) Import Encryption Clearance Requirements

Same as the other categories of controlled items, encryption products subject to the import or export licensing requirements shall only be imported into or exported from Hong Kong under and in accordance with the requisite import or export license. Items accompanying the user and for the user's personal use are exempted from Hong Kong's licensing control. There is also the exemption of mass market products. However, in practice, the mass market exemption should be confirmed with the Trade and Industry Department by submitting the same supporting documents as the application for an import or export license, including the cryptography

questionnaire signed by the brand owner, to ascertain that all the criteria for the mass market exemption are met.[9]

Encryption products imported into Hong Kong shall comply with all the license conditions as stated on the Hong Kong import license. In respect of the end use, an example of the license condition is for stock or resale to civil end users for civil use. A special condition for U.S. origin products is generally imposed to limit the civil end users to nongovernment end users. The possession, sale, or commercial use of such products within Hong Kong is not subject to any licensing requirement as long as the use complies with the license conditions as stated on the import license. If the importer of record is not the end user, it is required under the import license to inform the recipients of the products of all the conditions of the import license. Prior approval from the Trade and Industry Department is required if the products covered by the import license are not for civil end use, or in the case of U.S. origin products, are to be used by any government end user.

(c) Encryption Licensing Requirements

The production and sale of encryption products and software in Hong Kong to civil end users for civil use are not subject to any encryption licensing requirements.

(d) Penalties for Violation of Encryption Regulations

Importing or exporting encryption products subject to the licensing control without or not in accordance with the requisite license is an offence liable (1) on summary conviction to a fine of HK$500,000 and to imprisonment for a term not exceeding two years; and (2) on conviction on indictment to an unlimited fine and to imprisonment for a term not exceeding seven years. In addition, the Trade and Industry Department may impose administrative actions such as suspension of a license, refusal to issue a license, debarment of all licensing services to the relevant companies, and so on.

18.13 Blocking Laws/Penalties for Compliance with Sanction Imposed by Other Countries

There is no blocking law in Hong Kong to restrict the application in Hong Kong of a law made by a foreign jurisdiction. Hong Kong has not legislated to penalize a person who acts in the interest of a foreign country that imposes sanctions against Hong Kong. In 2019, the United States enacted the Hong Kong Human Rights and Democracy Act, which requires, among other things:

- An annual certification by the U.S. Secretary of State regarding the autonomy of Hong Kong;
- A U.S. government report that includes the following:
  - An assessment of the Hong Kong government's enforcement of U.S. law related to export controls, and U.S. and UN sanctions;
  - To the extent possible, an identification of the following:
    - Any items that were transferred from Hong Kong in violation of such laws;
    - The countries and persons to which such items were transferred;
    - How such items were used.
- An assessment of whether U.S. origin items (including software, technology, and services) have been transferred from Hong Kong to China in violation of U.S. law and have been used by China for mass surveillance, predictive policing, or for the social credit system.
  - A description of the types of goods and services transshipped or reexported through Hong Kong to North Korea, Iran, and other countries, regimes, or persons in violation of sanctions.

At the end of May 2020, the U.S. Secretary of State certified to the Congress that Hong Kong no longer enjoys a high degree of autonomy from the People's Republic of China. As a result, the United States has ended certain license exceptions for export/re-export to or transfer within Hong Kong with effect from June 30, 2020, and effective December 23, 2020, has ended the differential treatment of Hong Kong in relation to the People's Republic of China. In effect, the United States now treats Hong Kong and the People's Republic of China as one customs territory. The European Union and some other countries have followed suit to implement new export restrictions to Hong Kong. It is yet to be seen if Hong Kong would make any change to its laws in response to these new developments.

---

1. This Hong Kong chapter is contributed by Michael Cheung of Sam Zhang & Co. (http://www.szlegal.com).

2. https://www.elegislation.gov.hk/.
3. https://www.stc.tid.gov.hk/.
4. https://www.stc.tid.gov.hk/english/eaccount/e-account_content.html.
5. https://www.cedb.gov.hk/citb/en/Policy_Responsibilities/united_nations_sanctions.html.
6. https://www.stc.tid.gov.hk/english/eaccount/e-account_content.html.
7. https://www.stc.tid.gov.hk/english/eaccount/e-account_content.html.
8. Once selected by the Trade and Industry Department, the company will need to submit an application.
9. If the traders have not obtained the Trade and Industry Departments confirmation of mass market status, they risk that the exemption does not apply and therefore their exports will be found to be noncompliant. Hong Kong Customs and Exercise Department, as the enforcement agency, will obtain and rely on the Trade and Industry Department's opinion in its investigations. There is no self classification or self determination of exemption in Hong Kong.

19

Export Controls and Economic Sanctions in India

Sonia Gupta and Ashok Dhingra[1]

19.1 Overview

What Is Regulated: India regulates the export of arms and ammunition, explosives, dual-use items, that is, goods, software, technology, chemicals, weapons of mass destruction (WMD) and export of specified goods or services or technology.

Where to Find the Regulations: The Foreign Trade Policy (FTP), the Hand Book of Procedures to the FTP (HBoP), and Appendix 3 of Schedule 2 of the Indian Trade Classification (Harmonised System) Classification of Export and Import Items [ITC(HS)] of the FTP ("Appendix 3") can be accessed on the website of the Directorate General of Foreign Trade (DGFT) under the tab Regulatory updates.[2]

The Standard Operating Procedure for grant of Export Authorization by the Department of Defense Production (DDP) can be accessed on the website of the Ministry of Defense under the Defense Exports section.[3]

Guidelines for Nuclear Transfers (Exports) dated April 28, 2016, issued by the Department of Atomic Energy (DAE) can be accessed on the website of the DAE.[4]

Who Is the Regulator: The federal government notifies the FTP, and the DGFT in the Ministry of Commerce and Industry administers it. The

Customs authorities at the port of import or export are responsible for enforcement of the FTP.

Indian federal investigative agencies like the Directorate of Revenue Intelligence (DRI) are authorized to conduct investigations and initiate proceedings against importers or exporters for violating the FTP.

The dual-use items list of India is known as the SCOMET[5] List. Items on the SCOMET List are organized under nine categories wherein each category contains an exhaustive listing of items covered thereunder with specific conditions and exemptions, if any. For export of items, the DGFT is the licensing authority for the granting of licenses for items falling under Categories 1, 2, 3, 4, 5, 7, and 8 of the SCOMET List; the DAE for items falling under Category 0 thereof and Note 2 to the Commodity Identification Note to Appendix 3; and the DDP for items falling under Category 6 thereof. Further, the Ministry of Home Affairs (MHA) has delegated powers to issue licenses to the DDP for export of arms and ammunitions specified in the Schedule of the Arms Rules, 2016.

How to Get a License: For items falling under Categories 1, 2, 3, 4, 5, 7, and 8 of the SCOMET List, an application in specified format is to be made online to the DGFT[6] under the SCOMET Section along with prescribed documents uploaded as pdfs, including the End User Certificate (EUC) and proof of payment of application fees, which is INR 1,000 (US$14 approx.) per application. The original of the EUC from all entities in the supply chain, that is, foreign buyer, end user, and intermediary/consignee, is submitted in hard copy to the SCOMET Section of the DGFT (HQ), in New Delhi, along with electronic submission receipt.

For items falling under Category 6 of the SCOMET List, an application in specified format is made online to the DDP[7] along with prescribed documents uploaded as pdfs, including the EUC verified by the government of the end user or ultimate end-user country, before or after export, as specified. The original of the EUC from all entities in the supply chain is submitted to the DDP before issue of authorization or within 30 days of filing an application, as the case may be.

For items falling under Category 0 of the SCOMET List, an application in specified format[8] is made to the DAE in hard copy, along with prescribed documents, including the EUC and proof of payment of application fees, which is INR 500 (US$7 approx.) per application. Authorization will be

granted only when transfer is under adequate physical protection and covered under appropriate International Atomic Energy Agency (IAEA) safeguards or mutually agreed controls.

Key Websites:

- Directorate General of Foreign Trade: https://dgft.gov.in/CP/
- Department of Defense Production: https://ddpmod.gov.in/
- Department of Atomic Energy: http://www.dae.gov.in/

19.2 Structure of the Laws and Regulations

(a) International Treaties

India has adopted the United Nations Security Council (UNSC) Resolution 1540 leading to notification of the Weapons of Mass Destruction and Their Delivery Systems (Prohibition of Unlawful Activities) Act 2005 (WMD Act).

India is member of the following multilateral export control regimes:

- Missile Technology Control Regime
- Wassenaar Arrangement
- Australia Group

India is not a member of the Nuclear Suppliers Group but has adhered to it since 2008. India is not signatory to the Non-Proliferation Treaty and hence is not part of the Zangger Committee.

India is also party to various multilateral nonproliferation agreements, such as the Chemical Weapons Convention 1993 and the Biological and Toxin Weapons Convention. Additionally, India has been actively involved with the United Nations, the World Customs Organization, the Conference on Disarmament, and the IAEA on activities relating to export controls.

(b) Indian National Laws and Regulations on Export Controls

- The Foreign Trade Policy and Handbook of Procedures thereof, the Export Policy and the Import Policy of the Foreign Trade Policy, and

the Indian Trade Classification (Harmonised System) Classifications of Export and Import Items thereof [9]

- The Foreign Trade (Development and Regulation) Act 1992 and rules thereof (FTDR Act)[10]
- The Weapons of Mass Destruction and Their Delivery Systems (Prohibition of Unlawful Activities) Act 2005 and rules thereof [11]
- The Atomic Energy Act 1962 and rules thereof (Atomic Energy Act)[12]
- The Arms Act 1959 and rules thereof (Arms Act)[13]
- The Chemical Weapons Convention Act 2000 and rules thereof (CWC Act)[14]
- The Explosive Substances Act 1908
- The Explosives Act 1884 and rules thereof (Explosives Act)
- The Customs Act 1962 and rules and regulations thereof (Customs Act)
- The Environment (Protection) Act 1986 and rules thereof
- The United Nations Securities Council Act 1947 (UNSC Act)
- The Unlawful Activities (Prevention) Act 1967 and rules thereof (UAP Act)
- The Narcotic Drugs and Psychotropic Substances Act 1985 and rules and orders thereof
- The Prevention of Money Laundering Act 2002 (PML Act)

The aforementioned laws and legislations can be accessed at https://www.indiacode.nic.in/ which is digital repository for all Central and State Acts and their subordinate legislations.

(c) Controlled Lists

India's control list of dual-use items known as the SCOMET List and is contained in Appendix 3.[15] The SCOMET List is aligned with multilateral export control regimes, of which India is a member.

The Munitions List is Category 6 of the SCOMET List.

Category 0 of the SCOMET List corresponds to the Prescribed Materials, Prescribed Equipment and Technology List (PSPET List) notified under the Atomic Energy Act.

Category 1 of the SCOMET List corresponds to the CWC Act, read with the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction.

Additional lists of regulated arms, ammunitions, and explosives are also provided under the governing legislations listed earlier, in Section 19.2(b).

(d) India and UN Security Council Sanctions

India follows UN sanctions by publishing orders in the Official Gazette in terms of the UNSC Act. However, India does not follow unilateral sanctions imposed by other countries, such as the United States. For example, in terms of the FTP, trade in oil and refined oil products, modular refineries and related materials besides items of cultural (including antiquities), scientific, and religious importance is prohibited with the Islamic State in Iraq and the Levant (ISIL), Al Nusrah Front (ANF), and other individuals, groups, undertakings, and entities associated directly or indirectly with al-Qa'ida in compliance with UNSC Regulation No. 2199 (2015).

Additionally, there is prohibition on direct or indirect import/export from/to the Democratic People's Republic of Korea (DPRK) in terms of UNSC Resolutions under Chapter VII of the Charter of the United Nations on DPRK.

Further, direct or indirect export or import from Iran of items, material, equipment, goods, and technology mentioned in specified IAEA documents and UNSC resolutions/documents are permitted subject to Annexure B to UNSC Resolution 2231 (2015). And, in compliance with the UNSC Resolution 2036 (2012), direct or indirect import of charcoal from Somalia is prohibited.

(e) Indian National Laws on Economic Sanctions

Economic sanctions in relation to import and export of goods are implemented through the FTP, which are country, organization, groups, individual, and product specific. Currently, India imposes specific trade restrictions as following:

- Import and export of arms and related material from/to Iraq is prohibited. However, export of arms and related material to the

government of Iraq is permitted subject to No Objection Certificate from the DDP.

- Trade in oil and refined oil products, modular refineries and related materials, besides items of cultural (including antiquities), scientific, and religious importance, is prohibited with the Islamic State in Iraq and the Levant (ISIL), Al Nusrah Front (ANF), and other individuals, groups, undertakings, and entities associated with al-Qa'ida in compliance with UNSC Resolution No. 2199 (2015).
- Prohibition on direct and indirect import and export from/to DPRK and sectoral export prohibitions.
- Direct or indirect export/import from or to Iran of items, materials, equipment, goods, and technology listed in INFCIRC/254/Rev.9/Part 1 and INFCIRC /254/Rev.7/Part 2 (IAEA Documents) and the UNSC document S/2006/263 would be permitted subject to the provisions contained in Annex B to UNSC Resolution 2231 (2015).
- Direct or indirect import of charcoal from Somalia is prohibited in terms of the UNSC Resolution 2036 (2012).

(f) Indian Sanctioned Parties Lists

The DGFT may put a person/entity on the Denied Entity List[16] and refuse to grant license, certificate, scrip, or any instrument bestowing financial or fiscal benefits and recovery of benefits if any person makes or abets or attempts to make any export or import in contravention of the FTDR Act or rules and order thereunder or the FTP. The Denied Entity List is not currently published.[17]

Sanctions relating to national security, counterterrorism, and related activities are administered by the MHA under the UAP Act. India does not have a consolidated list of sanctioned/designated parties. However, India has implemented the UN Consolidated List through notifications/orders updated by the MHA from time to time.

Current lists of terrorist organizations itemized in First Schedule of the UAP Act, which also includes organizations listed in the Schedule to the UN Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order 2007, amended from time to time, can be accessed online.[18]

The PML Act along with the UAP Act are effective instruments used to combat offences relating to terrorist financing and money laundering. To combat terrorist financing and money laundering, the Reserve Bank of India (RBI) prohibits regulated entities[19] from opening accounts in the name of individuals or entities appearing on the UN lists of parties suspected of having terrorist links:

- The ISIL (Da'esh) & al-Qa'ida Sanctions List, which includes names of individuals and entities associated with al-Qa'ida, can be accessed at https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list.
- The 1988 Sanctions List, consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban can be accessed at https://www.un.org/securitycouncil/sanctions/1988/materials.
- Any other entities lists circulated by the MHA.

India is also member of the Financial Action Task Force (FATF).[20] The RBI takes into consideration statements issued by the FATF while specifically stating that regulated entities can conduct legitimate trade and business transactions with jurisdictions mentioned in the FATF statement provided they pay special attention and examine the background and purpose of transactions with persons from jurisdictions included in the FATF statements and with countries that do not at all or insufficiently apply the FATF recommendations and retain written findings with all documents, which can be produced before the RBI or other authorities on request.

India is also member of the Asia/Pacific Group on Money Laundering (APG).[21]

19.3 What Is Regulated: Scope of the Regulations

The FTDR Act empowers the Indian federal government to formulate and notify the FTP, which is amended from time to time. The FTP provides regulatory framework for the export and import of goods and services from and into India. The HBoP provides the procedure for implementing the FTP, and the ITC(HS) of the FTP provides whether a product is freely importable or exportable, or restricted or prohibited. The export policy and import

policy of the FTP provides regulatory compliances to be undertaken in relation to export or import of goods or services.

Exemptions and concessions provided under the FTP are implemented by way of notifications issued under the Customs and Goods and Services Tax laws.

Dual-use items are specified goods, software, technology, and chemicals that have both civil and military applications. The dual-use items list of India is known as the SCOMET List and is contained in Appendix 3. Export of items on the SCOMET List are regulated under the FTP, that is, they are either prohibited or permitted to be exported only under an authorization issued by the specified authority.

The WMD Act regulates the export, transfer, retransfer, transshipment, or transit of items related to relevant activity[22] falling under the SCOMET List and Schedule of the PSPET List notified under the Atomic Energy Act. Export of items not on the SCOMET List may also be regulated under the WMD Act.

Chapter IVA of the FTDR Act specifically deals with controls on export of specified goods, services, and technology[23] and, together with the WMD Act, prohibits the export of any material, equipment, or technology knowing that such material, equipment, or technology is intended to be used in design or manufacture of biological weapons, chemical weapons, nuclear weapons, or other nuclear explosive device, or in their missile delivery systems.

Import and export of arms and ammunitions is permitted only against license issued under the Arms Act. Likewise, import and export of explosives is regulated under the Explosives Act. Dual-use Chemicals[24] are regulated under the CWC Act read with the FTDR Act and Orders issued thereunder.

India also follows a catchall controls policy. Thus, if an exporter is notified by the regulator or has reason to believe that an item not covered under the SCOMET List has potential risk of use in or diversion to WMD end uses or in their missile systems or military end use, including use by terrorists and nonstate actors, export of such item requires a permit, which may be granted as a SCOMET authorization or denied.

19.4 Who Is Regulated?

Any person, both natural and legal, including individual, firm, society, company, corporation, or any other legal person who exports or intends to export restricted/controlled items is required to obtain authorization from the specified authority.

19.5 Classification

(a) Classification of Dual-Use Items

Items on the SCOMET List[25] are organized under the following nine categories, wherein each category contains an exhaustive listing of items covered thereunder with specific conditions and exemptions, if any:

- Category 0: Nuclear materials, nuclear-related other materials, equipment, and technology
- Category 1: Toxic chemical agents and other chemicals
- Category 2: Microorganisms, toxins
- Category 3: Materials, Materials-Processing Equipment and related technologies
- Category 4: Nuclear-related other equipment and technology not controlled under Category 0
- Category 5: Aerospace systems, equipment including production and test equipment, related technology, and specially designed components and accessories thereof
- Category 6: Munitions List
- Category 7: Reserved
- Category 8: Special Materials and related Equipment, Material Processing, Electronics, Computers, Telecommunications, Information Security, Sensors and Lasers, Navigation and Avionics, Marine, Aerospace and Propulsion

(b) Classification of Military Items

Category 6 (Munitions List) of the SCOMET List is composed of military items.

19.6 General Prohibitions/Restrictions/Requirements

IEC is a key business identification number that is mandatory for export from India or import into India. To get an IEC, an application is to be filed online to the DGFT.[26]

Export authorizations are not required for supply of SCOMET items from Domestic Tariff Area[27] to Special Economic Zone[28] (SEZ)/Export Oriented Unit (EOU),[29] though such supplies are to be reported to the jurisdictional Development Commissioner of SEZ/EOU by the supplier. An export authorization is required if SCOMET items are physically exported out of India from SEZ/EOU to another country.

Each category of item on the SCOMET List provides specific prohibitions and restrictions applicable. For example, the Notes to Category 6 provide that export of aircraft, lighter than air vehicles, unmanned aerial vehicles, aero engines and aircraft equipment, related equipment and components specially designed or modified for military use require No Objection Certificate from the Defense Research and Development Organization in addition to export authorization from the DDP.

Authorization for export of items in Categories 0, 3 (other than 3D), 4, 5, and 7 of the SCOMET List to Iran are subject to relevant provisions of Annexure B to the UNSC Resolution 2231 (2015).

Brokering is prohibited in relation to items under all categories on the SCOMET List. It is the stated policy of the Indian government not to allow "brokers" in defense deals. The term "brokering" is neither defined in the FTP nor in the FTDR Act. The FTDR Act provides for control on export of specified goods, services, and technology, which interalia provides that in relation to brokering, provisions of the WMD Act apply. While the term "brokering" is not defined in the WMD Act, section 12 thereof prohibits brokering by using the term *facilitate execution of any transaction*.

Further, Standard Operating Procedure issued by the DDP for issue of authorization for export of items on the Munitions List (Category 6 of SCOMET List) also provides that "brokering" is prohibited in terms of the FTDR Act and the WMD Act. It is pertinent to mention here that the FTP recognizes the role of "intermediary" in the export of items on the SCOMET List, wherein it is specified that the EUC is to be submitted from all entities in the chain of supply interalia including "intermediary" while filing an application for authorization for export of items on the SCOMET List. Since an EUC is also required from the intermediary, the intermediary is arguably a person involved in the supply chain of the export of SCOMET

items and is not merely acting as an agent on commission who facilitates the transaction. However, both the FTDR Act and the WMD Act prohibit brokering.

19.7 Licensing/Reasons for Control

(a) Types of Export Control Licenses and Permits for Dual-Use Items

The DGFT issues three types of SCOMET authorizations:[30]

- **General SCOMET Authorization** is a one-time authorization and is required to be applied afresh every time an exporter wants to export dual-use items on the SCOMET List.

  General SCOMET authorization issued by the DGFT is valid for 24 months. Inter-Ministerial Working Group[31] (IMWG) may issue a license for a shorter/longer period depending on contractual obligations and the recommendation of concerned ministry/department/agency. The SCOMET authorization can be revalidated twice for a period of six months each up to a maximum of 12 months.
- **Global Authorization for Intra-Company Transfers (GAICT)** for export/re-export of SCOMET items, including software and technology, under Category 8 of the SCOMET List, except items specifically excluded, issued subject to compliance with specified conditions. Some of the conditions are exports/re-exports to Wassenaar Arrangement member countries,[32] Master Service Agreement (MSA)/contract between Indian parent company or subsidiary and its foreign subsidiary or foreign parent/another subsidiary of foreign parent company, approved Internal Compliance Programme (ICP) of its own or compliant with ICP of parent company, quarterly post-export reporting requirements. The GAICT is valid for a period of three years from the date of issue and cannot be revalidated, but on expiry thereof exporters must apply for a new GAICT. By contrast, general SCOMET authorization can be revalidated for a period of six months at a time but up to a maximum of 12 months, and GAICT cannot be revalidated.

- **General Authorization for Export of Chemicals and Related Equipment (GAEC)** for export/re-export of SCOMET items under Categories/Subcategories 1C, 1D, 1E, 3D001, and 3D004 (excluding software and technology) of the SCOMET List to Australia Group member countries subject to compliance with specified conditions and quarterly post-export reporting requirements. The GAEC is valid for a period of five years from the date of issue and cannot be revalidated.

The DDP issues following types of export authorizations:

- **General export authorization** is a one-time authorization and is required to be applied afresh every time an exporter wants to export items falling under Category 6 of the SCOMET List. Validity of general authorization may be extended by the competent authority on a case-to-case basis, though no specific period is specified.

  General export authorization issued by the DDP is valid for a period of six months to two years, depending on the purpose for which it is applied and issued.
- **Open General Export License (OGEL) for Intra-Company Transfer of Technology** allows intra-company re-export of imported software or technology related to specified items falling under Category 6A021 and Category 6A022 of the SCOMET List imported from a parent country abroad or subsidiaries of a parent company abroad, to specified countries subject to compliance with specified conditions. Some of the conditions are MSA between parent company and Indian subsidiary for carrying out services, having a comprehensive set of internal controls in place, approved ICP of its own or compliant with ICP of parent company, specified declaration on commercial documents at the time of export, quarterly and annual post-export reporting requirements. Export or transfer of these items to SEZ is not permitted. OGEL for intra-company transfer of technology is valid for a period of two years from the date of issue.
- **OGEL for parts and components** allows transfer or export of specified parts and components for military end use to specified countries subject to compliance with specified conditions, including having a comprehensive set of internal controls in place, ICP of its own or compliant with ICP of principal/subsidiary abroad, specified

declaration on commercial documents at the time of export, quarterly and annual post-export reporting requirements. Export or transfer of these items to SEZ is not permitted. OGEL for parts and components is valid for a period of two years from the date of issue.

- **OGEL for export of major platforms and equipment** allows export of items listed in Category 6A014—night visions devices, thermal night sights, thermal binocular, and Category 6A015—only simulators, of the SCOMET List for military end use to specified countries subject to compliance with specified conditions, including having a comprehensive set of internal controls in place, ICP of its own or compliant with ICP of principal/subsidiary abroad, specified declaration on commercial documents at the time of export, quarterly and annual post export reporting requirements. Export or transfer of these items to SEZ is not permitted. OGEL for major platforms & equipment is valid for a period of two years from the date of issue.

(b) Export Control Licensing Procedure

(i) Items Falling under Categories 1, 2, 3, 4, 5, 7, and 8 of the SCOMET List

An application in prescribed format is to be filed online under the tab SCOMET.[33]

The following documents are to be uploaded along with the application:

- Profile of exporter in prescribed format
- Copy(ies) of Purchase Order (PO) from firm(s) involved in supply chain of item/product
- The EUC in specified format from all firms/entities involved in entire supply chain of product on letterhead signed by authorized signatory
- Detailed technical specification of item of export
- Copy(ies) of supply contract/agreement between foreign buyer and end user with third party, if third party or contractor involved
- Bill(s) of Entry into destination country for the SCOMET List items exported during last one year
- Copy of the DGFT authorization for the same product in case of repeat order

Pre-license checks are conducted through agencies and India's missions abroad. Further, SCOMET authorization may be granted subject to post-shipment verifications.

The IMWG under chairmanship of the Additional DGFT meets once a month and considers applications for export of items on the SCOMET List considering various criteria.[34] SCOMET authorization is generally issued within 45 days from the date of filing of complete documents, though the DGFT is working toward reducing this timeline to 30 days.

Specific procedures and document requirements are prescribed by the DGFT for SCOMET authorization for specified purposes as set forth here. These are not license exceptions, as a license is required for all purposes listed here, but the documentary requirements may be less stringent. For example, for cases like demo or display, a EUC is not required.

- Repeat orders
- Stock and sale
- Export of imported SCOMET item for repair/replacement; re-export of indigenous SCOMET items after repair/replacement
- Export of imported SCOMET items to same entity abroad or any authorized entity after repair in India
- Export of imported SCOMET items after participation in demo/display/exhibition/tenders/Request for Quotation (RFQ)/Request for Proposal (RFP)/Notice Inviting Tender (NIT) in India
- Export of indigenous/imported SCOMET item(s) for demo/display/exhibition/tender/RFP/RFQ/NIT abroad
- Re-export/return of imported SCOMET items to the same foreign entity or its Original Equipment Manufacturers (OEM), including agencies authorized by such OEM on account of obsolescence of technology of imported items, cancellation of order by Indian buyer/end user, dead on arrival
- The GAICT
- The GAEC

(ii) Items Falling under Category 6 of the SCOMET List

An application in prescribed format is to be filed online.[35] The following documents are to be uploaded along with the application:

- Brief write up on intent of application on letterhead of the company signed by authorized signatory
- Relevant classification/sub-classification under the SCOMET List, that is, 6A001, 6A002 should be clearly specified.
- Copy of PO/supply order/relevant documents like participation in Tender Enquiry/RFI/Exhibition/Testing and Evaluation as the case may be
- Technical specification of the item(s) to be exported
- The EUC signed and stamped by appropriate authority establishing clear chain of transaction/transmission, that is, parties involved and final end use/user. In case the original EUC is not in English, English translation duly certified by Notary Public/Embassy/Mission of India abroad
- Industrial license for manufacture of specified parts of firearms

Applications are forwarded to the Ministry of External Affairs (MEA) and other concerned agencies, including the ISRO, for comments, depending upon item to be exported. Export authorization to UN-sanctioned countries are considered in consultation with MEA.

Original copy of the EUC should reach the Defense (Export Promotion Cell) prior to issue of authorization or within 30 days of filing of online application. Export authorization is generally issued within four to six weeks from the date of filing of complete documents.

Specific procedures and less stringent documentary support requirements are allowed when applying for export authorizations for the following specified purposes:

- Re-export of an item after undertaking repair or rework
- Replacement on being rejected by the foreign OEM
- Export of an item that was imported for repair or replacement
- Export for exhibition purposes
- Export for testing and evaluation
- In principle approval for export for participating in tenders/RFP/NIT or for exploring export opportunities
- Approval for transfer of technology/software for design, development, manufacturing, training, maintenance services, upgrade and overhaul of items of Munitions List

- Export of an item imported for participation in tenders/RFP/RFQ/NIT/demo/display/exhibitions in India and exported back to foreign OEM

(c) Import and Export Licenses for Military Items

List of military items is contained in Category 6 of the SCOMET List. Licensing procedure for export of items contained therein is provided at Section 19.7(b)(ii).

Import and export of arms and ammunition require license under the Arms Act.

(d) Export Permits and Independent Expert Examination

India does not have any provision for export permits and independent expert examination. However, the IMWG consults and seeks comments from concerned administrative ministry/department/agency prior to grant of SCOMET authorization in case of need.

19.8 General Licenses/License Exceptions

(a) General Licenses

The DGFT issues the following general licenses:

- The GAICT for export/re-export of SCOMET items including software and technology under Category 8 of the SCOMET List, except items specifically excluded, to Wassenaar Arrangement member countries as discussed in Section 19.7(a).
- The GAEC for export/re-export of SCOMET items under Categories/Subcategories 1C, 1D, 1E, 3D001, and 3D004 (excluding software and technology) of the SCOMET List to Australia Group member countries as discussed in Section 19.7(a).

The DDP issues the following general licenses:

- OGEL for Intra-Company Transfer of Technology for intra-company reexport of imported software or technology related to specified items

falling under Category 6A021 and Category 6A022 of the SCOMET List, as discussed in Section 19.7(a).
- OGEL for parts and components to transfer or export specified parts and components for military end use, as discussed in Section 19.7(a).
- OGEL for export of major platforms and equipment to export items listed in Category 6A014—night vision devices, thermal night sights, thermal binoculars, and Category 6A015—only simulators, of the SCOMET List for military end use as discussed in Section 19.7(a).

(b) License Exceptions

India does not have license exceptions. Hence, if an item falls under the SCOMET List of India or Catchall controls, unless exempted, SCOMET authorization is required prior to export of such item.

19.9 Penalties, Enforcement, and Voluntary Disclosures

(a) Administrative Penalties

(i) The FTP and the FTDR Act

- Suspension or cancellation of IEC and/or license.
- Penalty of INR 10,000 (US$135 approx.) but not more than five times the value of such goods/services/technology, whichever is more, in case of any export or attempt to export or abetting in contravention of the FTP and the FTDR Act. Identical penalty for signing or using any declaration or statement or document knowing or having reason to believe it to be forged or tampered with or false.
- Confiscation by the adjudicating authority of goods, including goods connected with services or technology and conveyances in case of contravention of the FTP and the FTDR Act, which may be released on payment of redemption charges equal to market value of goods or conveyance.
- Entity may be placed on the Denied Entity List by the DGFT and refused grant or renewal of a license, authorization, certificate, scrip, or any instrument bestowing financial or fiscal benefits under the FTP.

- Penalties under the FTDR Act are in addition to penalties that may be imposed under any other laws for such violations.

(ii) The WMD Act

- Fine of INR 500,000 (US$6,680 approx.) or five times the value of materials, equipment, technology, or services, whichever is more, in case of using or signing forged documents knowing or having reason to believe it to be forged or tampered with or false.
- Fine of INR 300,000 (US$4,000 approx.) which may extend to INR 20,00,000 (US$26,670 approx.) for first offence of unauthorized export of item notified under section 13(4) of the WMD Act.[36] In case of any subsequent offence, imprisonment for a term of not less than six months, which may extend to five years and a fine.

(iii) The Customs Act

- Confiscation of goods attempted to be exported contrary to any prohibition imposed by or under the Customs Act or any other law that may be released on payment of redemption fine, which does not exceed market price of goods confiscated.
- In case of goods in relation to which any prohibition is in force under the Customs Act or any other law, penalty not exceeding three times the value of goods declared by exporter or determined under the Customs Act.
- Penalty equal to five times the value of goods in case of use of false or incorrect material in transaction of any business for purpose of the Customs Act.

(b) Criminal Penalties

(i) The FTDR Act

- Imprisonment for term specified in the WMD Act for contravention or attempt to contravene or abetment of provisions of Chapter IVA of the FTDR Act in relation to import or export of specified goods or services or technology.

(ii) The WMD Act

- In case any subsequent offence of unauthorized export of item notified under section 13(4) of the WMD Act, imprisonment for a term not less than six months, which may extend to five years and a fine.
- Imprisonment for five years, which may extend to imprisonment for life (ten years) in case of aiding non-state actor or terrorist.
- Imprisonment for six months, which may extend to five years and a fine for first offence. For any subsequent offence, imprisonment for one year, which may extend to seven years and a fine.
- In case no specific punishment is provided then imprisonment for a term that may extend to one year, or with a fine, or with both.
- Court will not take cognizance of offence punishable under Chapter IVA of the FTDR Act and the WMD Act without permission from the Indian federal government.

(iii) The Customs Act

- Imprisonment for a term that may extend to two years or with a fine, or both, in case of use or making of false declaration or documents in transaction of any business relating to customs knowing or having reason to believe the same to be false.
- Imprisonment for a term that may extend from three years to seven years and a fine for exporting or attempting to export any goods contrary to any prohibition imposed by or under the Customs Act or any other law.
- Imprisonment for a term that may extend to three years or with a fine, or with both, for making preparation to export any goods in contravention of the Customs Act.

Additionally, penalties are prescribed under governing legislations such as the Arms Act, the CWC Act, and so on, for contraventions thereunder.

(c) Enforcement

The Customs authorities at the port of import or export are primarily responsible for enforcement of the FTP and export controls. The Customs authorities also have the power to stop, examine, and seize any shipment being exported in violation of the FTP or other governing legislation.

Proceedings for levy of fiscal penalties on entities and its employees, undertaking unauthorized export of controlled goods in violation of the FTP are initiated under the Customs Act, the FTDR Act, the WMD Act, and other relevant governing legislations. In case of a serious violation, prosecution of company and its key managers can be initiated.

In addition, the DRI is the premier investigative agency undertaking investigations, adjudication of cases, and prosecution of arrested persons in cases of organized violations of the Customs Act, the FTP, the FTDR Act, and other governing legislation in relation to the export or import of goods and services.

Recently, members from the Risk Management Division of the Central Board of Indirect Taxes and Customs (CBIC) and economic intelligence agencies like the DRI have been included in the IMWG to strengthen enforcement of export controls in India. The DGFT and the DDP also mark copies of all denial cases to the DRI/Risk Management Division of the CBIC to prevent unauthorized export.

(d) Voluntary Disclosures

There is no specified process to handle voluntary disclosure in case of export control violations in India. Nevertheless, voluntary disclosures are a standard practice when any noncompliance comes to knowledge of any company, as they are considered as evidence that the exporter had no malafide intention and are generally viewed leniently by the authorities rather than when the authorities themselves detect any noncompliance. Voluntary disclosure helps save on penalties and prosecution of company and its employees. Accordingly, in case of noncompliance, voluntary disclosure is frequently advisable as a way to close out a given noncompliance issue.

19.10 Recent Export Enforcement Matters

Information in relation to enforcement matters pertaining to export control violations is presently not available in the public domain.

19.11 Special Topics

(a) Re-exports/Extraterritorial Application of Laws

The EUC, to be submitted as support for a license application, contains a declaration that the end user will not himself or through any other person cause the items or replicas of derivatives be retransferred or sold without the consent of the Indian federal government to any party within the country of destination or outside unless specifically exempted in the export authorization. Thus, unless specifically exempted, re-exports and retransfers to parties and countries not listed in the EUC require consent of the Indian federal government.

The Customs Act governs import and export of goods out of India. In 2018, the Customs Act was amended to provide extraterritorial jurisdiction and is applicable to any offence or contravention committed outside India by any person.

The WMD Act provides that any person who commits an offence beyond India will be dealt with according to the provisions thereof in the same manner as if such act had been committed in India. Further, the WMD Act applies to citizens of India outside India; companies or bodies corporate, registered or incorporated in India or having their associates, branches or subsidiaries, outside India; any ship, aircraft, or other means of transport registered in India or outside India, wherever it may be; foreigners while in India, persons in service of the Indian federal government, within and beyond India.

The CWC Act also applies to citizens of India outside India, companies or bodies corporate, registered or incorporated in India or having their associates, branches, or subsidiaries, outside India.

(b) Intangible Transfer of Technical Information

Exports[37] as defined under the FTDR Act includes supplying services or technology in India to service consumers of any other country or by a service supplier of India through commercial presence in any other country or presence of Indian natural persons in the territory of any other country. Thus, exports include deemed exports where there is transfer to foreign national within India or transfer to foreign national by an Indian entity having presence outside India or transfer to foreign national by a person located outside India.

Technology is defined in the FTDR Act as any information (including information embodied in the software), other than information in the public domain, that is capable of being used in:

- Development, production and use of any goods or software,
- Development of, or the carrying out of an industrial or commercial activity or provision of service of any kind.

Further, Glossary to Appendix 3, while defining technology, clarifies that information takes the form of technical data (blue prints, plans, diagrams, engineering designs and specifications, etc.) or technical assistance (instructions, training, working knowledge, transfer of technical data, etc.).

Each category of item listed in the SCOMET List has a subcategory for software and technology related to such item, except Category 1 and 2 thereof. Accordingly, transfer of technology of items covered under the SCOMET List is controlled. However, controls do not apply to technology that is the minimum necessary for installation, operation, maintenance, or repair of items that are not controlled or export of which is authorized. Further, controls also do not apply to technology that is in the public domain or basic scientific research or minimum necessary information for patent applications.

Similarly, controls do not apply to software that is generally available in the public domain by being sold from stock at retail selling points without restrictions by means of over-the-counter transactions, mail order transactions, electronic transactions, or telephone call transactions and designed for installation by user without substantial support from supplier; in public domain or minimum necessary object code for installation, operation, maintenance, or repair of those items whose export is authorized.

SCOMET authorization is not granted for export of technology or software under any category for demo/display/exhibition/tender, and so on.

The WMD Act prohibits transfer of technology of an item whose export is prohibited thereunder or any other relevant act relating to relevant activity.[38] The WMD Act further restricts transfer of technology subject to transfer controls. Transfer of technology may take place by transfer by a person or place within India to a person or place outside India *or* by a person or place outside India to a person or place outside India (only where transfer is by or within control of person citizen of India or resident in India).

The DGFT has provided specific procedure and document requirements for the GAICT, which includes transfer of software and technology.

The DDP has also specified procedure and document requirements for OGEL for Intra-Company Transfer of Technology and for transfer of Technology/Software in the Munitions List for design, development, manufacturing, testing, evaluation, maintenance services, upgrade, repair, and overhaul of the items thereunder. Furthermore, it is mandatory for all companies and their subsidiaries and business entities operating in India involved in manufacture, processing, and use of SCOMET items to obtain permission of the DGFT before entering into any arrangement to facilitate site visits, on-site verification or access to records/documents by foreign governments, foreign third parties, acting directly or through Indian party.

(c) Practical Issues Related to Export Control Clearance

Many companies are not aware of export control laws in India or that an item/product dealt with by them falls under the SCOMET List. This results in the unauthorized export of controlled items through oversight.

Time taken by the licensing authorities to grant license adds to lead time to complete a project/assignment. While export control laws have developed at a much faster pace in last couple of years, there is a need to bring in more clarity on a lot of issues, for example to introduce the concept of license exception, issue of bulk licenses, and so on.

(d) Recordkeeping

Every SCOMET authorization holder is mandatorily required to maintain the following records, either in manual or electronic form, for a period of five years from the date of export or import:

- All documents submitted to authorities at the time of making application for SCOMET Authorization
- Copies of all correspondence with buyer/consignee/end user or the DGFT or any other government agency
- Relevant contracts
- Relevant books of accounts
- Relevant financial records

- Any communication received from any government agency relating to application for SCOMET authorization or commodity classification request
- Shipping documents including shipping bill, bill of entry, bill of lading

The DDP may require additional records to be maintained and for a longer period notifying exporter about the same for items falling under Category 6 of the SCOMET List.

(e) How to Be Compliant When Exporting to India

If the item proposed to be exported to India falls within the scope of export control laws of the exporting country, obtain a license from appropriate Authority. In case the item falls under License Exception under the laws of the exporting country, specific reference to provision under which license exception is granted should be mentioned on the body of export documents.

Further, check if there is any regulatory compliance requirement under the Import Policy of the FTP to be complied with at the time of import of such items into India.

(f) How to Be Compliant When Exporting from India

Maintaining a robust ICP and regularly training employees play key roles in successful compliance with export control laws. Whenever an exporter or its employees comes across red flags (such as those illustrated next) they should engage in further detailed inquiry and involve their Trade Compliance team before proceeding with the transaction.

- Know Your Customer
  - Background—whether under list of designated countries/entities
  - Industry and products being manufactured
  - How long the company has been dealing with customer
  - Financial health of customer and funding pattern
  - Information available in public domain
- Know Your Product
  - Whether under prohibited or restricted category?
  - Does it fit into operations of customer?
  - Does customer have knowledge of item he is buying?

    - End use and end user.
    - Refusal of installation, commissioning, training, and routine maintenance.
- Logistics
    - Delivery dates vague.
    - Destination of item—embargoed/sanctioned country?
    - Oddity of port of discharge or mode and routing of shipment.
    - Third party delivery.
    - Is packaging inconsistent with stated method of shipment or destination.

19.12 Encryption Controls

(a) General Comments

The SCOMET List inter alia includes and regulates cryptographic information security equipments and components, software and technology. However, certain exemptions are provided therein, such as controls do not apply to:

- Products when accompanying their user for user's personal use;
- Items meeting all of the mass market criteria, that is, generally available to the public by being sold from stock at retail selling points and cryptographic functionality cannot be easily changed by the user and designed for installation by user without substantial support from supplier and details are accessible and can be provided to authorities in exporters countries to ascertain compliance, etc.

Further, restrictions under the FTP are applicable only to the export of cryptographic items, software, and technology from India and do not apply to imports thereof. In addition, section 84A read with section 87(zh) of the Information Technology Act 2000 (IT Act) empowers the Indian federal government to prescribe modes or methods of encryption. However, no rules and regulations have been notified by the Indian federal government as on date in this regard. Further, a draft national encryption policy was released by the federal government in September 2015 inviting comments from stakeholders, but the same was withdrawn immediately on account of severe criticism and new draft national encryption policy has not been

released so far. Thus, in spite of the IT Act authorizing the federal controls on encryption, no policy or rules have been notified for regulating encryption in India so far, except for the SCOMET List export controls discussed earlier. However, concerned regulators in a number of sectors, such as banking, finance, and telecommunications, have specified minimum standards of encryption to be used in securing transactions in these specific sectors.

(b) Import Encryption Clearance Requirements

Presently, the federal government has not notified any rules for modes and methods of encryption under the IT Act. Thus, there are no restriction on import and use of cryptographic software into India, except as regulated by sectoral restrictions placed by the Regulators.

(c) Encryption Licensing Requirements

See Section 19.12(a) for the SCOMET List licensing requirements.

(d) Penalties for Violation of Encryption Regulations

See Section 19.9 (a) and (b) for penalties for violations of the FTDR Act (for exports of SCOMET encryption items without the required license).

19.13 Blocking Laws/Penalties for Compliance with Sanction Imposed by Other Countries

Currently, India does not have blocking laws.

1. Partners, Ashok Dhingra Associates.
2. https://dgft.gov.in/CP/.
3. https://www.defenceexim.gov.in/.
4. http://www.dae.gov.in/writereaddata/nucl_tr_0516.pdf.
5. SCOMET is an acronym for Special Chemicals, Organisms, Materials, Equipment and Technologies.
6. https://www.dgft.gov.in/CP/?opt=export-management-system.
7. https://www.defenceexim.gov.in/guest_registration.php.
8. http://www.dae.gov.in/node/87.
9. https://www.dgft.gov.in/CP/?opt=ft-policy https://www.dgft.gov.in/CP/?opt=ft-procedures.
10. https://www.dgft.gov.in/CP/?opt=ftd-ract.
11. http://mea.gov.in/Uploads/PublicationDocs/27201_WMD_Act_notification_new.pdf.

12. https://www.indiacode.nic.in/handle/123456789/1413?sam_handle=123456789/1362.

13. https://www.indiacode.nic.in/handle/123456789/1398?view_type=browse&sam_handle=123456789/1362.

14. https://nacwc.nic.in/index.php.

15. https://content.dgft.gov.in/Website/dgftprod/f2f4a7a6-1644-4239-809d-1176d0a9bfec/Updated%20SCOMET%20List%2030-11-2022.pdf.

16. Rule 7 (1) of the Foreign Trade (Regulation) Rules, 1993 lists down 14 circumstances under a person/entity may be put under Denied Entity list which inter alia include contravention of law relating to customs or foreign exchange; application made or documents submitted in support thereof contain any false or fraudulent or misleading statement or when a person makes or makes or abets or attempts to make any export or import in contravention of the FTDR Act or rules and order thereunder or the FTP; applicant fails to any penalty imposed under the FTDR Act or has tampered with a license, certificate, scrip or any instrument bestowing financial or fiscal benefits.

17. To check if an entity is on the Denied Entity List, you need to know the company's Importer-Exporter Code (IEC code). On the DGFT website https://www.dgft.gov.in/CP/ under the Services tab go to View IEC Related Details – View any IEC, and you enter IEC number and name of the company and the system will show the IEC-related details including if IEC is valid (if not, it will tell you the date of cancellation or suspension) and also tell you if the entity is a Denied Entity.

18. https://www.mha.gov.in/en/divisionofmha/counter-terrorism-and-counter-radicalization-division/Banned-Organizations.

19. Banks, nonbanking financial companies, and other entities regulated by the Reserve Bank of India.

20. The FATF is an intergovernmental body that has developed recommendations and standards to ensure global coordinated response to prevent inter alia money laundering, corruption, terrorist financing, funding for weapons of mass destruction, and other related threats to integrity of international financial system.

21. The APG is a regional international intergovernmental body, members of which are committed to implement international standards against money laundering, financing of terrorism, and financing the proliferation of weapons of mass destruction.

22. Section 2(j) of the WMD Act—"relevant activity" means (1) the development, production, handling, operation, maintenance, storage or dissemination of a nuclear, chemical, or biological weapon; or (2) the development, production, maintenance, storage, or dissemination of missiles specially designed for delivering any such weapon.

23. Section 2(l) of the FTDR Act—"specified goods or services or technology" means the goods or services or technology, the export, import, transfer, retransfer, transit, and transshipment of which is prohibited or restricted because of imposition of conditions on the ground of their being pertinent or relevant to India as a Nuclear Weapon State, or to the national security of India, or to the furtherance of its foreign policy or its international obligations under any bilateral, multilateral, or international treaty, convenant, convention, or arrangement relating to weapons of mass destruction or their means of delivery to which India is a party or its agreement with a foreign country under the foreign trade policy formulated and notified under section 5 of the Act.

24. Toxic chemical or precursor listed in Schedules 1 to 3 of the Annex on Chemicals to the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction.

25. The SCOMET list can be found at https://content.dgft.gov.in/Website/dgftprod/f2f4a7a6-1644-4239-809d-1176d0a9bfec/Updated%20SCOMET%20List%2030-11-2022.pdf.

26. https://www.dgft.gov.in/CP/?opt=iec-profile-management.

27. Section 2(i) of the SEZ Act, 2005 "Domestic Tariff Area" means the whole of India (including the territorial waters and continental shelf) but does not include the areas of the Special Economic Zones.

28. Special Economic Zone is deemed to be a territory outside the customs territory of India for trade operations, duties, and tariffs. Supplies of goods and services into SEZ from DTA are treated as exports and goods and services coming from SEZ into DTA are treated as if they are imported.

29. Unit undertaking to export its entire production of goods and services (except permissible sales in DTA) may be set up under Export Oriented Unit Scheme, for manufacture of goods, including repair, re-making, reconditioning, re-engineering, rendering of services, development of software, agriculture including specified sectors. Trading units cannot be set up as EOU.

30. The term Authorization/License is both used interchangeably.

31. The IMWG consists of members from the Ministry of External Affairs, the DDP, Department of Space through Indian Space Research Organisation (**ISRO**), Defense Research and Development Organization (the **DRDO**), Department of Chemicals and Petrochemicals, National Authority of Chemical Weapon Convention (the **NACWC**) and Cabinet Secretariat and considers applications for grant of SCOMET authorization.

32. Export to other countries may be allowed on a case-to-case basis considering description/end use/end user of the products.

33. https://www.dgft.gov.in/CP/?opt=export-management-system.

34. The criteria considered include the end user, credibility of declaration of end use of item or technology, integrity of chain of transmission of item from supplier to end user, potential of the item or technology to contribute to end uses that are not in conformity with India's national security or foreign policy goals and objectives, and so on, assessed risk that exported items will not fall into hands of terrorists and non-state actors; export control measures instituted by recipient state, capabilities and objectives of programs of the recipient state relating to weapons and their delivery; and assessment of end use of items.

35. https://www.defenceexim.gov.in/.

36. Section 13(4) of the WMD Act provides that the federal government may notify any item as being subject to provisions of the WMD Act and such item exhibited, sold, supplied, or transferred to any foreign entity or a foreigner who is resident, operating, visiting, studying, or conduction research or business within the territorial limits of India or in its airspace or exclusive economic zone will constitute an offence. No item notified so far.

37. Section 2 (e) of the FTDR Act reads as under:

(e) "import" and "export" means,—

in relation to goods, bringing into, or taking out of, India any goods by land, sea or air;

in relation to services or technology,—

supplying, services or technology—

from the territory of another country into the territory of India;

in the territory of another country to an Indian service consumer;

by a service supplier of another country, through commercial presence in India;

by a service supplier of another country, through presence of their natural persons in India;

supplying, services or technology—

from India into the territory of any other country;

in India to the service consumer of any other country;

by a service supplier of India, through commercial presence in the territory of any other country;

by a service supplier of India, through presence of Indian natural persons in the territory of any other country";

Provided that "import" and "export" in relation to the goods, services and technology regarding Special Economic Zone or between two Special Economic Zones shall be governed in accordance with the provisions contained in the Special Economic Zones Act, 2005 (28 of 2005)."

38. Refer to footnote 22.

20

Export Controls and Economic Sanctions in Israel

Jeffrey Rashba, Tomer Broude, and Danielle Regev[1]

20.1 Overview

What Is Regulated: Israel's export control and economic sanctions system is somewhat labyrinthine, in the sense that it involves diffuse legislation and regulatory agencies. Article 2 of Israel's Import and Export Ordinance [New Version], 5739-1979[2] grants the Ministry of Economy and Industry[3] (MoE) broad authority to prohibit or regulate the importation and exportation of goods, services, and know-how. Under this authority, the Free Export Order, 5782-2022 (FEO), in its Article 2(a), establishes a default system whereby all goods are allowed for export. Goods that are nevertheless subject to some form of prohibition or regulation are listed in Articles 2 through 5 and in annexes to the FEO, which may be revised from time to time.

- Thus, the first annex lists over 170 regulated items that require an export license, focusing primarily on animals, narcotics, hazardous materials, and certain types of heavy machinery.[4]
- The second annex lists close to 1,000 items that require an export authorization, ranging from animals, foods and plants to diamonds and antiquities.[5]
- Article 2(a)(3) of the FEO refers to the Import and Export Order (Supervision of Chemical, Biological and Nuclear Exports), 5764-

2004, which regulates the manner of exporting goods, services, and technology that are either intended for the development of nonconventional weapons or may be used for this purpose.

- Article 2(a)(4) of the FEO refers to the Defense Export Control Law, 5766-2007 which regulates the manner of exporting any goods that are listed in the annexes of the following laws: The Defense Export Control Order (Combat Equipment), 5768-2008; The Defense Export Control Order (Missile Equipment), 5768-2008; The Defense Export Control Order (Controlled Dual-Use Equipment), 5768-2008; and The Defense Export Control Order (Controlled Dual-Use Equipment Transferred to the Palestinian Civil Jurisdiction Areas), 5768-2008.
- Article 2(a)(5) of the FEO prescribes that goods requiring an export license according to the Import and Export Order (Supervision of the Export of Goods, Dual-Use Services and Technology), 5766-2006, are permitted for export according to that order.

In addition to the Free Export Order, there are specific laws that regulate the export of particular types of goods, involving specialized agencies. For example, the Israeli Antiquities Law, 5738-1978 mandates a special license in order to remove antiquities from Israel.[6] The Plant and Plant Products Export Control Law, 5714-1954 requires that all plants be examined prior to export, and approved in accordance with rules promulgated under the law.[7] The Animal and Animal Products Export Control Law, 5717-1957 permits the Minister of Agriculture to subject the export of certain animals and animal products to examination in order to ensure the quality of such exports.[8] The export of fruit, vegetables, and poultry is also regulated under Israeli law and may involve other agencies.[9]

This chapter of the Handbook, however, will focus almost exclusively on Israel's defense and defense-related export controls, which regulate the export of defense equipment, defense know-how, defense services, dual-use items, and encryption items. These categories have become of particular importance over the last few decades, both because of their relative economic weight in Israeli exports and because of Israel's strengths in research and development in these fields, which stems in large part from its overall security situation in the Middle East.

Where to Find the Regulations: As noted earlier, the legal regime regulating most items can be found in the Free Export Order and its annexes, or derived from them, through reference to other laws, regulations, rules, and directives. Each item listed is regulated by the relevant Israeli government ministry or agency.[10] Regarding defense exports, the chief responsible ministry is the Israeli Ministry of Defense (MoD) and, more specifically, the MoD's Defense Export Control Agency (DECA). Information, in Hebrew, regarding export controls on military and dual-use goods can be found on DECA's website. https://exportctrl.mod.gov.il/Pages/default.aspx (last visited: December 27, 2022). The DECA website also includes information regarding international treaties, Israeli law, and controlled lists. In addition, DECA's website provides instructions for defense exporters, as well as forms and related paperwork necessary to apply for the various defense export licenses. However, websites such as DECA's are not necessarily regularly updated, nor are they fully reflective of administrative requirements.

Who Is the Regulator: The MoD is the regulator with the lion's share of responsibility for defense exports, while the MoE is primarily responsible for dual-use export items.

The Ministry of Defense (MoD)

Defense Export Control Agency (DECA)

Under the Defense Export Control Law (DECL),[11] DECA is the licensing authority for all defense marketing, brokering, and export licenses. DECA was established in 2006 with the express purpose of ensuring Israel's national security and defense interests by regulating all forms of licensing and exporting of defense equipment, know-how, and services.[12]

International Defense Cooperation Directorate (SIBAT)

SIBAT is not a regulator per se, but it is responsible for facilitating international cooperation through its various services, such as generating intergovernmental agreements, identifying cooperation opportunities with Israel's defense industry, locating relevant technological solutions for specific requirements, establishing joint ventures, managing sales of IDF inventory, and providing in-depth information on Israel's defense industry.[13]

The Ministry of Economy

The MoD will consult the MoE whenever a license for export of dual-use items is requested. In such cases, a representative from the MoE will join the advisory committee reviewing the application for the export license.[14] Moreover, when dual-use exports are to a civilian end user in an exhaustive list of countries (see Section 20.7(b)(iv)), licensing may be conducted in an expedited manner by MoE, in consultation with MoD and the Ministry of Foreign Affairs (MFA).

The Ministry of Foreign Affairs

The Ministry of Foreign Affairs (MFA) participates in the defense licensing process. When reviewing an application for an export license, representatives from the MFA will often take part in an advisory capacity and advise the MoD on issues bearing on foreign relations. In fact, the MoD is required by law to consult with the MFA prior to granting any defense export license.[15]

The Ministry of Finance's Economic Sanctions Office

Although the Sanctions Office does not regulate export as such, it is responsible for implementing Israel's sanctions policy. Its main focus is on implementing sanctions against trading with the enemy, Iran (in particular), and entities involved in the proliferation of weapons of mass destruction. The Sanctions Office is authorized to investigate and research matters concerning Israel's sanctions policy and advise the Israeli government according to its findings. The Sanctions Office cooperates with all government ministries in order to establish recommendations to policy makers regarding sanctions.[16]

How to Get a License: Prior to obtaining any defense export license, an Israeli citizen, resident, or corporation must first procure a marketing license with respect to defense marketing activity for defense exports and dual-use goods, unless the Defense Minister has granted an exemption from such requirement.[17] In order to obtain a license to market, export, and transfer military and dual-use objects, Israeli citizens must apply for a general or specific license through DECA, which, as the licensing authority, is the final arbiter on all license applications submitted. DECA does consider recommendations of an advisory committee appointed by the Minister of Defense but constituted in coordination with the MFA.[18] The

export and trade of certain *non*-defense-related goods is obtained through the relevant regulating ministry, depending on the nature of the product exported. The Free Export Order prescribes the regulating ministry for each item requiring an export license.[19] An exporter must apply for an export approval or license with the MoE, Ministry of Agriculture, Ministry of Health, or Ministry of Transport, depending on the type or classification of goods intended for export.[20]

Key Websites:

- MoE—International Trade Administration, Export Control Unit: https://israel-trade.net/
- DECA: http://www.exportctrl.mod.gov.il/English/Pages/default.aspx
- SIBAT: http://www.sibat.mod.gov.il/Pages/home.aspx

Caveat Emptor: These websites provide only general information and are not regularly updated.

20.2 Structure of the Laws and Regulations

(a) International Treaties

Generally, Israel has refrained from formally acceding to international treaties or other international arrangements on defense-related export controls, so as not to overly restrict its national security considerations. However, it does voluntarily declare adherence to existing international arrangements, most clearly and importantly to the following:

- The Wassenaar Arrangement. Israel is not a party to the Wassenaar Arrangement, but it has nonetheless incorporated, at minimum, the Wassenaar Arrangement definitions of dual-use items and has adopted the Wassenaar Munitions List.[21]
- The Missile Technology Control Regime (MTCR). Israel is not a party to the MTCR. In September 1991, however, Israel undertook to adhere to the MTCR guidelines without formally joining the regime.[22] Israel has also adopted the MTCR definitions of Missile Technology.[23]

(b) Israel's National Laws and Regulations on Export Controls

The following is a nonexhaustive survey of the main Israeli legislative and regulatory instruments that cover the export of defense, dual-use, and other items.

(i) Israeli Law

- General:
  - Import and Export Order (New Version), 5739-1979[24]
  - Free Export Order, 5782-2022[25]
  - Antiquities Law, 5738-1978[26]
  - Plant and Plant Product Export Control Law, 5714-1954[27]
  - Animal and Animal Product Export Control Law, 5717-1957[28]
  - Council for Fruit and Vegetables (Production and Export) Law, 5733-1973
  - Council for Poultry Law, 5723-1963[29]
  - Diamond Import and Export Control Order, 5739-1979[30]
- Laws and Orders Regarding Defense Export
  - Defense Export Control Law, 5766-2007
  - Import and Export Order (Control of Dual-Purpose Goods, Services and Technology Exports), 5766-2006
  - Import and Export Order (Control of Chemical, Biological and Nuclear Exports), 5764-2004

(ii) Israeli Regulations and Orders

- Defense Export Control Regulations (Methods of Maintaining Registration of Information Regarding Defense Export Deals), 5775-2015
- Defense Export Control Regulations (Licenses), 5768-2008
- Defense Export Control Regulations (Consulting the Ministry of Foreign Affairs when Authorizing Defense Export Licenses), 5768-2008
- Defense Export Control Regulations (Deduction of Economic Sanctions), 5768-2008
- Defense Export Control Regulations (Deduction of Civil Financial Penalty), 5768-2008

- Defense Export Control Regulations (Registration in the Defense Export Registry), 5768-2008
- Defense Export Control Regulations (Exemption from Defense Export License), 5777-2017
- Defense Export Control Regulations (Exemption from Defense Marketing License), 5768-2008[31]
- Defense Export Control Regulations (Extent of Defense Export by Virtue of an Agreement between the State of Israel and Another Country Brought to the Authorization of the Ministers' Committee for National Security), 5768-2008
- Defense Export Control Regulations (Appeal on Decision on the Licensing Authority), 5768-2008
- Defense Export Control Order (Combat Equipment), 5768-2008
- Defense Export Control Order (Controlled Dual-Use Equipment), 5768-2008
- Defense Export Control Order (Missile Equipment), 5768-2008
- Defense Export Control Order (Controlled Dual-Use Equipment Transferred to the Palestinian Civil Jurisdiction Areas), 5768-2008

(c) Controlled Lists

Specific relevant controlled lists have been issued pursuant to the DECL as follows:

- The Israeli Munitions List—Annex to the Defense Export Control Order (Combat Equipment), 5768-2008[32]
- Controlled Dual-Use Equipment—Defense Export Control Order (Controlled Dual-Use Equipment), 5768-2008[33]
- Missile Equipment—Defense Export Control Order (Missile Equipment), 5768-2008[34]
- Transfer to the Palestinian Civil Jurisdiction Areas—Defense Export Control Order (Controlled Dual-Use Equipment Transferred to the Palestinian Civil Jurisdiction Areas), 5768-2008[35]

(d) Israel and UN Security Council Sanctions

Israeli citizens, residents, and corporations are prohibited from brokering transactions between foreign parties with whom the UN Security Council

has prohibited or restricted the transfer of military objects (sanctioned entities).[36] Defense marketing without a license, which is intended to advance transactions with a sanctioned entity, would be considered an offence under severe circumstances and the offenders would be fined accordingly.[37]

(e) Israel's National Laws on Economic Sanctions

(i) Law on the Struggle Against Iran's Nuclear Program, 5772-2012

The law imposes sanctions on all entities aiding Iran in advancing its nuclear program. The law imposes restrictions on corporations that have economic relations with Iran or operate on behalf of Iran or in Iran's territory.[38]

As applied to non-Israeli entities and corporations aiding the Iran nuclear program, the law specifically prohibits Israelis from conducting business with such foreign entities and requires Israelis otherwise engaged with such entities to cease all business activities taking place with them.[39] Israeli individuals violating this prohibition are liable to be sentenced to up to three years in prison or assessed a criminal fine of up to 904,000 NIS.[40] In the event that the violation is committed by an Israeli corporation, the criminal fine is doubled and can amount to as much as 1,808,000 NIS.[41] Furthermore, owners of foreign corporations aiding the nuclear program are prohibited from taking part in any public tenders in Israel, cannot be granted any form of licenses and permits, and will not be entitled to any Israeli government assistance.[42]

The Law on the Struggle Against Iran's Nuclear Program also prohibits Israelis from investing in corporations having economic ties with Iran.[43] Israeli individuals who invest in these foreign corporations may be liable to one year of imprisonment or subject to a criminal fine of up to 678,000 NIS.[44] When the violation is committed by an Israeli corporation, the fine will be doubled and can amount to as much as 1,356,000 NIS.[45] These corporations (which maintain economic ties with Iran) are also prohibited from taking part in public tenders in Israel, cannot be granted licenses and permits, and will not be entitled to any form of Israeli government assistance.[46]

(ii) Other National Laws Imposing Economic Sanctions:

- Law for the Prevention of Distribution of Weapons of Mass Destruction, 5778-2018

  The Law provides that any person or entity involved in assisting in the development, production, distribution or financing of weapons of mass destruction (such as through the transfer of technology or information) will be punished with nine years in prison or a fine of 904,000 NIS. If an entity transferred the technology or information that furthered the development of such weaponry, it will be fined 1,808,000 NIS.[47] Additionally, if an offense has been committed under this law, the officers of the accused entity must prove that they did everything in their power to prevent the offense, otherwise they will be sanctioned with a fine of 226,000 NIS.[48]
- Trade with the Enemy Order (Enemy in Regard to this Order), 5771-2011

  The order provides a list of various companies and persons involved in Iran's nuclear program or related to the Islamic Revolutionary Guard Corps (see Section 20.2(f)).
- Trading with the Enemy Ordinance, 5699-1939

  The ordinance prohibits trade with the enemy and prescribes criminal sanctions for persons who conduct trade with the enemy. According to the ordinance, a person who violates this prohibition will be subject (at a court's discretion) to ten years in prison, and/or a criminal fine of 1,130,000 NIS. If the violation was conducted by a corporate body, the fine is doubled to 2,260,000 NIS. In the ordinance, the term "enemy" is defined as "a country or leader of a country at state of war with Israel; persons living in an enemy country; groups of people (whether organized or not) that conduct business and are under the supervision of one who is considered an 'enemy'; and groups of people that unionized or organized in a country in a state of war with Israel." The following countries are classified as enemy counties: Iran, Iraq, Syria, and Lebanon, though commencing in 2018, Iraq has enjoyed periods of exemption from the list.[49]
- The Counter Terrorism Law, 5776-2016

The law defines “a terrorist organization” as any of the following: (i) “a body of persons in an organized and continuous structure that operates with the intention that terrorist acts will be committed” (the term “terrorist act” is defined within the law), and as (ii) “a body of persons in an organized and continuous structure that acts, directly or indirectly, to assist an organization [as mentioned earlier], and as (iii) “an organization that has been designated outside of Israel as a terrorist organization, provided it has been designated as such pursuant to Part B of the law.”[50] Indeed, part B of the law authorizes the MoD to declare that a group of people qualifies as a terror organization. According to section 18(a) of the law, these MoD determinations would be published on the MoD’s website.[51] The law imposes severe punishments for activities that were intended to aid terror.

The law considers the following as criminal offenses: providing a service or resources to a terrorist organization, where doing so may assist or promote the organization’s activity;[52] performing a property transaction that is capable of assisting, advancing, or financing the commission of a grave terrorist offense (the term “grave terrorist offense” is defined within the law) or rewarding its commission;[53] performing a transaction in property of a terrorist organization or property connected to a grave terrorist offense;[54] and transfer of property to a terrorist organization.[55]

According to article 32(b) of the law, anyone who transacts with property of a person whom he knows to be a “Terrorist Operative” (as defined in the law), or knows that such person or organization in which he takes an active part is subject to a designation pursuant to the law, “will be presumed to have done so knowing that that act is capable of assisting, advancing or financing the commission of a grave terrorism offense or rewarding its commission, as the case may be, unless he proves that he did not know so.”

(f) Israel’s Sanctioned Parties Lists

As of this writing, the following entities are sanctioned by Israel, which essentially means that Israeli citizens may not have economic ties with them

nor invest in them, and such entities may not receive any form of assistance —including licenses or permits—from the Israeli government:[56]

- **Entities involved in Iran's Nuclear and Ballistic Missile Program** —42 corporations involved in the nuclear program.
- **Islamic Revolutionary Guard Corps**—Three companies that are part of the Islamic Revolutionary Guard Corps.
- **Entities owned, operated by, or operating on behalf of the Islamic Revolutionary Guard Corps**—15 corporations operated or controlled by the Islamic Revolutionary Guard Corps.
- **Entities owned, operated, or controlled by the Islamic Republic of Iran Shipping Lines (IRISL)**—Three entities controlled by IRISL.
- **Additional Entities**—12 additional entities related to Iran's nuclear program.
- **Persons Involved in Iran's Nuclear and Ballistic Missile Program or Activities Related to the Program**—20 persons involved in the program.
- **Key Persons in the Islamic Revolutionary Guard Corps**—Seven key members.
- **Additional Persons**—14 persons involved in Iran's nuclear program.

As of November 2022, 75 companies and corporations and 41 persons are sanctioned by Israeli law for their involvement in Iran's nuclear and ballistic missile program. The sanctioned list is based on the following UN Security Council Resolutions:

- Resolution 1737—Lists entities involved in the nuclear program, entities involved in the ballistic missile program, persons involved in the nuclear program, persons involved in the ballistic missile program, and persons involved in both the nuclear and the ballistic missile programs.[57]
- Resolution 1747—Lists entities involved in the nuclear or ballistic missile activities, Iranian Revolutionary Guard Corps entities, persons involved in nuclear of ballistic missile activities, and Iranian Revolutionary Guard Corps key persons.[58]
- Resolution 1803—Lists persons and entities involved in either the nuclear or the ballistic missile program.[59]

- Resolution 1929—Lists individuals and entities involved in nuclear or ballistic missile activities; entities owned, controlled, or acting on behalf of the Islamic Revolutionary Guard Corps; and entities owned, controlled, or acting on behalf of the Islamic Republic of Iran Shipping Lines (IRISL).[60]

20.3 What Is Regulated: Scope of the Regulations

The DECL regulates the export of defense equipment and dual-use objects, the transfer of defense know-how, and the provision of defense services.[61] In addition to national security considerations, the stated purposes of the DECL include safeguarding foreign relations concerns, the fulfillment of international obligations, and preserving other vital interests of the State of Israel.

Export of defense equipment refers to all actions of transferring defense equipment outside of Israel. The regulations also apply to the transfer of defense equipment to the Palestinian Civil Jurisdiction areas,[62] and to a diplomatic or consular representation of a foreign state within Israel.[63]

Israel also regulates the transfer of defense know-how from Israeli sources to persons and entities abroad, as well as to persons and entities within Israel's borders who are not Israeli citizens or residents (including, if applicable, foreign corporations operating in Israel).[64] In general, however, defense know-how is regulated by the same means as defense equipment and can only be transferred and retransferred after obtaining the necessary licenses. Information required for the development or production of defense equipment or its use cannot be transferred without an appropriate license. Furthermore, know-how regarding Israel's defense forces, including information regarding the organization, operation, and policies of Israel's military and police forces, is regulated by the MoD.[65]

All Israeli citizens and corporations also require a license in order to provide defense services to persons who are not Israeli citizens or residents, or to a foreign entity. Such services include those relating to the development, production, maintenance, and use of defense equipment, as well as instruction, training, and consulting relating to defense know-how.[66]

20.4 Who Is Regulated?

Israeli export control regulations apply to all Israeli citizens, residents, and corporations. Israeli corporations are those incorporated in Israel (including, for example, Israeli subsidiaries of non-Israeli business entities), or corporations that have their center of business in Israel and are controlled directly or indirectly by an Israeli citizen or resident.

20.5 Classification[67]

(a) Classification of Dual-Use Items

Dual-use items are classified as materials and equipment initially intended for civilian use, but which are also compatible for defense use.[68] As already noted, Israel has voluntarily incorporated the equipment classification included in the list of the Wassenaar Arrangement into its legal system, as follows:[69]

Category 1: Advanced Materials
Category 2: Materials Processing
Category 3: Electronics
Category 4: Computers
Category 5(1): Telecommunications
Category 5(2): Information Security[70]
Category 6: Sensors and Lasers
Category 7: Navigation and Avionics
Category 8: Marine
Category 9: Propulsion

(b) Classification of Military Items

Military items consist of missile equipment and combat equipment.[71]

- **Missile equipment.** Equipment and software regarding missiles set forth in the appendix on equipment, software, and technologies of the International Missile Technology Control Regime (MTCR).

- **Combat equipment.** Equipment included in the munitions list of the Wassenaar Arrangement; however, restrictions may apply to a broader group of munitions.

20.6 General Prohibitions/Restrictions/Requirements

All cases of exportation or transfer of defense equipment, controlled dual-use items, defense know-how, and defense services by Israeli citizens, residents, and corporations must be authorized by the licensing authority. DECA, in cooperation with the MFA and the MoE (regarding dual-use items), may grant the appropriate license to those who request to take part in defense marketing. Defense marketing is a critical stage in any export process, and if undertaken without appropriate licensing, can lead to criminal or administrative sanctions.

20.7 Licensing/Reasons for Control

(a) Types of Export Control Licenses and Permits for Dual-Use Items

(i) Defense Marketing License[72]

A Defense Marketing License (DML) is required *prior to* conducting any defense marketing activity. Defense marketing activities consist of those activities aimed at promoting defense export transactions and may be geared toward a certain customer or toward the general public. Marketing activities include brokering toward a defense export transaction. Brokering activities may include forging ties between parties to a contract in a defense export transaction, participating in negotiations toward a contract between the parties involved in such a transaction, or representation of a party involved in such a transaction. All these promotional efforts constitute marketing activity, irrespective of whether such activities ultimately result in a defense export transaction.

(ii) Defense Export License[73]

A Defense Export License (DEL) is a prerequisite to exporting defense equipment, transferring defense know-how, or providing a defense service. Israeli citizens, residents, and corporations wishing to take part in any of the aforementioned activities with a person who is not an Israeli citizen or resident, or with a foreign corporation, must obtain such a license in order to export regulated items.

As indicated earlier, in order to procure a DEL, the applicant must first obtain a DML. The issuance of a DML, however, does not obligate the licensing authority to grant a DEL for the same transaction.[74]

(iii) Retransfer License[75]

A defense export license stipulating the identity of the end user would, by its terms, obligate the licensee to prohibit the end user from transferring the security equipment or security knowledge to a third party. In order to permit such transfer to another person, the exporter must obtain a retransfer license from the licensing authority (DECA). The retransfer license will set forth any conditions and terms for transferring the equipment to a different person. However, when the DEL includes a stipulation regarding the end use, it will obligate the licensee to prohibit the end user from making any modifications to the equipment or know-how in its possession.[76]

(iv) End-Use Modification License[77]

Often, a defense export license will be issued with a clear stipulation prohibiting the end user from modifying the end use of the equipment or the know-how. In order to permit modification by the end user, the exporter must obtain an End-Use Modification License from the licensing authority (DECA).

(v) License for Defense Equipment in Transit[78]

A license for Defense Equipment in Transit is issued in connection with, and is necessary in order to effect, export of defense equipment originating from outside of Israel.

(vi) License for Transfer to Palestinian Civil Jurisdiction Areas[79]

In order to transfer controlled dual-use equipment to Palestinian civil jurisdiction areas, the exporter must obtain this specialized form of export license.[80]

(vii) License for Brokering between Foreign Entities[81]

Israeli residents and corporations can only engage in defense-related brokering activity between foreign entities if they first obtain a brokering license. The License for Brokering between Foreign Entities, however, does not permit Israeli citizens, residents, and corporations from engaging in brokering activities that violate any resolution of the United Nations Security Council which forbids or limits the transfer of military equipment to certain foreign entities.[82]

(b) Export Control Licensing Procedure

(i) Defense Export Registry

In order to obtain a DML or DEL, a prospective defense exporter must first register in the Defense Export Registry.[83] Such registration may be denied on a variety of grounds, including a criminal record of the applicant or one of its principals, or a violation of the defense export rules.[84]

(ii) Defense Marketing Licensing Procedure[85]

An applicant for a Defense Marketing License will apply for the license with DECA. The application must include information regarding the equipment, know-how, and services one wishes to market. In addition, the applicant must state the foreign entities with which it intends to trade, and a list of end users. After submitting the application, it is reviewed by DECA. Once the Defense Marketing License is granted, it is valid for four years.

(iii) Defense Export Licensing Procedure[86]

After obtaining the DML, an applicant is eligible to apply for a DEL. The applicant must specify the equipment, know-how, and services it wishes to export, along with the foreign entities to whom it intends to export, and the identity of the end user. After submitting the application, it is reviewed by DECA. Once the license is granted, it is valid for three years.

All applications are submitted to the licensing authority for review (meaning to the Director-General of the MoD, and by the head of DECA, or by a senior official in DECA who has been authorized by the Director-General for that purpose).[87] While reviewing the application, DECA may demand any information regarding the license application, including:

- Declarations by the applicant regarding the end use and the end user of the defense equipment exported;
- Declarations by the end user regarding the intended end use of the defense equipment exported;
- Certificates by the government of the state where the end user is located regarding the identity of the end user and the intended end use of the defense equipment exported; and
- Certificates by the government of the state where the end user is located authorizing the import of the defense equipment.[88]

All applications are reviewed by an interministerial Advisory Committee, which makes its recommendations to the licensing body authorized to grant the license requested. The Advisory Committee includes representatives from the MoD, the MFA, and the Defense Forces (such as the Israel Defense Forces, the Israel General Security Services, the Mossad, the Israeli Police, and the Penitentiary Service). In addition, when reviewing applications regarding dual-use equipment, the Advisory Committee will include a representative from the MoE.[89]

(iv) License to Export Dual-Use Items

As part of the Import and Export Order (Control of Dual-Purpose Goods, Services and Technology Exports), 5766-2006, export of dual-use items listed in the Wassenaar Arrangement requires licensing from the MoE.[90] In cases where the end user is a military user, the licensing authority is DECA.[91] License applications are generally handled within 20 days, following the MoE's consultations with the MoD and the MFA.[92] However, a fast-track procedure also is in place whereby export licenses may be expedited and be granted within five days. The countries eligible for the fast-track approval process are currently: Austria, Australia, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania,

Luxemburg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, the United Kingdom, and the United States.[93]

20.8 General Licenses/License Exceptions

(a) General Licenses

There are no general licenses, but there are expedited licenses (see Section 20.7) and exemptions from licensing.

(b) License Exceptions

(i) Exemptions from a DML

The Licensing Authority may exempt an applicant from having to procure a DML if the subject matter of the application involves the following activities:[94]

- Exhibiting, showing, or demonstrating defense equipment in an exhibition with the intention of marketing (assuming the equipment is not classified).
- Advertising through the internet, or other mass media platforms, information regarding marketing of defense equipment, know-how, or services (provided these items are not classified).
- Defense marketing activities with an entity in a country listed for this exemption, provided that the defense export is not classified.
- Defense marketing activities in preparation for exporting defense equipment that was returned to Israel for servicing, but not for modification or improvement.
- Defense marketing activities in preparation for exporting defense equipment necessary to receive defense services outside of Israel for said equipment.
- Defense marketing activities intended to transfer defense know-how that is not classified and that is necessary for the production of defense equipment outside of Israel (for ultimate reshipment back to Israel).

- Defense marketing activities in preparation for transferring technical specifications necessary for production of an unclassified component outside of Israel (for ultimate reshipment back to the provider of the technical specifications, in Israel).
- Defense marketing activities in preparation for the return of defense knowhow (that was initially and legally transferred to Israel) back to the entity outside Israel that transferred the said know-how.
- Actions in preparation for the transfer of defense know-how that has been authorized by the MoD.
- Actions in preparation for the transfer of defense know-how which has been classified as "common knowledge."[95]

(ii) Exemptions from a DEL

An applicant will be exempt from having to procure a DEL for the following activities:[96]

- Transfer of defense know-how for the production of unclassified military equipment outside of Israel, in a permitted country (for ultimate reshipment back to the provider of the know-how, in Israel).[97]
- Returning defense know-how to an entity outside Israel (which had originally transferred the know-how to Israel).
- Export of certain unclassified defense equipment for the purpose of presenting the equipment in an exhibition in a permitted country (subject to limitations on the number of items of equipment and the length of time such equipment may be outside the State of Israel).
- Export of certain unclassified defense equipment for the purpose of demonstrating the equipment's use to the end user, in a permitted country (subject to limitations, as above).
- Export of unclassified defense equipment (legally exported no more than ten years beforehand) that belongs to an end user in a permitted country, after the equipment was serviced in Israel.
- Return of (fewer than 50 items of) unclassified defense equipment that was not produced in Israel and was not modified or improved while in Israel.
- Transfer of defense know-how that has been classified as common knowledge.[98]

The State of Israel is exempt from all licensing requirements. That is, a government-to-government agreement is not subject to the restrictions of the Defense Export Control Law and does not require licensing.[99]

20.9 Penalties, Enforcement, and Voluntary Disclosures

With respect to covered products, know-how, and services, DECA's Enforcement Unit is responsible for overseeing compliance with the defense export laws and regulations. The Enforcement Unit can make recommendations to the administrative authority regarding the imposition of economic or criminal sanctions for those who violate the terms of Israel's export controls.

Exporters suspected of violating these terms may be summoned to a hearing before an enforcement committee chaired by the head of DECA and other representatives of the MoD. Following the hearing, the committee can choose to begin a criminal investigation or impose administrative sanctions.[100]

(a) Administrative Penalties

The licensing authority may impose a civil penalty in the amount of 15 percent of the fine established under the criminal penalties section of the DECL when there are reasonable grounds to assume that defense marketing activities or defense exports were conducted in contravention to the licensing requirements.[101]

(b) Criminal Penalties

Acts of defense marketing, exporting, transferring, and brokering that are conducted without an appropriate license are punishable by three years' imprisonment for those found guilty of such actions, or a fine of 6,780,000 NIS (30 times the sum of the amount prescribed in section 61(a)(4) of the Criminal Law).[102]

If any of the preceding offenses are committed under severe circumstances, the sentence will be five years imprisonment or a 11,300,000 NIS fine (50 times the sum of the amount prescribed in section

61(a)(4) of the Criminal Law). The law defines the term "severe circumstances" to include:

- Defense marketing or exporting intended to advance a transaction with the enemy.
- Export of equipment, know-how, or services deemed "classified" by the relevant security agency.
- Marketing or exporting activities intended to advance a transaction with a foreign entity in violation of a Security Council resolution.
- Marketing activity or export that violates one of the stipulations of the license granted as it pertained to the restriction on marketing or export to certain counties.[103]
- Mediating between foreign parties intending to promote a transaction with an enemy.

(c) Enforcement

DECA's Enforcement Unit is responsible for overseeing that all transactions regarding defense export comply with Israeli export controls.

(d) Voluntary Disclosures

Voluntary disclosures do not exempt the offender from penalties and sanctions but may result in the mitigation of penalties amounting to 25 percent of the corresponding civil fine.[104] Three recent voluntary disclosure cases, in which exporters admitted to failing to obtain the necessary license or failing to comply with license terms, resulted in administrative fines after appearances before DECA enforcement unit administrative hearings.[105]

20.10 Recent Export Enforcement Matters

Since 2014, there have been 36 reported cases of export control violations where enforcement was implemented and offenders (in closed cases) were punished. All the cases involved exporters marketing, exporting, or re-exporting without an appropriate license, or not complying with the terms of the license they legally obtained. In addition, all the enforcement actions have been administrative, resulting in hearings before DECA's enforcement

unit. Since 2014, there has only been one defense export case where the dispute was brought before an Israeli court.

In addition, the enforcement punishment in all the closed cases was the imposition of an administrative fine on the violating exporters. In six of the cases, the exporters—each a repeat offender or an offender who operated under severe circumstances—were fined the maximum amount permitted by the DECL.[106]

20.11 Special Topics

(a) Re-exports/Extraterritorial Application of Laws

The foreign end user of Israeli defense equipment or defense know-how is prohibited from re-exporting the equipment or know-how to a third party unless the Israeli DEL holder has obtained a re-transfer license from the licensing authority.[107]

(b) Intangible Transfer of Technical Information

As noted in Section 20.3 Israel regulates the transfer of defense know-how, and any transfers of technical information, through whatever media (including email or other electronic or web-based means), are forbidden unless the transferor is in possession of a defense export license, or has been granted an exemption from the requirement to do so.[108] Article 15(a)(2) of the DECL provides, in relevant part, that unless a person holds the requisite license, such person may not "transfer defense know-how through any means, including orally—from Israel to outside of Israel, or in Israel to a person who is not an Israeli citizen or an Israeli resident, or a foreign corporation. . . ."[109] The DECL leaves little doubt that the term "technology" is subsumed within the broad definition of the term "defense know-how,"[110] so a DEL would indeed be required for any person intending to export controlled technology, as well as for any person involved in any deemed export of controlled technology to a person in Israel who is not an Israeli citizen.

(c) Recordkeeping

Export license holders are obligated to maintain records describing the transactions they have conducted. These records must detail the defense equipment, know-how, and services transferred, as well as specific information regarding the interim and end users and the end use of the equipment, know-how, and services transferred. These records must reflect the dates of the transactions and must be maintained for ten years from the transaction completion date.[111]

20.12 Encryption Controls

(a) General Comments

Israel regulates the use of encryption items outside the framework of its Defense Export Control Law, through the Order Regarding the Engagement in Encryption Items 5734-1974, as amended in 1998, promulgated pursuant to the Law Governing the Control of Goods and Services, 5717-1957 (referred to collectively herein as the Encryption Order).[112] The MoD regulates engagement in this field through a system of control and licensing for encryption items, the purpose of which is to enable the Israeli encryption industry's development while safeguarding Israel's national security interests. A special encryption committee within the MoD is responsible for reviewing license applications to engage in encryption activities.

The Encryption Order defines the term "Engagement in Encryption Items," in part, as the development, production, possession, use, import, transfer, handling from one location to another or from one person to another, distribution, sale or purchase of encryption items, encryption key, or records relating to encryption,[113] and the MoD is empowered via the Encryption Order to either enable (via license or exemption) or prohibit such activities. That is, transactions (such as sales and distribution via import and export) involving engagement in encryption items, whether as stand-alone items or integrated into defense or other dual-use goods, require a scope of review to areas (development, production, possession, etc.) extending beyond the marketing and export controls for defense products and services.

Though the type of encryption-related activities subject to MoD review is indeed broader than those subject to the general export control rules, in practice the MoD has adopted a commercially focused approach to its review process with encryption items. For example, under the letter of the law, commercial encryption may be regarded as dual use and therefore subject to control. However, since the MoD does not recognize commercial encryption (i.e., encryption that has been designed and intended for commercial use) as a military product, the control over commercial encryption items differs from defense export controls as described in the encryption licensing requirements that follow.

(b) Import Encryption Clearance Requirements

An importer who wishes to sell commercial encryption items needs to obtain a license for selling and distributing encryption items within the State of Israel. The applicant is required to submit information to the MoD regarding the encryption item, including its description and function, the encryption algorithm, and the relevant key length for each algorithm.[114] Once licensed, the importer must record sales information and submit said information to the MoD upon request.[115]

(c) Encryption Licensing Requirements

Engagement in encryption items requires a license authorized by the Director General of the MoD. Persons wishing to engage in encryption items must submit an application for a license to the Director General.[116] Each application shall be reviewed by an advisory committee (which must include a representative from the public), which will make recommendations to the Director on whether to grant, refuse, stipulate conditions for, suspend, or revoke a license.[117]

There are three categories of licenses for engagement in encryption:[118]

(i) General License

The general license grants the license holder free use of a particular encryption item with no time limit as to its validity. The sale of the encryption item pursuant to the General License is not controlled and is not subject to reporting procedures.

(ii) Special License

License for a specific engagement. The special license is geared toward a specific engagement, including a particular transaction, in certain encryption items such as sales to customers who are not subject to the limitations or prohibitions one would encounter with a restricted license. Such a license is valid for one year.

(iii) Restricted License

The restricted license imposes limitations on engagement in encryption items, including restrictions applicable to otherwise permissible forms of engagement in encryption items, or to the nature of permissible sales. The restricted license will generally be focused on preventing improper use of the encryption item and restricting the sale of encryption items to certain countries and sectors. This form of license is generally valid for one year.

Though the regulatory regime for items of encryption can appear strict, the MoD has taken a fairly commercially minded approach to the trade in encryption technologies in certain circumstances. This follows the 1998 amendment to the Encryption Order which introduced a "Free Means" exemption from the encryption regulatory regime. The term "free means" is defined as "a means of encryption for which a general license has been granted, or for which the Director General of the MoD has relieved control."[119] An encryption item that has been defined as a free means is free of all licensing restrictions. As of November 2022, there were more than 13,000 free means encryption technologies.[120]

The MoD updates its policies regarding encryption items with a series of announcements, including in areas where it maintains tight controls. For example, the MoD has made clear that it is absolutely prohibited from exporting any items of encryption to a list of "prohibited countries," which currently means (inclusive) no trade in encryption whatsoever with or to Iran, Syria, North Korea, Lebanon, Sudan, and Cuba.[121]

(d) Penalties for Violation of the Encryption Order

Persons who violate the Encryption Order may be imprisoned for up to three years or fined. Violations committed under severe circumstances may warrant a punishment of five years imprisonment or a fine.[122] If violations

are conducted by a group of people, all group members are liable for the punishment. Should the violations be conducted by an employee pursuant to an employer's instructions, the employer is also liable for punishment.[123] For example, in 2016 an Israeli company was fined for violating encryption license restrictions by signing a contract to sell Israeli software to a foreign entity and transfer the software's encryption code. Though the transfer was never completed, the company was fined the sum of 355,950 NIS.[124]

---

1. Adv. Jeffrey Rashba, a member of the Israeli and District of Columbia Bar Associations, co-chairs the international transactions practice at S. Friedman, Abramson & Co. (Haifa, Jerusalem & Tel Aviv; www.sfa.law); Tomer Broude is the Dean of the Faculty of Law and the Bessie & Michael Greenblatt, Q.C., Chair in Public and International Law at the Faculty of Law and Department of International Relations at the Hebrew University of Jerusalem; Danielle Regev is an LLM student specializing in public and international law at the Hebrew University of Jerusalem.
2. Israeli laws are identified by the year of their enactment, according to both the Hebrew calendar (listed first) and the Gregorian calendar, hence the numerals following the law's name.
3. The Ordinance refers to the Ministry of Industry, Trade and Tourism, which has changed its name several times over the years but is referred to herein as the Ministry of Economy, or MoE.
4. Annex 1, Free Export Order. 5782-2022.
5. Annex 2, Free Export Order, 5782-2022.
6. Antiquities Law § 15, 5738-1978.
7. Plant and Plant Product Export Control Law, 5714-1954.
8. Animal and Animal Product Export Control Law, 5717-1957.
9. Council for Fruit and Vegetables (Production and Export) Law, 5733-1973; Council for Poultry Law, 5723-1963.
10. Free Export Order, 5782-2022.
11. Defense Export Control Law (DECL) § 2, 5766-2007.
12. https://exportctrl.mod.gov.il/About/Pages/Goals.aspx.
13. https://english.mod.gov.il/Departments/Pages/InternationalDefenseCooperation.aspx.
14. Defense Export Control Law § 24(b)(3), 5766-2007.
15. *Id*. § 27.
16. https://www.gov.il/he/departments/general/about_sanctions_headquarters.
17. Defense Export Control Law, § 14(b) and 16, 5766-2007.
18. *Id*., Articles D–E.
19. Annex 1, Free Export Order, 5782-2022.
20. *Id*.
21. Defense Export Control Law § 2, 5766-2007; and the Dual-Use Order.
22. https://exportctrl.mod.gov.il/Hakika/Pages/MTCR.aspx.
23. Defense Export Control Law § 2, 5766-2007.
24. Last Update: 2022.
25. Last Update: 2022.
26. Last Update: 2010.
27. Last Update: 2015.
28. Last Update: 2015.
29. Last Update: 2018.
30. Last Update: 2014.
31. The list of items not exempt from a defense marketing license was last updated in 2018.

32. The Controlled Lists promulgated pursuant to the Defense Export Control Law and referenced in Section 20.2(c) herein are available for review (as of November 2022) only in Hebrew-language sources, as follows: https://exportctrl.mod.gov.il/Hakika/Pages/240618.aspx.
33. https://exportctrl.mod.gov.il/Hakika/Pages/240618.aspx.
34. https://exportctrl.mod.gov.il/Hakika/Pages/240618.aspx.
35. https://exportctrl.mod.gov.il/Hakika/Pages/240618.aspx.
36. Defense Export Control Law § 22, 5766-2007.
37. *Id*. § 33.
38. Law on the Struggle Against Iran's Nuclear Program § 1, 5772-2012.
39. *Id*. § 4.
40. *Id*. § 29. Criminal fines referenced in this section are accurate as of November 2022.
41. *Id*.
42. *Id*. § 5.
43. *Id*. § 10.
44. *Id*. § 29.
45. *Id*.
46. *Id*. § 11.
47. Law for the Prevention of Distribution of Weapons of Mass Destruction, § 13, 5778-2018.
48. *Id*. § 16.
49. General Authorization According to the Order of Trade with the Enemy, 1939 (File No. 8059). The Minister of Finance has even authorized trade with Iraq on occasion since 2018 (including an extension—as of the time of this writing—until March 31, 2023), but the status of any contemplated trade with Iraq must be checked and confirmed regularly.
50. The Counter Terrorism Law, § 2 5776-2016.
51. https://nbctf.mod.gov.il/he/Announcements/Pages/nbctfDownloads.aspx.
52. The Counter Terrorism Law, §23 5776-2016.
53. *Id*. § 32(a)(1).
54. *Id*. § 32(a)(2).
55. *Id*. § 32(a).
56. Order of Trade with the Enemy (Enemy in regard to this Order), 5771-2011.
57. United Nations Security Council Resolution 1737 (2006).
58. United Nations Security Council Resolution 1747 (2007).
59. United Nations Security Council Resolution 1803 (2008).
60. United Nations Security Council Resolution 1929 (2007).
61. Defense Export Control Law § 1.
62. DECL § 20, with reference to the definition of these areas in Article 2 DECL, essentially the areas whose civil administration was transferred to the Palestinian Authority in 1995 under the Israeli-Palestinian "Interim Agreement." The Defense Export Control Order (Controlled Dual-Use Equipment transferred to the Palestinian Civil Jurisdiction Areas), 5768-2008, deals with the transfer of dual-use equipment to the Palestinian Authority.
63. DECL § 2.
64. *Id*. §15(a)(2).
65. *Id*.
66. *Id*. § 15(a)(3).
67. This section relates exclusively to defense and defense-related exports.
68. DECL § 2 (definition of "dual-use equipment").
69. Order of Defense Export Control (Controlled Dual-Use Objects), 5768-2008.
70. Category 5(2) generally includes the regulation of the export of encryption products. Apart from items regulated within the Order Governing the Control of Commodities and Services (Engagement in Encryption Items), 5734-1974 (see Chapter 20.12 herein), the term "Means of

Encryption" refers to tools of encryption, encryption code, and records relating to encryption or methods of encryption. One will not undertake an activity relating to means of encryption without a specific license from the Director-General of the MoD.

71. Defense Export Control Law § 2.

72. *Id*. § 14.

73. *Id*. § 15.

74. *Id*. § 16.

75. *Id*. § 17.

76. *Id*. § 18.

77. *Id*. § 18.

78. *Id*. § 19.

79. *Id*. § 20.

80. For definition of "Palestinian civil jurisdiction areas" see provision referenced in footnote 63 *supra*.

81. DECL § 21.

82. *Id*. § 22.

83. *Id*. § 3(a)(1).

84. *Id*. § 4.

85. https://exportctrl.mod.gov.il/Guide/Pages/Step4.aspx.

86. https://exportctrl.mod.gov.il/Guide/Pages/Step5.aspx.

87. Defense Export Control Law, § 2 [definition of "licensing authority"]; an online licensing portal (in Hebrew) can be found at https://exportctrl.mod.gov.il/About/Pages/Froms.aspx.

88. DECL § 6(b).

89. *Id*. § 24.

90. For the online licensing portal, see (in Hebrew) https://forms.gov.il/globaldata/getsequence/getHtmlForm.aspx?formType=fta5newhasava@moital.gov.il&maslul=6.

91. Directive 3.5 of the Director General of the MoE, § 1.3, 5778-2018.

92. *Id*. § 8.3.

93. *Id*. §§ 6.2, 8.5. Countries with which Israel enables the fast-track process enjoy favorable trade relations with Israel overall. In addition to the fast-track status for the United States, it is worth noting that Israel has no "blocking" or anti-boycott legislation to try to prevent or restrict the extraterritorial legal and economic effects of U.S. sanctions laws (such as those implemented vis-à-vis Cuba and Iran).

94. Defense Export Control Regulations (Exemption from Defense Marketing License), 5768-2008.

95. See DECL § 2 definition of "Security Knowledge." "Common Knowledge" is defined in the Defense Export Control Law as information that has been made public by legal means, and is not subject to restrictions on its distribution.

96. Defense Export Control Regulations (Exemption from Defense Export License), 5777-2017.

97. A list of "permitted countries" is maintained by the MoD, is not a matter of public record, and is made available only to entities registered in the MoD's Defense Export Registry (see Section 20.7(b) *supra*). Following admittance to the Registry, entities may receive the permitted countries list, but solely on the conditions that such list will not be disclosed to any third party and will be treated in the strictest confidence.

98. For definition of "common knowledge," see footnote 95.

99. Defense Export Control Law § 47.

100. https://exportctrl.mod.gov.il/Achifa/Pages/about.aspx.

101. Defense Export Control Law § 35.

102. *Id*. § 32.

103. *Id*. § 33.

104. Defense Export Control Regulations (Reduction of Civil Fines) § 2(2), 5768-2008.

105. https://exportctrl.mod.gov.il/Achifa/Pages/events.aspx.

106. *Id*.

107. Defense Export Control Law, § 17.

108. Article 15(a)(2) DECL. Article 15(b) of the DECL specifically enables the Minister of Defense to prescribe an exemption from the obligation to obtain a DEL with respect, inter alia, to certain types of defense equipment and defense know-how.

109. Article 15(a)(2) DECL.

110. The term "defense know-how" is defined broadly in Article 2 (Definitions) of the DECL, in part, as "Information that is required for the development or production of defense equipment or its use, including information referring to design, assembly, inspection, upgrade and modification, training, maintenance, operation and repair of defense equipment or its handling in any other way as well as **technology i**ncluded in the order under paragraph (1) of the 'Controlled Dual-use Equipment' definition and in the orders under the 'Missile Technology' and 'Defense Equipment' definitions; for this purpose, information—**including technical data or technical assistance**."

111. Defense Export Control Law § 31.

112. The Encryption Order defines the term "encryption item" to mean any device, mechanical, electro-mechanical or electronic instrument or any part thereof, or any model of a device or instrument or any part of said model, that is or can be operated semi-automatically or manually, including secret writing that is or can be activated by writing or printing and that cause or are intended to cause total or partial scrambling of data for any period of time by someone who has or does not have an encryption key.

113. The definition is found in a declaration which was attached to the Order and confirmed that engagement in encryption items was a controlled service, and is known as the Declaration Regarding the Control of Goods and Services (Engagement in Encryption Items), § 1.

114. For the online licensing portal, see (in Hebrew) https://www.mod.gov.il/English/Encryption_Controls/Pages/FAQ-Encryption-Controls-.aspx.

115. *Id*.

116. Order Governing the Control of Commodities and Services (Engagement in Encryption Items), 5735-1974, §§ 2–3; for the online licensing portal, see https://forms.mod.gov.il/EncryptionLicenseHe.

117. *Id*. § 10a.

118. https://www.mod.gov.il/English/Encryption_Controls/Pages/default.aspx.

119. Order Governing the Control of Commodities and Services (Engagement in Encryption Items), 5735-1974 §§ 1, 3(b).

120. For a list of all "free means" encryption technologies, see https://www.mod.gov.il/Service_Business/API/encryption/Pages/FreeMeans.aspx.

121. https://www.mod.gov.il/English/Encryption_Controls/Pages/FAQ-Encryption-Controls-.aspx (valid as of December 2022).

122. Law Governing the Control of Commodities and Services § 39(b), 5718-1957.

123. *Id*. § 39a-b.

124. https://exportctrl.mod.gov.il/Achifa/Pages/events.aspx.

21

Export Controls and Economic Sanctions in Italy

Marco Zinzani and Simone Cadeddu[1]

21.1 Overview

Italy is a member state of the European Union (EU), which has exclusive competence in the common commercial policy pursuant to Article 3, paragraph 1, letter (e), of the Treaty on the Functioning of the European Union (TFEU). Consequently, Italy fully adheres to the EU commitments with regard to export controls and abides by all relevant policies set up at the EU level.

Similarly, Italy fully adheres to the sanctions regimes established by the EU. The EU sanctions policy falls within the framework of the Common Foreign and Security Policy (CFSP). Sanctions regimes are established by CFSP Decisions, which are binding on EU member states. CFSP Decisions are normally implemented by further secondary legislation in the form of EU regulations (which are adopted under Article 215 of the TFEU).

EU regulations concerning export controls and economic sanctions are binding in their entirety and are directly applicable in all EU member states from the time they enter into force, in accordance with Article 288 of the TFEU. Therefore, they are not subject, in their implementation or further effects, to the adoption of any subsequent measure by the member states. Nevertheless, each member state, including Italy, is requested to lay down the rules applicable to the infringements of the provisions of the relevant EU regulations and to take all measures necessary to ensure that such

provisions are fully implemented. While military goods export legislation was traditionally exempt from EU rules, since 2009 (Directive 2009/43/EC) a common framework aimed at regulating intra-European movement of military items has been adopted, including a common military goods list. Extra EU movement of military goods is still left to member states legislation, under the general framework of the European Common Military Policy.

(a) What Is Regulated?

(i) Export Controls

In adherence to the policies of the European Union, the export from Italy to non-EU countries of a certain number of products is subject either to prohibitions or restrictions. The most significant controlled goods are listed here, each of them with the applicable EU legislation, and the relevant national legislation (if any).

Goods	**Applicable EU legislation**	**National legislation**
Dual-use items	Regulation (EU) 2021/821	Legislative Decree No. 221/2017
Firearms, their parts and components and ammunition	Regulation (EU) No. 258/2012	Law No. 110/1975
Military technology and equipment	Council Common Position 2008/944/CFSP	Law No. 185/1990
Cultural goods	Regulation (EU) 2019/880	Legislative Decree 42/2004
Goods that could be used for capital punishment, torture, or other cruel, inhuman, or degrading treatment or punishment	Regulation (EU) 2019/125	Legislative Decree No. 221/2017
Dangerous chemical substances	Regulation (EU) No. 649/2012	Legislative Decree No. 28/2017
Drugs and psychotropic substances	Regulations (EC) No. 273/2004; 111/2005; 1277/2005	Legislative Decree No. 50/2011
Supervision and control of shipments of radioactive waste and spent fuel	Directive 2006/117/EURATOM	Legislative Decree No. 101/2020
Responsible and safe management of spent fuel and radioactive waste	Directive 2011/70/EURATOM	Legislative Decree No. 101/2020

Shipments of waste	Regulation (EC) No. 1013/2006	Legislative Decree No. 152/2006
Cat and dog furs	Regulation (EC) No. 1523/2007	Law No. 189/2004 and Legislative Decree No. 47/2010
Wild fauna and flora	Regulation (ECC) No. 338/1997	Law No. 150/1992 and Legislative Decree No. 275/2001
Substances that deplete the ozone layer	Regulation (EC) No. 1005/2009	Legislative Decree No. 108/2013
Fluorinate greenhouse gases	Regulation (EC) No. 842/2006	Legislative Decree No. 163/2019
Food and food additives	Regulation (EC) No. 882/2004	Legislative Decree No. 194/2008
Genetically modified organisms	Directive 2001/18/CE, Regulation (EC) No. 1946/2003	Legislative Decree No. 224/2003
Common rules for export (Article 5 permits the Commission to adopt temporary export control measures in order to prevent or remedy critical situations arising from shortages of essential products)	Regulation (EU) 2015/479	—
Mercury	Regulation (EU) 2017/852	Penalties pursuant to Legislative Decree No. 189/2021
Rough diamonds	Regulation (EC) No. 2368/2002	Penalties pursuant to Royal Legislative Decree no. 1923/1926
Materials used in the main components of footwear for sale to the consumer	Directive 94/11/EC	Ministerial Decree 11th April 1996
Textile fiber names and related labeling and marking of the fiber composition of textile products	Regulation (EU) No. 1007/2011	Legislative Decree No. 190/2017

(ii) International Economic Sanctions

Italy, as a member state of the European Union, fully implements economic sanctions adopted at the European level and provided by EU regulations concerning restrictive measures imposed against third countries.

(b) Where to Find the Regulations

As shown in the table, the legislation in force on export controls and economic sanctions is spread among various legislative and regulatory acts, mostly originating from the EU.

All EU export control and sanctions laws and regulations are publicly available in English and can be accessed on the official repository of EU law (www.eur-lex.europa.eu). Italian pieces of legislation can be accessed through online repositories of laws or on the dedicated webpages of the competent ministries/authorities.

Italian Legislative Decree 221/2017—which came into force on February 1, 2018—lays down a set of rules regarding (1) the adaptation of national law to the European legislation with a view to simplifying and rationalizing the procedures for obtaining export authorizations of dual-use products and technologies; (2) the application of restrictive measures adopted pursuant to Article 215 of the Treaty on the functioning of the European Union (TFUE); and (3) the export of goods listed in Regulation (EC) No. 1236/2005 concerning trade in certain goods that could be used for capital punishment, torture, or other cruel, inhuman, or degrading treatment or punishment. The adoption of Legislative Decree 221/2017 was welcomed by economic operators since before that there was no single and consistent piece of Italian legislation governing export controls and economic sanctions and there remained scope for differing interpretations of the applicable provisions by the operators and the various competent authorities. Until 2018, for instance, significant legal uncertainties existed, in particular, with regard to the penalties applicable to infringements of the provisions of Regulation (EU) no. 267/2012 concerning restrictive measures against Iran.

As far as restrictions against designated persons and entities are concerned, Legislative Decree no. 109/2007 “measures to prevent, counter and punish the financing of terrorism and the activities of countries that threaten peace and international security, implementing Directive 2005/60/EC”; it includes provisions applying to Italian persons and entities relating to sanctions in the form of the freezing of certain natural and legal persons’ funds and economic resources.

Specifically, this act provides for some definitions such as those of “funds” and “economic resources”; it is worthwhile noting that Article 5(4) of the act expressly prohibits funds or economic resources to be directly or indirectly made available to designated persons or applied to their benefit.

In order to verify if there are restrictions in place on a particular good or for certain services, a database is made available by the Customs Agency at https://aidaonline7.adm.gov.it/nsitaricinternet/.

Three main bodies of primary legislation regulate cross-border transactions concerning military goods:

- Law 9 July 1990 no. 185 (New Rules on Import, Export and Transit Controls of Military Goods) is the text of reference for both intra-EU transfers and extra-EU export controls, including rules on imports, exports, licenses, offsets, and penalties (the current enactment regulation was adopted with Ministry of Foreign Affairs decree 7 January 2013 no. 19).
- Royal Decree 18 June 1931, no. 773, regulates national military goods production and manufacturing and contains provisions (art. 28) on the export of weapons not included in the military good lists and self-defense items intended for law enforcement agencies.
- Additional rules are included in Legislative Decree 15 March 2010, no. 66 (Military Legal System Code) and its implementing provisions (President of the Republic Decree 15 March 2010, no. 90), which dictate how an undertaking may become registered with the National Registry of Undertakings, thus becoming eligible to apply for export authorizations of military goods.

Further enactment provisions include the Italian Military Control List issued with Ministry of Defense Decree 29 September 2021 and the Italian Regulation 6 May 2015, no. 104 on government-to-government cooperation.

(c) Who Is the Regulator?

Italian rules on export controls and economic sanctions require the involvement of several administrative and regulatory authorities. Leaving aside those authorities in charge of managing certain sectorial export controls regimes, it is worth mentioning the following authorities.

The Foreign Affairs Ministry, DG for Global Affairs (*Ministero degli Affari Esteri e della Cooperazione internazionale*), holds primary political responsibility for implementing the economic sanctions regimes and participates at the international and European level in negotiations with regard to restrictive measures in force and possible waivers.

The Unit for Authorizations of Military Goods—UAMA within the Ministry of Foreign affairs—DG for the Promotion of the National System (*Unità autorizzazioni materiali d'armamento*) is an administrative body that enjoys wide autonomy as the national authority responsible for the authorization of export, import, transit, provision of technical assistance and brokering services related to military goods, and, as of January 1, 2020, dual-use products, "not listed" dual-use items, goods subject to Regulation (EU) 2019/125 of the European Parliament and of the Council of 16 January 2019 concerning trade in certain goods that could be used for capital punishment, torture, or other cruel, inhuman, or degrading treatment or punishment (hereinafter, the Anti-torture Regulation) or items listed as a result of EU restrictive measures against certain third countries, adopted in accordance with Article 215 TFUE.

High level political guidance is provided by the Interministerial Committee on Exchanges of Military Goods (*Comitato interministeriale per gli scambi di materiali d'armamento per la difesa*), which comprises the Ministries of Defense, Foreign Affairs, Interior, Economy and Economic Development. The head and deputy head of UAMA are officials from the Ministry of Foreign Affairs, holding envoy rank, but the Unit personnel includes analysts from the Ministry of Defense and the Armed Forces. Informal guidance can be sought and obtained by undertakings consulting UAMA, even if no formal process exists. UAMA does publish a number of directives and guidelines concerning the license and authorization procedures falling within its jurisdiction.

UAMA authorization proceedings concerning military goods are conducted with the support of the General Secretariat of the Ministry of Defense, the Defense Staff and the Advisory Committee whose functions are provided by Article 7 law no. 185 of 1990. The Committee is chaired by a representative from the Ministry of Foreign Affairs and made up of 11 representatives from the Ministries of Interior, Defense, Economic Development, Economy and Environment. A diplomatic official from the Ministry of Foreign Affairs acts as secretary. Meetings are held monthly. The opinions rendered by the Committee on each export authorization are mandatory but nonbinding, meaning that UAMA cannot issue an authorization without first obtaining the Committee's opinion on that authorization, but is not obliged to follow such Committee's opinion—in

such a case, UAMA would be required to provide a detailed explanation of the reasons why it decided not to follow the Committee's advice.

With regard to dual use and other controlled goods, UAMA avails itself of the opinion, compulsory but nonbinding (see preceding description), of an Advisory Committee set up by Legislative Decree 221/2017. The consultative committee is composed of representatives of the Ministries of Economic Development, Economic Affairs and Finance, Defense, Interior, Communications, Education-University-Research, and Health. Meetings of the Advisory Committee generally take place once a month.

The Ministry of Economy and Finance (*Ministero dell'Economia e delle Finanze*—MEF) is in charge of monitoring the national system for the prevention and sanctioning of financing terrorism and money laundering. While it plays no role with regard to the export controls policy, it certainly plays an important role in the implementation of international economic sanctions. The Ministry is assisted in its tasks by the Financial Security Committee (FSC), an intergovernmental body whose status, functioning, and powers are provided for by Article 3 of Legislative Decree no. 109 of 2007. The Committee is chaired by the Director General of the Treasury and made up of 11 representatives from the Ministries of Foreign Affairs, Interior and Justice, the Bank of Italy, CONSOB (Italy's Stock Exchange Commission), the Ufficio Italiano dei Cambi (Italy's Unit of Financial Information), the Guardia di Finanza (Customs Police), DIA (the Anti-mafia Investigative Directorate), and the Carabinieri Corps. The Committee has far-reaching powers that include waiving provisions of the existing secrecy laws to obtain information from all government ministries. Legislative Decree no. 109/2007 also empowers the FSC to submit proposals to the competent UN or EU authorities on the listing or delisting of individuals or entities subject to restrictions on financial transactions and/or asset freezes for combating the financing of terrorism purposes. The FSC is in charge of issuing authorizations for financial assistance related to goods and technology subject to EU restrictive measures, if and when required. The FSC is also responsible for conducting controls in the area, applying administrative sanctions and, if necessary, alerting the public prosecutor.

The Italian Customs Agency (*Agenzia delle Dogane e dei Monopoli*) is in charge of enforcing the companies' compliance with export control and economic sanctions particularly on the exported or imported goods. The

agency operates alone and in cooperation with the police forces (among these the specialized finance police, Guardia di Finanza is the most active). Despite it being subject to the coordination of the Ministry of the Economy and Finance, the Customs Agency constantly communicates to UAMA, the other police forces, and the intelligence apparatus any relevant information acquired during its controls on imported/exported goods. Should any irregularities be found, a warning may be issued or an official report to the judiciary be drawn up. The latter, through the public prosecutor, will then decide whether an investigation and/or a trial is necessary. There are more than 80 peripheral offices of the Customs Agency and their methods for handling export controls may vary among them to some extent, despite the efforts for harmonization by the Agency's Antifraud Central Office.

(d) How to Get a License

The requirements for authorizations are determined by the specific export controls regime, which governs the controlled products at stake. Thus, for instance, the requirements for authorizations of dual-use items are listed in Regulation (EU) 2021/821 in conjunction with Legislative Decree 221 of 2017. See Section 21.7 for a description of how to apply for dual-use and military export control licenses. Law 185/90 and enactment legislation sets forth the license requirements provided by the Italian military items export controls, while more detailed and practical guidance is provided by UAMA through its directives and guidelines (see Section 21.5).

(e) Key Websites

- UAMA: https://www.esteri.it/mae/it/ministero/struttura/uama/legislazione.html
- Ministero dell'Economia e delle Finanze: http://www.dt.mef.gov.it/it/attivita_istituzionali/prevenzione_reati_finanziari/
- Agenzia delle Dogane e dei Monopoli: https://www.adm.gov.it/portale/
- Data base made available by the Customs Agency: https://aidaonline7.adm.gov.it/nsitaricinternet/

21.2 Structure of the Laws and Regulations

(a) International Treaties

Italy participates in a number of international treaties on export controls through the European Union, and its national laws are based on such treaties.

(b) National Laws and Regulations on Export Controls

As regards national laws and regulations on export controls, please refer to Section 21.1(a)(i).

(c) Control Lists

As described earlier, Italy—as a member state of the European Union—fully implements the lists of controlled goods adopted at the European level; therefore, with the exception of the list of armaments, the lists of controlled goods adopted by Italy fully correspond to those adopted by the European Union. The Italian Military Control list includes the list adopted at EU level and could include additional items, even if as of today the Italian government has not included any additional items or categories.

(d) Italy and UN Security Council Sanctions

Since EU member states are member of the United Nations as well, all the economic sanctions adopted by the Security Council have been implemented by the European Union; therefore, Italy—both as a member of the United Nations and of the European Union—fully implements all the economic sanctions adopted by the Security Council.

(e) National Laws on Economic Sanctions

With reference to this topic, please refer to Section 21.1(a)(ii).

(f) Sanctioned Parties Lists

Individuals and entities sanctioned by the European Union shall be considered sanctioned by Italy as well: the lists of sanctioned individuals

and entities are contained in the annexes to the relevant CFSP Decisions and EU regulations concerning sanctions regimes (accessible through the website www.sanctionsmap.eu). Pending the EU implementation of the Resolutions of the UN Security Council, or the adoption of EU restrictive measures, or any intervention by the judicial authority, Article 4(a) of Legislative Decree no. 109 of 2007 grants the Ministry of Economy and Finance the power to adopt national interim measures, such as freezing the assets of persons and entities, with the aim of combating terrorism, proliferation of weapons of mass destruction and threats to international peace and security

21.3 What Is Regulated: Scope of the Regulations

With reference to the scope of the applicable regulations, please refer to Section 21.1(a).

21.4 Who Is Regulated?

Italian citizens, entities established under Italian laws and regulations, along with any natural or legal persons conducting import/export activities to/from Italy or coordinating such activities among other countries are bound by the Italian provisions concerning export control and economic sanctions.

21.5 Classification

(a) Classification of Dual-Use Items

Annex I of Regulation (EU) 2021/821 contains the list of items (including software and technology) classified as dual-use products. The latest amendment of Annex I (list of items submitted to authorization) has been adopted through Commission Delegated Regulation (EU) 2022/1 of 20 October 2021 amending Regulation (EU) 2021/821 of the European Parliament and of the Council as regards the list of dual-use items.

The control list is compulsory for Italian exporters and for the Italian licensing authority. Therefore, it does not leave room for the Italian

competent authority to exempt a controlled item listed in Annex I from regulation.

Nevertheless, if a dual-use item is not listed in Annex I, this does not necessarily mean that it does not need an export, transit, or brokering authorization. Such authorization can be required as a consequence of a "catchall" clause (see Articles 4, 5, 6, 8, and 10 of Regulation (EU) 2021/821).

The list in Annex I should be considered as exhaustive and is based on the technical characteristics of the controlled products. It lies under the responsibility of the exporter to check if the item he/she intends to export is listed in Annex I. In order to verify if an item or certain services, such as technical assistance, fall within the scope of Regulation (EU) 2021/821, it is necessary to consider the description of the controlled goods/technologies and their technical characteristics.

The software tool AIDA—*Tariffa doganale d'uso integrata* (Integrated Automation Customs Excises—Customs Tariff in use) is made available by the Italian Customs Agency at the following link: https://aidaonline7.adm.gov.it/nsitaricinternet/. Through said software, which implements the EU Commission correlation table matching Combined Nomenclature (CN) codes with dual-use codes, the licensing requirements for each shipment can be screened against the control lists. When a CN code is entered in the AIDA tool, an alert is returned where the CN code encompasses products that may trigger the applicability of dual use controls. Even if this solution is apparently quite straightforward, there are at least two major issues jeopardizing its effectiveness and leading to potential shortcomings:

1. The technical correlation between dual use products listed in Annex I of Reg. 2021/821 with their CN code is discretionary and technically questionable; and
2. Even the CN code selected by the economic operator might be wrong, further hampering the helpfulness of dual-use warnings based on the CN code.

Consequently, even if the AIDA tool may appear helpful, it should not be relied upon completely, given that when judging whether a good or component is to be considered controlled, it is necessary to assess primarily the technical characteristics of the goods. In order to determine whether a

product is controlled, the technical characteristics of the goods must thus be compared to the descriptions appearing on the lists of dual-use goods, which is contained in Annex I of Regulation (EU) 2021/821 (the text of the Regulation can be found via https://eur-lex.europa.eu/homepage.html).

Article 8, paragraph 5, of Legislative Decree 221/2017 introduced the so-called *Licenza Zero* ("Zero License," already existing in other EU countries). It is a statement, which could be issued by the Italian competent authority upon a specific request from the applicant, stating that the export of a certain item is not subject to prior authorization, and thus such an item can circulate without restrictions. However, as of July 2022, such process was not yet operational. Product classification thus continues to be carried out by the exporters themselves, either relying on the company's technical capacities or resources or involving external specialized counsels.

(b) Classification of Military Items

The Italian Control List of Military Items (Ministry of Defense Decree 29 September 2021) contains a comprehensive catalog of military goods divided into categories and subcategories. However, the list does not contain detailed technical specifications, but rather broad definitions of items and technology divided by categories. Such categories and entries often refer solely to the "special design for military use" of an item as a key distinguishing element in relation to items that—conceptually—could have both military and civilian purposes. By way of example, category 10.c controls "unmanned airborne vehicles and related equipment" only if such items were "specially designed or modified for military use, as follows, and specially designed components therefor." In fact, every instance in which the military list includes any item that is not inherently military (such as guns, bombs, explosives, weaponized toxic agents, weapon systems), the military purpose of its design and specifications becomes the key distinguishing element between military and nonmilitary items.[2]

According to section 1.b and section 2 of law 185/90 the statutory definition of "military items" (it. *materiali d'armamento*) refers to both the items listed in the Annex to the EU directive 2009/43/EC (the "EU military list," which applies to intra-EU relations and transfers) and items that, according to section 2, "pursuant to their technical, manufacturing and design requirements or specifications, are to be deemed manufactured for a

prevailing military, armed forces or law enforcement forces use." Please note that the combination of this very wide definition, with the also very wide categories of military items included in the EU and Italian military items control list, make this akin to a catchall clause whose scope may prove difficult to limit.

The second paragraph of section 2 law 185/90 lists the categories in which military items shall be divided (e.g., (a) nuclear, biological and chemical weapons; (b) automatic firearms and related munitions; etc.).

The third paragraph of the provision clarifies that a national list of military items has to be drafted and updated regularly, taking into account the EU military list and complying with the categories listed in the same section of the law. As Italian legislation in its current form, national enactment administrative decrees and EU military list all derive from the "Munitions list" agreed by the states participating into the 1996 Wassenaar Arrangement, there is substantial identity between the Wassenaar, EU, and national set of categories and subcategories (in fact, the Wassenaar Munitions List is an integral part of the WA Lists of Dual-Use Goods and Technologies and the Munitions list, which cover the entire range of controlled items from dual-use items to conventional arms).

Section 2 of law 185/90 paragraph 3 states that the introduction of new military items categories and the update of the national military list, although required by EU rules, must be effected with decree of the Ministry of Defense, in agreement with the Minister of Foreign Affairs, the Minister of the Economy and Finance, and the Minister of Economic Development.

The key notion of "military items" stems from the material relationship between the requirements and specifications and the circumstance that such requirements and specifications clearly point at a "design intent" of an item for military purposes. In other words, technical specifications, requirements, and design shall objectively demonstrate that an item is intended for a prevailing military use (or prevailing use by armed forces or law enforcement agencies).

The classification of an item as a "military item" is therefore exclusively a result of the "prevailing use" for which an item is intended, designed, and subsequently manufactured. Such "prevailing use," in turn, does not depend either by a mere "use designation" by the manufacturer or by the actual utilization of an item. In other words, if a manufacturer designs a military item (an item with inherent military capabilities), the fact

that the manufacturer markets or advertises it only for civilian use cannot change the “military nature” of the item for classification purposes.

The classification of an item as a “military item” can only be the result of an objective analysis of the technical requirements and technical specifications of such item, whenever such requirements and technical specifications would not be compatible with or justified by a prevailing civilian use. Please note, however, that while such analysis is usually referred to the historical moment when the item has been designed, de-classification requires an explicit decision by export control authorities. The responsibility for making sure that an item is correctly classified for import/export purposes lies ultimately with the importer/exporter presenting the item to Italian customs for import/export. Unfortunately, no regular public consulting services on export classification matters are available from the Italian government or export controls authorities in relation to military items. Please also bear in mind that, as stated earlier, under Italian national legislation, any entity holding, manufacturing, selling, or maintaining military items in Italy needs to be specifically authorized by the Ministry of Interior—and cannot present any item to Italian customs for export or import unless it proves that it possesses such authorization.

For the reasons explained in paragraph 5.1, as the definition of military goods in the Italian Military Control List is quite broad and seldom includes technical details, relying on AIDA—which does identify certain military goods—is even less advisable.

21.6 General Prohibitions/Restrictions/Requirements

With regard to dual-use items, general prohibitions/restrictions/requirements are laid down in Regulation (EU) 2021/821. Special provisions adopted by Italy do not deviate from those EU provisions, and Italian authorities have not provided any specific interpretative guidance on the scope of those provisions. Intra-EU cross-border transfer of military items is also harmonized at the EU level (Directive 43/2009/EC and subsequent amendments), while the rules on exports outside of the EU and imports of military items remain regulated at the national level. A general prohibition proscribes the manufacturing, import, export, transit, intra-Community transfer and brokering of anti-personnel landmines, cluster munitions, biological, chemical, and nuclear

weapons, and related technology, including tools and technology specifically designed for the construction of the aforementioned weapons along with those suitable for the manipulation of man and the biosphere for military purposes. Specific prohibitions on cross-border transactions concerning military items also apply to countries at war (unless supply is required under international treaties or agreements), countries responsible for human rights violations, countries subject to international arms embargoes, or countries that have misused Italian financial aid for military purposes.

The main requirement for entities wishing to engage in cross-border transactions of military items from Italy is registration in the National Register of Undertakings (NRU). Furthermore, export, transit, and brokering are allowed only if they involve foreign governments or undertakings duly authorized by the destination country government. More details are included in Section 21.7.

21.7 Licensing/Reasons for Control

(a) Types of Export Control Licenses and Permits for Dual-Use Items

Italian authorities license exports in keeping with the EU requirements concerning individual and global export authorizations, and Union General Export Authorizations. A national general export authorization is also available in Italy.

In particular, Legislative Decree 221/2017 sets out four types of authorizations that can be issued with regard to different categories of items: dual-use products; “not listed” dual-use items; goods subject to Regulation (EU) 2019/125 of the European Parliament and of the Council of 16 January 2019 concerning trade in certain goods that could be used for capital punishment, torture, or other cruel, inhuman, or degrading treatment or punishment (the Anti-torture Regulation); or items listed as a result of EU restrictive measures against certain third countries, adopted in accordance with Article 215 TFUE:

- **Specific individual export authorization.** Issued to a single exporter, broker, or provider of technical assistance. It applies to one

or more products for a specific end user. The authorization is valid from six months to two years, but the recipient may request an extension at least 30 days before its expiry. The extension may be issued only once.

- **Global individual authorization.** Addressed to one specific and "not occasional" exporter (i.e., it has already been granted with other similar authorizations for dual-use items or other items subject to the Decree); it lasts for a maximum of two years, is suitable to be extended upon request, and it applies exclusively for the products and countries mentioned thereto.
- **Union general export authorization (UGEA).** This authorization is limited to the items, the purposes, and the countries of destination specified by EU dual-use and Anti-torture Regulations.
- **National general export authorization.** Applicable to certain categories of transactions involving dual-use items, and to certain destination countries, both previously determined by the competent authorities.

(b) Export Control Licensing Procedure

As of 1 January 2020, all applications for authorizations concerning the export, transfer, brokerage, technical assistance, and transit of dual use items must be addressed to the Dual Use Materials Division of the National Authority (UAMA). UAMA issues the authorizations for the export, transfer, brokering, technical assistance, and transit of dual-use items; it also issues the authorizations for the trade of goods subject to the Anti-torture Regulation and the authorizations for direct and indirect trade of items listed as a result of EU restrictive measures against certain third countries.

The procedure for the issuance of individual licenses is provided by Article 10, Legislative Decree 221/2017.

As of July 1, 2022, the application to UAMA for licenses (see instructions and templates available via www.esteri.it/mae/it/ministero/struttura/uama/legislazione.html) must be submitted through an e-licensing platform. The e-licensing platform was developed by the European Commission's Directorate-General for Trade with the aim of adopting an identical structure within the European Union, enabling uniform and transparent procedures and the exchange of

information and data between member states and, where necessary, with partner countries.

In order to access the platform, each exporter must have its own “ECAS Identity,” also known as an “EU Login.” This is the digital identity of every citizen of the European Union and is required for access to any EU digital program. Through the digital platform, exporters can submit the applications and the necessary documents, monitor progress, and receive responses from UAMA.

The application to UAMA for individual licenses include, inter alia, a filled-in license application form, with a brief but detailed description of the restricted goods; the applicant’s constituent documents; and a written declaration concerning the end use of the goods (end-user statement).

The exporter is responsible for the quality of the data and information submitted in the application and in any attachment. If it is incomplete or erroneously completed, the applicant has the right to correct the application.

The end-user statement must specifically state, among other things, the following information:

- The exact name or company name of the end user, the exact indication of the registered office, and the type of activity that the end user carries out;
- A description of the exported items, including their quantity and value, and details of the relevant contract, and a copy of it;
- An indication of the specific civil use the items will be put to and their precise destination;
- A commitment not to use such items for military applications or nuclear explosives;
- A commitment not to re-export, transfer, or deviate the imported items during their transit.

The declaration must be dated, stamped, and signed by a legal representative of the end user. UAMA is also allowed to ask the exporter for an international import certificate and/or an end-use certificate, issued by the relevant administrative authority in the end user’s own country.

If necessary, UAMA can request that the exporter submit other documentation, especially in order to prove the declaration of the importer. Naturally, the operator must promptly communicate any variation that occurs after presentation of the application. Documentation required for

individual specific or global authorizations must be kept available to the competent authority for a period of not less than three years, starting from the end of the year in which the operations took place.

The competent authority has to conclude the administrative proceedings for the issuance of an authorization within 180 days from the receipt of the application. Yet, the duration of the relevant procedure can be (and often is) even shorter: the time needed to obtain an individual or global authorization is, in fact, around 30 to 60 days. Such time is extended on a few occasions, when the sensitivity of the end user, the items concerned, or the necessity to organize internal or external consultations influence the assessment of the application.

Italian authority does not request to operators a fee to apply or to issue a license.

On average, the Italian competent authority grants 1,500 to 1,800 authorizations for the export of dual-use and controlled items per year, with an overall value of 1 billion euros.

Italy is currently developing its e-licensing system.

(c) Import and Export Licenses for Military Items

While an authorization (provided by other legislation) is required to carry out manufacturing, holding, and selling of military goods within Italian borders, any cross-border transaction (import, export, intra-EU transfer, brokering, delocalization) is subject to authorization and can be carried out only by legal undertakings duly registered with the National Registry of Undertakings (RNU) maintained by the Ministry of Defense (DNA-SERNI).

A six-member Commission presided over by a Council of State Justice and including representatives from the Ministries of Foreign Affairs, Interior, Economy, Defense, and Economic Development is tasked with deliberating on new registrations and providing nonbinding opinions on cancellations and suspensions.

The registration with RNU is a prerequisite for any export and is obtained through an application process pursuant to which key individuals in the corporate structure and the undertaking itself undergo background checks. The undertaking shall be in good standing and appoint as representative for the purposes of military goods export controls a natural

person residing in Italy or in a country with whom Italy has a judicial cooperation agreement. The said representative's signature is deposited and must be used to sign all communications and authorization application concerning military goods. The registration with RNU has to be renewed every three years.

Special simplified authorization procedures apply to cross-border transactions pertaining to intergovernmental joint programs and intra-EU transfers of military goods, and to the provision of training and maintenance services.

All transactions involving end users outside the EU and/or brokering services need to undergo a two-phase authorization procedure, as both the negotiations resulting in a contractual agreement and the material execution of the transaction need to be individually authorized. Please note that no agreement, PO, or other contractual document can be signed by the parties before such an authorization is granted. If the negotiations involve classified information, a prior authorization for transfer of classified information must also be obtained.

The first phase concerns contractual negotiations concerning import, export, transit, brokering, and manufacturing delocalization of military goods, which must be notified prior to their commencement to the Ministries of Foreign Affairs and Defense. The Ministry of Foreign Affairs can prohibit the negotiations within 60 days of notification or merely dictate conditions and limitations. If the foreign counterparty and end user are from an EU or NATO country, the negotiations have to be communicated only to the Ministry of Defense, which can only set conditions or limitations within 30 days. If no prohibition or condition is communicated within the indicated deadlines, the negotiations can continue.

A mere nihil obstat (*nulla osta*)[3] by the Ministry of Defense is required for negotiations of import-export operations concerning the following:

- Spare parts and services pertaining to already authorized transactions falling out of the scope of such authorizations;
- Temporary re-import or re-export of regularly exported goods for repair and maintenance reasons;
- Imported or exported materials that need to be returned to manufacturers for faults;
- Equipment necessary for testing of regularly exported goods;

- Military goods to be displayed temporarily at trade fairs and military shows and used for technical demonstrations.

The communications and nihil obstat applications shall identify the foreign counterparty, the exact number and category of military goods affected—which shall be maintained throughout the two-stage authorization process—and provide additional information about the transaction.

Intra-EU transfers are no longer subject to the negotiation authorization requirement, since 2012, and application for the transfer can be directly submitted once negotiations have been carried out.

Once the negotiations are concluded and the parties have entered into a binding agreement (which could be conditional upon the issue of a final license to execute the transaction), the second phase concerns the license for the actual import, export, transit, brokering—arranging cross-border transactions concerning military items between countries other than Italy—and manufacturing delocalization, that is, moving production facilities outside Italian borders.

In the event of an intra-EU transfer of military goods, or of brokering services concerning an intra-EU transfer of military goods, the authorization could be general (see Chapter 8), global, or individual.

Imports from EU countries are not subject to prior authorization.

If no applicable general authorization exists, the authorization for intra-EU transactions can be global, covering specific military goods without quantity or value limitations to end users in EU member states, or individuals, covering specific quantities and values of military goods for specific end users. The application process is virtually identical to the process described later in the chapter in relation to extra-EU transactions (the application package does not need to include any copy of authorization or nihil obstat to negotiations as it is no longer required for intra-EU transfers).

In the event of a transaction involving an import from outside the EU customs territory or an export to an end user outside the EU customs territory, brokering services, delocalization manufacturing outside the EU, an application for an individual authorization must be submitted to the Ministry of Foreign Affairs (UAMA). It must be signed by the legal representative of the applicant, include an application form provided by UAMA, and include the following attachments:

- A copy of the contract;
- A copy of the authorization or nihil obstat to the negotiations;
- In the event of export licenses, an end-user certificate issued by the government of the end-user country stating that the goods are imported for use by the importing country and that they will not be re-exported without the prior consent of the Italian competent authorities. Such certificate shall be legalized and countersigned by Italian consular authorities in the end-user country.

Information on compensations paid to intermediaries, potential offset measures, and financial obligations undertaken by national administrations must also be reported in the application form.

The application and all documents attached to the application must be in Italian or accompanied by a certified sworn translation into Italian. Filing can be done electronically through certified email (PEC).

For all authorization applications, an administrative fee is levied, relating to the costs incurred by UAMA for the processing of the application (currently amounting to a few hundred euros).

Authorizations are issued within a 60-day statutory deadline (the actual time required on average is about 30 days for authorization concerning actual import and export, but may take the full 60 days to obtain the authorization to negotiate) and take the form of individual licenses, covering the materials and the end user specifically identified for the duration of time listed on the authorization. If the transaction is part of a joint program for R&D, manufacturing of military goods with undertakings from other EU or NATO members, a broader global project license may be issued covering all foreseen transactions by the same economic operator within the program framework.

The advice of the Advisory Committee is not mandatory if the operation concerns a EU or NATO member, but is almost always nonetheless required by UAMA.

Once the authorization is issued, it is communicated directly to the Customs Agency and the operation can usually be carried out within 10 to 15 days. Authorization denials can be challenged before Italian administrative courts within 60 days of formal notice of the denial, even though the judicial annulment of such denials is extremely rare.

Authorized exports can be split into multiple shipments within the quantities and the timeframe indicated in the authorization.

The execution, even if incomplete, of authorized transactions concerning exports, brokering, transit, and intangible transfers must be notified within 20 days to UAMA. The completion of export and transit-authorized transactions must be notified to UAMA within 180 days, along with a copy of transport and/or customs documents attesting such completion.

UAMA has inspection powers including access to premises by designated inspectors and analysis of documents of all undertakings operating under the Italian NRU. Please note that such inspection powers cannot be deemed to be limited in any way by any foreign piece of legislation, which—according to EU and Italian legal principles—cannot supersede national legislation. Cooperation programs in force between UAMA and extra-EU export controls authorities (such as the U.S. Bureau of Industry and Security) may allow some degree of reconciliation between Italian and foreign export controls requirements concerning military goods, but such arrangements do not amount to any acknowledgment of effectiveness of foreign export control rules inside the Italian borders.

All banking transactions related to activities authorized under law 185/1990 must be communicated within 30 days by the relevant banking institution to the Ministry of Economy. The undertaking requesting or benefiting from the banking transaction shall provide all the necessary information to the bank.

(d) Export Permits and Independent Expert Examination

With reference to the dual-use licensing procedure, the National Authority (UAMA) relies on an Inter-Ministerial Advisory Committee, which is called upon to give mandatory, but not binding, opinions on the issuance of export authorizations in accordance with Article 5 of Legislative Decree 221/2017. In addition to the Ministry for Foreign Affairs and International Cooperation and the Customs and Monopolies Agency, the following Italian ministries are represented in this Committee: Interior, Defense, Economy and Finance, Economic Development, Cultural Heritage, Health. The Head of the Dual-Use Materials Division shall act as Secretary.

The Inter-Ministerial Advisory Committee (*Comitato Consultivo*) usually meets once per month. Meeting of the Committee are attended by

technical experts in the field of dual use export control, who do not have voting rights.

At present, there are no independent test laboratories accredited with the National Authority in Italy that can confirm to exporters whether or not products require an export control license.

21.8 General Licenses/License Exceptions

(a) General Licenses

The Union General Export Authorization (UGEA) is granted directly at the EU level. No complementary national authorization is necessary.

Notification and registration requirements have been implemented by Italy in line with EU legislation. In particular, a registration is made when an exporter notifies the National Authority of his/her intention to use an UGEA, prior to the first use.

An exporter shall apply to the National Authority to obtain the right to use the UGEA through the e-licensing platform. The National Authority then checks whether the applicant complies with the requirements for the UGEA and will reply confirming the applicant's registration number, usually within ten working days. Such registration is unlimited.

As for reporting requirements applied by Italy, within 30 days from the end of each calendar semester, the exporter shall send to the competent authority a list of the export transactions made under the regime of the UGEA. Such a notice shall contain the following information: entries of invoice and contract; quantity and value of the items; categories and sub-categories of reference; corresponding customs tariff section; country of destination; particulars of the consignee and of the end-user; dispatch date; and type of export (final, temporary, transit).

Pursuant to the Decree of 4 August 2003 published in the Official Journal No. 202 of 1 September 2003, a National General Export Authorization applies for export of certain dual-use items to the following destinations: Antarctica (Italian bases), Argentina, Republic of Korea, Turkey.

The total of Italian companies registered to use GEA (national or UGEA) until 31 December 2018 was, cumulatively, 439. Italian companies using National General Export Authorizations on the same date were 153.

UAMA is empowered to publish general intra-EU transfer authorizations covering intra-EU transactions. If the intra-EU transaction falls under a general authorization published by UAMA, the relevant undertaking registered with the NRU can submit a declaration that it is availing itself of the existing General Transfer Authorization (AGT) in relation to specific countries and/or end users, specific intergovernmental joint development programs, and specific military goods.

Since 2014, UAMA has published six AGTs: AGT 1 applies to all transfers for armed forces of EU member states and to all nonclassified military goods related to a list of intergovernmental programs; AGT 2 covers transfers to EU-certified undertakings[4] in connection with specific intergovernmental programs; AGT 3 concerns specific military items repair and maintenance; AGT 4 applies to selected categories of military items and covers transfers to EU certified undertakings; AGT 5 applies to transfers for armed forces of EU/EES member states, and to all nonclassified military items; and AGT 6 concerns transfers necessary for participating in fairs and exhibitions. Such AGTs do not cover intangible transfers of technology or software.

The declaration is due only once, 30 days prior to the first use of the AGT, and shall be made in accordance with forms attached to the published AGT. Such forms include details of the applicant, details of the end user and categories of materials to be transferred, and must be signed by the legal representative of the declaring undertaking. All further transactions carried out under an AGT do not require additional declarations, but must be duly registered in a logbook by the undertaking. The logbook shall be kept for five years and be exhibited to UAMA for inspection upon request.

(b) License Exceptions

With regard to the export of dual-use items, license exceptions are laid down in Regulation (EU) 2021/821. Special provisions adopted by Italy do not deviate from those EU provisions, and Italian authorities have not provided any specific interpretative guidance on the scope of those provisions. Exceptions for military items are very rare and are listed in Law 185/90. Among the more significant, imports of components (pursuant to section 2.4 of the Law) and import of technical data if carried out with digital means are not subject to a license (while exports carried out by

digital means are subject to a license: see paragraph 11.3), but the imported items and data are still subject to a license if re-exported and remain classified as military items for all purposes.

21.9 Penalties, Enforcement, and Voluntary Disclosures

(a) Administrative and Criminal Penalties

Focusing on dual-use and not listed items transactions, and transactions involving items covered by the Anti-torture Regulation or listed under EU restrictive measures, Legislative Decree 221/2017 establishes the sanctions applicable to infringements of the relevant rules.

Different sanctions apply, depending on the type of item exported (dual-use items and not listed items, goods regulated under the Anti-torture Regulation, and listed items as an effect of restrictive measures under Article 215 TFUE).

Pursuant to Article 11 of Royal Legislative Decree no. 1923/1926, anyone who exports goods whose export is prohibited and is not covered by specific national legislation is punished with:

- An administrative fine from 413 to 2,478 euros per violation, and
- Confiscation of the goods in question.

The offences relating to the breach of the obligations related to dual use items are detailed in Article 18 of Legislative Decree 221/2017. Anyone who carries out export transactions, intangible transmission of dual-use and not listed items, as well as brokering services carried out without a preventive authorization or with one obtained through false declarations and documents, may be punished with either:

- Imprisonment from two years to six years, or
- A fine from 25,000 to 250,000 euros.

Where transactions and services of restricted items are carried out in breach of the terms of an existing authorization, the punishment is either:

- Imprisonment from two years to four years, or
- An administrative fine from 15,000 to 150,000 euros.

Mandatory confiscation applies to the items used or aimed at committing the offense, and the person whose goods are confiscated is also obliged to pay the lease of the warehouse where the goods have been stored during the seizure. When the preceding measure is not possible, a confiscation can be ordered on other goods of the offender for a value corresponding to the price or profit of the offense. Similar sanctions apply in the case of a breach of the provisions applying to items listed under the Anti-torture Regulation.

For export violations regarding items listed under EU restrictive measures, Article 20 of Legislative Decree 221/2017 sets the following penalties:

- Export transactions, brokering, or technical assistance services of products listed under EU restrictive measures, in breach of the prohibitions set forth thereto, are punished with the sanction of imprisonment from two to six years.
- The transactions and services made without a preventive authorization or on the basis of an authorization obtained through false declarations or documents are sanctioned with imprisonment from two to six years or with a fine from 25,000 to 250,000 euros.

Mandatory confiscation also applies to offenses concerning products listed under EU restrictive measures.

The main administrative offences relating to the breach of financial sanctions are detailed in Legislative Decree no. 109/2007. The regime is enforced by the Ministry for the Economy and Finance, which is responsible for applying sanctions. In particular, the following breaches of financial sanctions are punished with an administrative fine between 5,000 and 500,000 euros, pursuant to Article 13 of Legislative Decree no. 109/2007, as well as with confiscation of the goods:

- Transfer, provision, or use of frozen funds;
- Transfer, handling, or use of frozen economic resources to obtain funds, goods, or services in any manner;
- Making available funds and economic resources, directly or indirectly, to or on behalf of designated persons or entities; and
- Deliberate participation in activities directly or indirectly aimed at circumventing freezing measures.

The procedure is regulated by the Consolidated Law on Foreign Exchange (*Testo Unico in materia valutaria*) pursuant to the Decree of the President of the Republic no. 148 of 31 March 1988 and subsequent amendments.

Crimes concerning the illicit exportation of goods (see, for instance, cultural goods or dual use items) can be accompanied by the crime referred to in Article 483 of the Italian Criminal Code (ideological falsity committed by a private party in a public act), which is punished with imprisonment up to two years.

Furthermore, if such crime has been committed by persons holding representative, administrative, or (*de facto*) managerial positions in the company, or by persons working under their control, provided that these persons have committed the crimes at least "also" in the interest of or for the benefit of the company, and the company cannot demonstrate to have taken adequate measures to prevent the committal of such crimes (through a model of organization, management, and control—the so-called Organizational Model), the latter might trigger the company's liability as provided for in Legislative Decree no. 231 of 8 June 2001. ("Provisions governing the administrative liability of legal entities, companies and associations also without legal status, in accordance with Article 11 of Law no. 300 dated September 29, 2000.") The relevant pecuniary fines are based on a quota system.

According to the case law of the Italian Supreme Court (see, in particular, Court of Cassation, Section III, Sentence no. 43818, 9 October 2008), the legal representative of the entity is responsible for the violations, and the delegation of tasks does not affect the responsibility of the delegating person, except under limited circumstances. The conditions that have to be met for the delegation to work as an exemption of criminal liability and listed in this case law are the following: (1) delegation must be explicit and precise; (2) the delegate person must be professionally and technically qualified; (3) delegation must be justified on the ground of the firm's organizational needs; (4) delegation must imply also a transfer of decisional power and budget management; and (5) the existence of the delegation must be judicially proved. In the same judgment, the Court clarified that a professional exporter is deemed to know the requirements laid down by all applicable laws and regulations, and that ignorance of the applicable laws cannot be invoked.

The most common defenses in relation to the criminal offences of breach of financial/trade sanctions relate to the absence of the material element of the offence (such as the relevant goods do not fall under the export prohibition) or of the *mens rea* (that is, for instance, lack of intent to breach the export prohibition).

Violations concerning export controls rules on military items carry harsher penalties. Willful submission of false information to obtain a license is punished with imprisonment from two to six years or a fine ranging from one one-tenth to three-tenths of the value of the relevant contract. Initiating or continuing negotiations without the necessary authorization is punished with imprisonment up to four years and a fine ranging from 25,822 to 258,228 euros. Carrying out a transaction without the required authorization is punished with imprisonment from three to 12 years or a fine from 25,822 to 258,228 euros. Infringement of authorization conditions and delivery requirements is punished with imprisonment up to five years or with a penalty from two-tenths to five-tenths of the value of the relevant contract. All military goods subject of illicit transaction must be confiscated. Administrative fines up to 20,000 euros apply to minor administrative infringements, and a specific administrative fine of 25,000 euros punishes the failure to communicate the financial transaction concerning military items to the Ministry of economy.

The illicit provision of technical assistance in the production, storage, or diffusion of nuclear, chemical, or biological weapons carries prison sentences from two to six years.

Enforcement cases are unfortunately not public. Prosecution and criminal cases mostly become public only when decisions arrive to the Italian Supreme Court (*Corte di Cassazione*), which happens very rarely (a handful of cases were decided over the last ten years). The two most recent decisions concern the lack of Italian jurisdiction on military supplies carried out by foreigners between foreign countries, even when reported to Italian authorities, when there is no proof that cargo at least crossed Italian territorial waters (Cass. Pen, Ist panel, 17 June 2020, n. 19762) and the criminal liability of exporters who carried out cross-border transactions concerning military items regardless of whether they were registered as military items manufacturers or potential exporters (Cass. Pen, Ist panel, 14 October 2009, n. 39992).

(b) Enforcement

Pursuant to Italian legislation, companies in breach of the obligations related to export controls and economic sanctions can be subject to criminal and/or administrative sanctions. The public prosecutors are responsible for investigating and prosecuting criminal offences. Administrative fines are imposed by the competent administrative authorities.

The administrative sanctions are governed by the general principles on administrative sanctions for decriminalized conduct, mainly arising from Law no. 689/1981, which is the main legislative reference for the entire Italian system of administrative sanctions. With regard to the principles applicable to administrative sanctions provided for in export controls and sanctions matters, it should be stressed that Article 3 of Law no. 689/1981 establishes a presumption of guilt on the accused, leaving on him or her the burden of proving the absence of guilt. It is generally possible for the infringer to waive the right of challenging the fine and pay a reduced amount within a short deadline. Pursuant to Article 13 of Law 689/1981, when a case entails an administrative fine, the competent authorities can assume information, make inspections on the places different from private homes, take samples, and seize the goods that can be the object of confiscation as provided by the Procedural Criminal Code.

Data on enforcement cases are generally not publicly available and there is a lack of case law related to violation of export controls and economic sanctions legislation. The case dealt in Court of Cassation, Section III, Sentence no. 43818, 9 October 2008 (mentioned earlier), concerned an export without authorization of 243 barrels of cyanide, which is an item listed in Annex I of Regulation (EC) No. 428/2009. In that case, the exporter was sanctioned with a fine of 18,000 euros, taking into account generic extenuating circumstances.

Legislative Decree 221/2017 provides for inspection measures that can be carried out at different stages of the transactions and may consist of a mere document review or inspections at the exporter, broker, or provider’s premises. The competent authority can request documents that prove the effective arrival of authorized items in the designated country.

(c) Voluntary Disclosures

Italian entities or individuals are not legally required to report any violation of Italian export control and sanctions laws. Furthermore, there are no penalties in Italian law for nondisclosure or failure to report. Since voluntary disclosures provide no practical advantages, Italian persons and entities tend not to make use of such programs. Furthermore, public servants are legally bound to report any conduct they become aware of that could be deemed a punishable crime. Therefore, voluntarily disclosed violations that are criminal violations would be immediately reported and give rise to prosecution.

21.10 Recent Export Enforcement Matters

While EU export controls and sanctions legislation has significantly increased over the last decade, there is still little published enforcement history. It appears that prosecution is mainly based on export controls breaches or on relevant common criminal offences (e.g., Article 483 of the Italian Criminal Code; discussed earlier in the chapter).

In 2018, two breaches were reported pursuant to Regulation (EU) no. 44/2016 concerning sanctions against Libya; one pursuant to Regulation (EC) no. 428/2009; one pursuant to Regulation EU 267/2012 for Iran. These four breaches were reported by the Italian Customs Agency. The state of the proceedings and the penalties imposed, if any, are not publicly available.

21.11 Special Topics

(a) Re-exports/Extraterritorial Application of Laws

Italy has not adopted any specific provisions relating to the re-export of controlled goods. Therefore, Italian law does not control re-exports of Italian controlled items outside Italy that are not carried out by the exporter who had committed not to re-export without the consent of Italian authorities.

In line with EU law, a commitment of the recipient of controlled items not to export or re-export such items without a prior consent of the Italian licensing authorities is included in the end-use statements/end-use

certificates required for the issuance of the export authorizations. However, such commitments remain vague and hardly enforceable in practice.

As regards Italian law controls on deemed exports of controlled technology to non-EU citizens located in the EU, as regulated by Article 6.1 of Legislative Decree 221/2017, see Section 21.11(c).

(b) Brokering Activities Related to Unlisted Dual-Use Goods

Legislative Decree 221/2017 specifically addresses brokering activities related to listed and nonlisted dual-use goods and goods controlled under EU restrictive measures. In line with EU Law, only those brokering activities of dual-use goods that present a risk of diversion are subject to authorization, that is, when the broker has been informed by the competent national authority or is aware that the provision of brokering activities might lead to production or delivery of weapons of mass destruction in a third country.

The provisions applicable to the brokering activities of goods controlled under EU restrictive measures provide, under certain circumstances, for stricter rules (please consider, for instance, the license under Article 4(3) of Regulation (EU) 833/2014 concerning Russia, which is always required in connection with the brokering of items listed in Annex II, regardless of the risk of diversion for those items).

Article 18 of Legislative Decree 221/2017 states that any person conducting brokering activities in violation of the EU provisions on dual-use goods may be subject to incarceration from a minimum of two to a maximum of six years or, alternatively, to a monetary penalty ranging from 25,000 to 250,000 euro. A similar wording is found in Article 20, which provides for the imposition of the same penalties should the authorities find a violation of EU restrictive measures adopted pursuant to Article 215 TFEU.

Brokering activities of military items are treated as general cross border transactions; see Chapter 7.

(c) Intangible Transfer of Technical Information

Pursuant to Article 6.1 of Legislative Decree 221/2017, projects, designs, the software and technology cannot be transferred—electronically or through any other electronic means, fax, email, or telephone—outside the

territory of the European Union without prior authorization to be issued pursuant to the decree (as regards penalties subsequent to the infringement of this provision, refer to Section 21.9). Article 6 specifies that the concept of "intangible transfer," as described earlier, also includes access to servers and sharing of information. In this regard, exporters, intermediaries, and technical assistance providers who intend to perform intangible transfers are requested to adopt secure and traceable access procedures, and an access reporting system, in order to allow any checks by the competent authority. Article 6.1 of Legislative Decree 221/2017 rules that a license is required for transfers of technology to non-EU citizens *temporarily located* in the territory of the European Union.

Intangible transfers of military technology (i.e., technology or software pertaining to military goods transmitted outside national borders through fax, email, digital means) also require an export license. Please note that the current definition of intangible transfers only mentions outbound movement of data or technology originating from the Italian territory. This means that any transmission of technology and data—even a simple email in relation to a technical assistance matter—not already included in an export authorization should be authorized by UAMA. Please note that in-country transfers are not "deemed exports" but would still subject the recipient to a license requirement because, as previously stated, holding military items or technology cannot happen within Italian borders without a proper government license.

As going through the authorization procedure for each transfer would be extremely impractical, in early 2014, the Ministry of Foreign affairs adopted guidelines that provide for authorizations covering digital safe transfer systems. Repeated information digital exchanges through dedicated servers are authorized, provided that all exchanges are digitally logged and UAMA is granted the possibility of supervising the logged exchanges through a special access to the dedicated server and to the logs.

(d) Practical Issues Related to Export Control Clearance

With regard to dual-use items and the software tool AIDA (discussed earlier), when the Combined Nomenclature (CN) code chosen by the Italian exporter shows a correlation with a dual-use item according to the mentioned correlation system, it must be indicated whether the items to be

exported are subject to export control or not by inserting special codes in the Single Administrative Document (SAD; i.e., the EU Customs declaration) box 44, as follows:

- Code Y901—items not controlled
- Code X002 (along with license details)—items controlled

This is a mutually exclusive system, *tertium non datur*. Either the product is not controlled, or the product is controlled and a license has been duly obtained by the exporter. Hence, controlled items cannot be exported without a proper license.

(e) Recordkeeping

Pursuant to Legislative Decree 221/2017, exporters of dual-use items shall keep detailed registers or records of their exports for at least three years from the end of the calendar year in which the export took place or the brokering service was provided. They shall be produced, on request, to the competent authorities.

Specific provisions concerning export transactions of military items require that all documents pertaining to a transaction be kept for at least five years from the completion of the transaction (i.e., the delivery of the items/technology to their intended final destination). Such documents have to be produced, on request, to the competent authorities.

Taking into account the recordkeeping requirements deriving from other applicable pieces of legislation, including anti-money laundering and tax law, the documentation that is relevant under export control and sanctions laws and regulations is normally kept by exporters (on paper or by electronic means) for a period of ten years.

(f) Bank of Italy—Enhanced Due Diligence

The EU legal framework on international economic sanctions interacts with certain Anti Money Laundering and Countering Financing of Terrorism provisions (AML/CFT) in Italy. More specifically, Legislative Decree 231/2007 (consolidated AML Law in Italy, implementing the EU framework), as amended, identifies a number of high-risk factors that the regulated financial entities (e.g., banks, investments firms, insurance companies, etc.) must take into account for the purpose of adopting

enhanced customer due diligence measures. Among the risk factors listed thereof, two of them create a direct link between AML laws and EU sanctions regulations (i.e., EU restrictive measures). The first risk factor is found in Article 24.2(c)(3) of the AML Law, which refers to "third countries subject to embargoes or similar restrictive measures" and the second in Article 24.2(c)(4), which refers to "countries supporting or sponsoring terrorism or in which terrorist organizations operate."

Article 24 of the AML Law was implemented in 2019 with the enactment of the Bank of Italy's Rules on Customer Due Diligence for Countering Anti Money Laundering and Financing of Terrorism (30 July 2019) (the "Rules"), in force since 1 January 2020 and applicable to all entities regulated by the Bank of Italy.

The Rules require financial institutions to take a risk-based approach to AML compliance. This risk-based principle, enshrined in Part I, Section I of the Rules, mandates that the regulated financial entities calibrate the degree of thoroughness of their AML/CFT controls in light of the specific risk factors detected in specific transactions on a case-by-case basis. Hence, the involvement in a specific transaction of a connection with "third countries subject to embargoes or similar restrictive measures" or "countries supporting or sponsoring terrorism or in which terrorist organizations operate" triggers an obligation for the financial institutions to implement enhanced customer due diligence measures (as further detailed in the Rules) and therefore to acquire further and more detailed information regarding the transactions under scrutiny.

The expression "embargo or similar restrictive measures" must be strictly interpreted as a reference to restrictive measures adopted by the EU (and the UN) and not to sanctions programs adopted by other jurisdictions (USA, UK, etc.). The term "embargo," in EU Law, does not bear the same meaning assigned in other legal systems (i.e., a comprehensive sanctions program toward a certain country), as it only refers to specific restrictive measures regarding arms traffic (i.e., an arms embargo).

In contrast to risk-based discretion conferred by the AML provisions, regulated entities are also subject to mandatory law provisions, such as the ones imposing to freeze funds and assets belonging to EU-listed entities or individuals (see Legislative Decree 109/2007). Such obligations, as already mentioned, are imposed by several EU regulations, which in many cases have implemented Resolution of the UN Security Council.

Although the objectives of AML laws were originally limited to prevent illicit funds to be "laundered" through the financial system, since the beginning of the 2000s, various legislative measures have been taken to incorporate the fight against global terrorism within AML framework. Countering Financing of Terrorisms, however, does not share identical goals with AML, nor with international economic sanctions law (which purposes go well beyond the fight against terrorism and are used as a foreign policy instrument). Despite this misalignment, Italian law requires financial intermediaries to apply AML due diligence measures also in cases where there is a connection with sanctioned countries, therefore further expanding the scope of AML measures to transactions that might violate EU restrictive measures.

(g) ICP

The Italian legal framework does not deviate from the discipline set out in the EU Commission's recommendation (EU) 2019/1318 on internal compliance programs (ICPs) for dual-use trade controls under Council Regulation (EC) 428/2009. Exporters using a global export authorization or certain general authorizations must implement an internal compliance program (ICP) and submit it to UAMA for its scrutiny.

21.12 Encryption Controls

There are no Italian import/export restrictions/trade control specific requirements applying to cryptology-related items and deviating from EU rules. Therefore, encryption items are subject to the standard EU export controls, but there are no additional license or other requirements imposed on the import or use of encryption items within Italy.

21.13 Blocking Laws/Penalties for Compliance with Sanctions Imposed By Other Countries

There are no legal instruments currently in force in Italy, other than the EU Blocking Statute, prohibiting compliance with extraterritorial provision of foreign sanctions programs. Pursuant to Article 9 of EU Regulation (EC) 2271/96 (EU Blocking Statute), however, Italy has enacted Legislative

Decree 346/1998, setting out the national legal framework for sanctions applicable in connection to the violation of the relevant provision of the EU Blocking Statute. More specifically, Article 1 of the Legislative Decree provides for the imposition of monetary penalties for violations of Article 2 and Article 5.1 of the Blocking Statute.

It must be remembered that Article 2 of the Regulation provides that

> Where the economic and/or financial interests of any person referred to in Article 11 are affected, directly or indirectly, by the laws specified in the Annex or by actions based thereon or resulting therefrom, that person shall inform the Commission accordingly within 30 days from the date on which it obtained such information; insofar as the interests of a legal person are affected, this obligation applies to the directors, managers and other persons with management responsibilities.

Hence, any EU natural and legal person (as listed in Article 11) who might be negatively affected by the extraterritorial laws listed in the Annex to the Regulation has a duty to inform the EU Commission. According to Article 1.1 of the Legislative Decree, failure to comply with such communication obligation is punished with a monetary penalty between 7,746.85 and 92,962.16 euro.

According to Article 1.2 of the Legislative Decree, failure to comply with the prohibition of Article 5.1 of the Blocking Statute (as described in the relevant chapter) is punished with a monetary penalty between a minimum of 15,493.69 euro and a maximum of 92,962.16 euro.

Following the transfer of prerogatives from the Ministry of Economic Development (MISE) to the Ministry of Foreign Affairs (MAECI) regarding the implementation of the EU restrictive measures, it is expected that Legislative Decree will be amended to transfer the authority to enforce the Blocking Statute to the MAECI.

---

1. Marco Zinzani (Studio Legale Padovan); Simone Cadeddu (Bird&Bird).
2. This is the case for “Ground vehicles” (Category 6); “vessels” (Category 9); “aircraft,” “lighter than air vehicles,” and “aero-engines” (Category 10); “Electronic equipment” (Category 11); “Cryogenic and superconductive equipment” (Category 20); and “Software” (Category 21).
3. From Latin “nothing hinders,” “nothing stands in the way,” is a kind of simpler authorization by which a government body states it has no objection to a certain private conduct.
4. Certified undertakings are undertakings that have adopted internal measures, such as creating a direct datalink accessible by UAMA and hiring of a military goods export compliance specialist, that ensure their higher reliability to comply with the relevant export controls regimes.

22

Export Controls and Economic Sanctions in Japan

Fumiko Oikawa

22.1 Overview

(a) What Is Regulated?

Export controls in Japan are based on treaties in which leading industrial nations participate and play a central role, such as the Chemical Weapons Convention and international export control agreements (international export control regimes). Japan implements the minimum controls necessary for Japan's national security and the maintenance of international peace and security on the export of materials and equipment related to the development and manufacturing of weapons of mass destruction (WMD), conventional weapons, and related general-purpose goods, as well as the provision of related technology to nonresidents.

(b) Where to Find the Regulations

Japanese laws and regulations are available on the official legal information website at:

- Japanese language: https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0100/
- English language: www.japaneselawtranslation.go.jp/?re=02

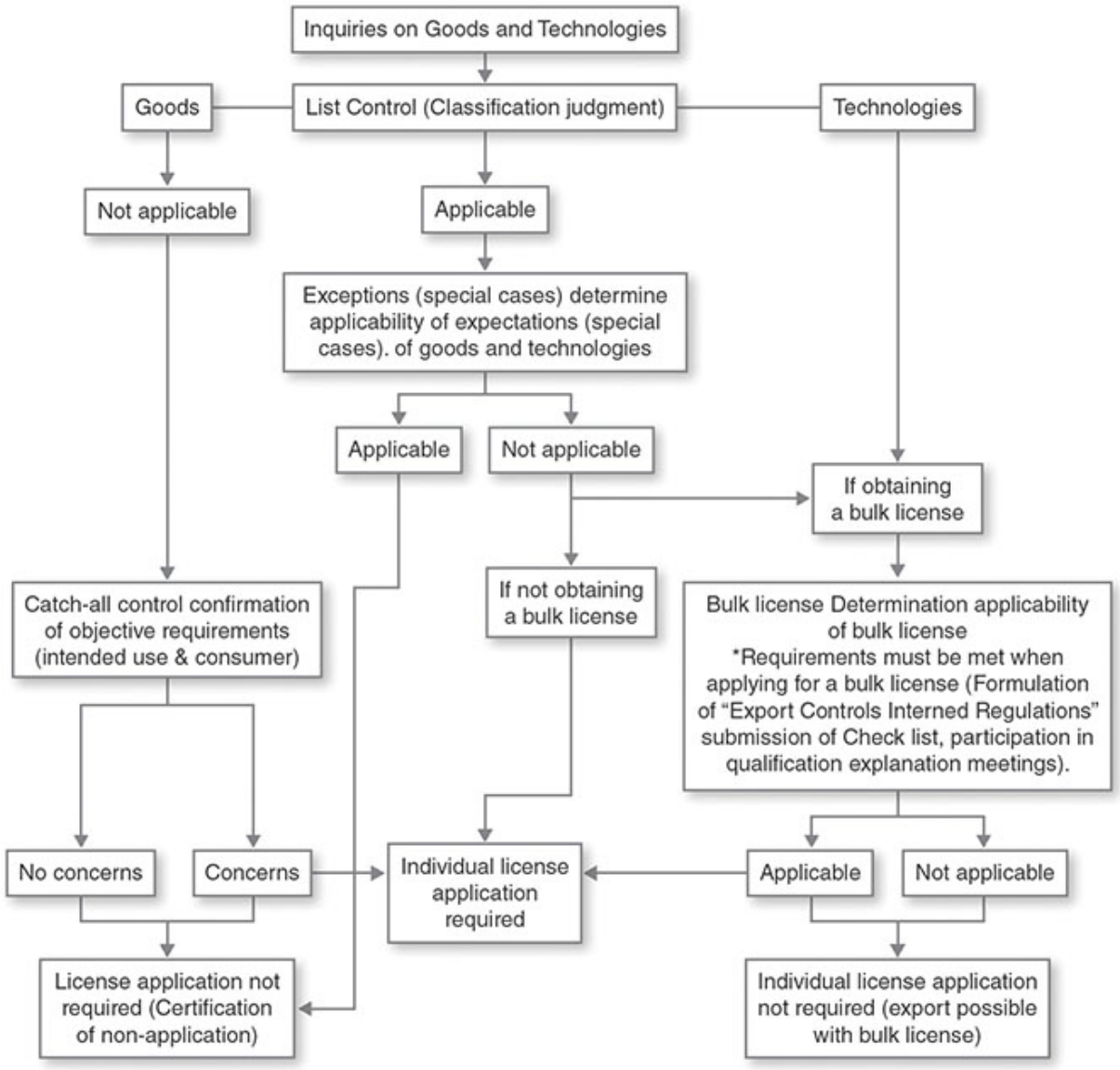
Japanese export control regulations are on the website of the Ministry of Economy, Trade and Industry (METI), the main governmental body responsible for export controls at: https://www.meti.go.jp/policy/anpo/law00.html.

(c) Who Is the Regulator?

The main regulator is METI.

(d) When and How to Get a License

The decision as to whether or not to apply for an export license and the application procedure are shown in the following flow chart.



*Note: When applying the small amount exception, it is necessary to confirm whether or not objective requirements are satisfied. confirmed.

Created by editing the flowchart of export license application procedure (METI) (https://www.meti.go.jp/policy/anpo/apply01.html)

(e) Key Websites

- Ministry of Economy Trade and Industry (METI), Security Export Control: https://www.meti.go.jp/policy/anpo/index.html
- Center for Information on Security Trade Control (CISTEC): https://www.cistec.or.jp/export/index.html

- Japan External Trade Organization (JETRO): https://www.jetro.go.jp/world/japan/qa/

22.2 Structure of the Laws and Regulations

(a) International Treaties

As mentioned earlier, Japan participates in a number of international treaties on export controls, and its national regulations are based on those treaties. In particular, Japan participates in the following international treaties:

Regulation of nuclear, biological, and chemical weapons

- Treaty on the Non-Proliferation of Nuclear Weapons (NPT)
- Biological Weapons Convention (BWC)
- Chemical Weapons Convention (CWC)

Trade controls on general-purpose goods used for the development of conventional weapons and WMD:

- Nuclear Suppliers Group (NSG)
- Australia Group (AG)
- Missile Technology Control Regime (MTCR)
- Wassenaar Arrangement (WA)
- Zangger Committee (ZC) (a group that is not legally binding)

Major government-level understandings and agreements, on security export controls:

- United Nations Security Council Resolution 1540 (April 2004) (withholding support to nonstate actors attempting to develop weapons of mass destruction and implementation of effective measures to establish internal controls, of materials, related to weapons of mass destruction)
- G8 Summit (Sea Island) (June 2004) “G8 Action Plan on Non-Proliferation”
- Global partnership against WMD and their supply (measures on the issue of nuclear nonproliferation by North Korea and Iran)
- G8 Summit (Gleneagles) (July 2005) “G8 Summit Statement on Non-Proliferation”: Universalization and promotion of the

nonproliferation system, 2005 NPT Review Conference
- G8 Summit (St. Petersburg) (July 2006) “G8 Summit Statement on Non-Proliferation” (measures on the issue of nuclear nonproliferation by North Korea and Iran)

(b) Japanese National Laws and Regulations on Export Controls

Export controls in Japan are implemented under the following laws.

- Foreign Exchange and Foreign Trade Act (FEFTA), Articles 48, Article 25: https://www.japaneselawtranslation.go.jp/en/laws/view/3700/en
- Export Trade Control Order (ETCO), Appended Table 1: https://www.japaneselawtranslation.go.jp/ja/laws/view/3389
- Foreign Exchange Order (FEO), Appended Table: https://www.japaneselawtranslation.go.jp/en/laws/view/4102
- Ministerial Order Specifying Goods and Technologies Pursuant to the Provisions of the Appended Table 1 of the ETCO and the Appended Table of the FEO (MOSG): https://www.japaneselawtranslation.go.jp/en/laws/view/2851
- Operation of the ETCO (Notification): https://www.meti.go.jp/policy/anpo/law_document/tutatu/26fy/unyou_tsutatsu.pdf
- Transactions or Acts to Provide Technologies requiring Licenses under the provisions of Foreign Exchange and Foreign Trade Act, Article 25, paragraph 1 and FEO Article 17, paragraph 2 (Notification): https://www.meti.go.jp/policy/anpo/law_document/tutatu/t10kaisei/ekimu_tutatu140814.pdf

(c) Controlled Lists

The security-restricted export controlled goods and technologies in Japan are set out in the following tables:

- ETCO, Appended Table 1: https://www.japaneselawtranslation.go.jp/en/laws/view/3389

- FEO, Appended Table: https://www.japaneselawtranslation.go.jp/en/laws/view/4102
- In addition, a list of goods that require an application for export approval is set out in ETCO, Appended Table 2: https://www.japaneselawtranslation.go.jp/en/laws/view/3389

(d) Japan and UN Security Council Sanctions

Japan may impose necessary economic sanctions if a matter, whether in or out of Japan, is (1) subject to sanctions imposed by the Security Council; (2) the Minister of Economy, Trade and Industry ("Minister") and the Minister of Finance "find it necessary to fulfil international obligations in good faith" or "find it necessary as part of Japan's contribution to international efforts to achieve international peace"; or (3) if "the Cabinet specifically decides to take countermeasures necessary to maintain peace and security in Japan."

As of December 2, 2022, economic sanctions, including measures such as asset freezing, are being taken against the following organizations and senior officials:

- The previous Iraqi administration or their related parties;
- Taliban-related parties and terrorists;
- Persons who have violated arms embargoes, against the Democratic Republic of the Congo (DRC);
- Persons hindering the Darfur peace-keeping force in Sudan;
- Persons involved in North Korea's missile or WMD programs;
- Persons subject to asset freezing and other measures based on United Nations Security Council resolutions related to North Korea;
- Payments to individuals, etc., with addresses, etc., in North Korea;
- Persons who have violated the arms embargo against Somalia;
- Leaders of the Libyan Gaddafi Revolution and related persons;
- Syrian President Al Assad and related persons;
- Persons who are directly involved in the Crimean "annexation" or destabilization of Eastern Ukraine;
- Organizations and individuals in the Russian Federation subject to asset freeze and other measures;
- Certain banks, etc., the government, and government agencies of the Russian Federation subject to prohibition on issuance or offering of

securities;
- Organizations and individuals in the Republic of Belarus subject to asset freezing and other measures;
- Persons involved in acts that threaten peace in the Central African Republic;
- Persons involved in acts that threaten peace in the Republic of Yemen;
- Persons involved in acts that threaten peace in South Sudan;
- Persons involved in Iran's nuclear activities
- Persons involved in acts that threaten peace in the Republic of Mali; and
- Persons involved in acts that threaten peace in Haiti.

(e) Japanese National Laws on Economic Sanctions

FEFTA Article 10 provides that "If it is particularly necessary to do so in order to maintain peace and security in Japan, it may be decided, in a cabinet meeting, that responsive measures will be taken," and trade regulations, remittance regulations, service provision regulations, and capital transaction regulations may be taken.

In addition, if it is particularly necessary to do so in order to maintain peace and security in Japan, it may be decided, in a cabinet meeting, that the entry into a port of Japan of a vessel or aircraft of a specified foreign nationality shall be prohibited in accordance with the Act on Special Measures concerning Prohibition on Entry of Specified Ships into Ports.

(f) Japanese Sanctioned Parties Lists

The Ministry of Finance maintains a list of sanctioned parties designated under the FEFTA, which can be found at: https://www.mof.go.jp/policy/international_policy/gaitame_kawase/gaitame/economic_sanctions/list.html

22.3 What Is Regulated: Scope of the Regulations

Japan's security export control regime is based on treaties and international agreements on international export control. Japan has two main licensing

regimes for the export of goods or the transfer of technology, both of which require a license from the Minister:

1. The “List Control” for the export of goods or technology with certain specifications or functions, such as carbon fiber or numerically controlled machine tools, and
2. The “Catchall Control” for the export of goods or technology that do not fall under the List Control, and if certain requirements are met (“informed requirements” or “objective requirements”).

In addition, Japan has intermediary trade rules that require a license from the Minister for transactions related to buying and selling, leasing, or gifting, which involves the movement of goods between foreign states.

Japan’s security export control laws includes the concept of deemed exports which controls transactions intended to provide certain sensitive technologies to nonresidents in Japan, and requires prior permits from METI (FEFTA, Article 25, paragraph 1).

22.4 Who Is Regulated?

(a) Export of Goods

Anyone who intends to export certain kinds of goods to certain regions that would compromise the maintenance of world peace and international security as specified by a Cabinet Order is subject to regulation (FEFTA, Article 48, paragraph 1).

“Certain regions” and “certain kinds of goods” are listed in the Appended Table 1 of ETCO (https://www.japaneselawtranslation.go.jp/en/laws/view/3389).

(b) Provision of Technology

A resident or a nonresident who intends to conduct a transaction with the objective of providing technology that is associated with the design, manufacture, or use of a specific kind of good as being found to compromise world peace and international security in a specified foreign state, is subject to regulations (FEFTA, Article 25, paragraph 1).

The Appended Table of the FEO (https://www.japaneselawtranslation.go.jp/en/laws/view/4102) states what constitutes "technology that is associated with the design, manufacture or use of a specific kind of good" and "specified foreign state."

The term "resident" means a natural person with a domicile or residence in Japan or a corporation with a principal office in Japan. Further, regardless of whether the Japanese branch office, local office, or other office of a nonresident has the legal authority to represent that nonresident, it is deemed to be a resident even if its principal office is located in a foreign state (FEFTA, Article 6, paragraph 1, item (v)).

The term "nonresident" means a natural person or corporation other than a "resident" (FEFTA, Article 6, paragraph 1, item (vi)); a person can therefore be in Japan but still be a nonresident and technology can be transferred to such a person but not constitute an "export."

(c) Intermediary Trade Transactions of Goods

A resident who intends to conduct a transaction related with nonresidents concerning buying and selling, leasing, or gifting that involves the movement of goods between foreign states that would compromise the maintenance of world peace and international security, as specified by a Cabinet Order, is subject to regulation (FEFTA, Article 25, paragraph 4).

22.5 Classification

For the classification of dual-use items and military items, refer to Appended Table 1 of the ETCO (https://www.japaneselawtranslation.go.jp/en/laws/view/3389), and for the types of technology, refer to the Appended Table of the FEO (https://www.japaneselawtranslation.go.jp/en/laws/view/4102).

22.6 General Prohibitions, Restrictions, and Requirements

(a) General Prohibitions and Restrictions

As mentioned in Section 22.3, there are two types of export control under the FEFTA, List Control and Catchall Control; both require that a license be

obtained in advance from the Minister for the export of controlled goods or transfer of controlled technologies. In addition, there are intermediary trade rules that require a license be obtained in advance from the Minister for the intermediary trade transactions of goods.

(b) Requirements

(i) List Control Requirements

If goods to be exported fall under items 1 to 15 of Appended Table 1 of the ETCO (https://www.japaneselawtranslation.go.jp/en/laws/view/3389), or technologies to be provided fall under items 1 to 15 of the Appended Table 1 of the FEO (https://www.japaneselawtranslation.go.jp/en/laws/view/4102), and if the goods or technologies have the specification or functions designated by the MOSG, regardless of the use or destination, a license from the Minister is required in advance for the export of the goods or provision of the technologies.

These details are also provided in the MOSG (https://www.japaneselawtranslation.go.jp/en/laws/view/2851).

(ii) Catchall Control Requirements

If goods or technologies are not subject to the List Control regime but are likely to be used for the development, manufacture, use, or storage of WMD or conventional weapons, their export requires a prior Catchall Control license from the Minister.

The Catchall Control has two types: (1) when there is a risk of the goods or technologies being used for the development of WMDs, the "catch-all control for WMD" requires a license, and (2) when there is a risk of the goods or technologies being used for the development of conventional weapons, the "complementary export control of conventional weapons" requires a license, and both are regulated by the (i) objective requirement and (ii) informed requirement.

Under the objective requirement it is necessary to apply for a license if, based on the exporter's confirmation of use of the goods or technologies or identity of the consumer, there is a risk that the goods or technologies may be used either for the development, manufacture, use, or storage of WMD, or for the development, manufacture, or use of conventional weapons.

The “confirmation of use” specifically confirms:

- Whether the goods or technologies will be used for the development, manufacture, use, or storage of WMD or nuclear fuel material; and
- Whether the destination is a country or region listed in the Appended Table 3-2 of the ETCO (refer to the following table), and, if so, will the goods or technologies be used for the development, manufacture or use of conventional weapons.

The “confirmation of consumers” confirms, having regard to the identity of the consumer, whether or not it is likely that the goods to be exported or technologies to be provided will be used for the development of WMDs, specifically:

- Will the consumer develop, manufacture, use or store WMDs? or
- Is the consumer on the Foreign User List (https://www.meti.go.jp/policy/anpo/3_userlist_asof2020.pdf)?

Under the informed requirement, it is necessary to apply for a license if notification is received from the Minister that the exporter or technology provider should apply for a license because the goods or technologies are likely to be used for the development, manufacture, use or storage of WMDs or for the development, manufacture, or use of conventional weapons.

However, since it is considered unlikely that goods exported or technologies provided to a consumer in regions listed in Appended Table 3 of the ETCO will be used for restricted purposes, such exports or provisions are outside the scope of the Catchall Control.

The preceding rules are summarized in the following table.

		Catchall Control		
	List Control	**Weapons of Mass Destruction, etc. (April 2002)**	**Conventional Weapons (From November 2008)**	
Items Subject to Regulations	*Items Controlled by Government Ordinance* Weapons, sensitive general purpose products (nuclear power, biological	*All Items except List Control Items* (excluding food and wood, etc.)		

	weapons, chemical weapons, missile-related items, advanced materials, machine tools, etc.)			
Subject Regions	**All Regions**	**All Regions Except (A) Below**	**Countries of (B) Below**	**All Countries of (C) Except (A) and (B) Below**
Requirements	—	If there is a risk it may be used for the development, etc. of weapons of mass destruction, etc. 1. Notice from the Minister 2. Exporter's judgment: (i) use at the importer etc. (ii) involvement of importers and consumers in nuclear development, etc.	If there is a risk it may be used for the development, etc. of conventional weapons 1. Notice from the Minister 2. Exporter's judgment: (i) use at the importer etc.	If there is a risk it may be used for the development, etc. of conventional weapons 1. Notice from the Minister

(A): Countries that participate in each international export control regime and strictly implement export controls (26 countries in total): Appended Table 3, Export Trade Control Order
Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, United Kingdom, and United States of America
(B): Countries for which the export of weapons and related products, etc., is prohibited by a resolution of the United Nations Security Council (ten countries in total): Appended Table 3-2, Export Trade Control Order Afghanistan, Central Africa, Democratic Republic of the Congo, Iraq, Lebanon, Libya, North Korea, Somalia, South Sudan, Sudan
(C): All countries except those listed in (A) and (B) above
Iran, Syria, China, Russia, Ukraine, Turkey, Pakistan, Myanmar, etc.

Created by editing the table on page 6 of Security Export Guidance [Introduction] (December 2022) (METI) (https://www.meti.go.jp/policy/anpo/guidance/guidance.pdf)

(iii) Intermediary Trade Rules

With regard to transactions related to the buying and selling, leasing, or gifting that involve the movement of goods between foreign states, a license from the Minister is required in advance in the following cases (FEFTA, Article 25, paragraph 4, FEO, Article 17, paragraph 3).

- Goods falling under item 1 of Appended Table 1 of the ETCO (* All countries and regions are subject to the rules.)
- Goods falling under items 2 to 16 of Appended Table 1 of the ETCO that are likely to be used for the development and so on of WMD (* With the exception of regions listed in Appended Table 3 of the ETCO, all countries and regions are subject to the rules.)

22.7 Licensing Reasons for Control

(a) Types of Export Control Licenses and Permits for Dual-Use Items

Any goods or technologies that are convertible to military use (dual-use items) are also subject to the List Control and Catchall Control described earlier under Section 22.6. In particular, the Catchall Control applies to all items excluding List-Controlled items, food, and wood, so it is necessary to carefully judge whether or not the item falls under the Catchall Control. If any questions arise in the examination process and/or evaluation of the need for a license, it is advisable to consult METI or an external expert such as an attorney.

(b) Export Control Licensing Procedure

Please refer to the chart in Section 22.1(d).

(c) Import and Export Licenses for Military Items

(i) Import Licenses for Military Items

Under the FEFTA, the import of military items requires an approval of the Minister. Any person who intends to import machinery, weapons, or ammunition must obtain the approval of the Minister under the FEFTA. Key definitions relating to military items are set out as follows.

- Machinery includes motors and engines for military aircraft, tanks and other armored vehicles, and warships.
- Weapons include military weapons, handguns, hunting guns, target guns, air guns, swords, bayonets, daggers, and underwater guns.
- Ammunition includes bombs, grenades, and missiles.

It is necessary to obtain the prior approval of the Minister to import any item where the place of origin or place of shipment is North Korea, and the import of weapons and other goods from North Korea is prohibited (https://www.meti.go.jp/english/press/2021/0406_001.html).

(ii) Export Licenses for Military Items

Under the FEFTA, the export of military items requires a license from, or approval of, the Minister and the export of "weapons" or "high technology general-purpose products that can also be used for military purposes agreed by the international export control regime" and that are designated as List Control items requires a license from the Minister. Key definitions relating to military items are set out as follows.

- Weapons include military vehicles, military vessels, and military aircraft.
- High-technology general-purpose products include goods related to WMD, goods related to conventional weapons, and goods that are likely to be used for the development, and so on, of WMD and conventional weapons.
- Goods related to WMDs means nuclear weapons, chemical weapons, biological weapons, or missile-related goods.
- Goods related to conventional weapons means advanced material processing, electronic equipment, computers, communications equipment, sensors and/or lasers, navigation equipment, marine equipment, and propulsion equipment.

As mentioned in Section 22.6, if a good falls under the List Control and contains designated specifications or functions, or falls under the Catchall Control, it is necessary to obtain a license from the Minister prior to export.

All exports of goods destined for North Korea require the prior approval of the Minister, and the export of military items to North Korea is prohibited.

(d) Export Permits and Independent Expert Examination

The examination by the Minister of an application for an export license for military equipment will be conducted in accordance with the Three Principles on Transfer of Defense Equipment and Technology (the "Principles") approved by the Japanese government on April 1, 2014. The Principles are:

- First Principle: Clarification of cases where transfers are prohibited; transfers of defense equipment are not allowed where the transfer:
  1. Violates obligations under treaties and other international agreements that Japan is party to: for example, the Chemical Weapons Convention, Convention on Cluster Munitions, and Convention on the Prohibition of Anti-Personnel Mines, and so on;
  2. Violates Japan's obligations under UN Security Council resolutions: for example, UN Security Council resolutions, and so on, that determine the prevention of transfer of weapons, and so on, to specific country such as UN Security Council Resolution 1718 (Nuclear Issue of North Korea) and UN Security Council Resolution 1929 (Nuclear Issue of Iran), and so on; and
  3. Is of goods destined for a country party to a conflict (a country against which the UN Security Council is taking measures to maintain or restore international peace and security in the event of an armed attack);
- Second Principle: Limitation to cases where transfers may be permitted as follows and to secure transparency when conducting a strict examination. Such cases include:
  1. Where the transfer contributes to the active promotion of world peace and international cooperation; and
  2. Where the transfer contributes to Japan's national security.

  When deciding whether or not to grant a Minister's license, a strict examination will be conducted. This examination will consider whether the transfer conforms to the approved cases of transfers of military equipment overseas, and whether the appropriateness of the destination and final consumer as well as the extent to which the transfer of the weapons, and so on, poses a threat to Japan's security. In addition, if the government has not

previously decided that it may allow overseas transfers for similar items, the matter shall be considered by the Executive Committee of the National Security Council (NSC). Important matters shall also be considered by the NSC. The Minister must judge whether or not to grant a license based on these deliberations; and

- Third Principle: Limitation to cases where appropriate controls regarding additional uses and transfers to a third country are ensured:

  1. The Government of Japan will, in principle, oblige the government of the recipient country to obtain its prior consent regarding additional uses and transfers to a third country.

The Minister must prepare an annual report on the status of permissions granted by it with regard to overseas transfers of military equipment. The report will be submitted to the NSC and must then be published. The government must disclose the matters deliberated by the NSC as important matters that require particularly careful consideration. Such disclosures of information to the public ensure transparency in the examination and judgment on the transfer of military equipment overseas.

22.8 General Licenses and License Exceptions

(a) General Licenses

Export licenses and licenses for a service transaction regarding the provision of technologies from the Minister under the FEFTA are usually granted individually for each contract (the “individual license”). However, taking into consideration whether the transactions are with a country participating in an international export control regime and the type or destination of the goods and technology, a “bulk license” may be granted to allow multiple export or service transactions if it is determined that there are no security or trade control issues to prevent granting such a license.

Bulk licenses include the following types (https://www.meti.go.jp/policy/anpo/apply13.html):

Special general bulk license	A system to bulk license the export of less sensitive goods and technologies for certain combinations of destinations and items, including those to regions other than those listed in Appended Table 3 of the FTCO.

(special bulk)	
General bulk license	A system to bulk license the export of less sensitive goods and technologies for certain combinations of destinations and items, limited to those shipped to regions listed in Appended Table 3 of the Export Order; exporters must apply for this license only electronically.
Specific bulk license	A system to bulk license the export of goods and technologies that is conducted between an exporter and the same counterparty in a continuing trading partnership.
Special bulk license for returns, etc.	A system to bulk license the export of items that fall under Appended Table 1-1 of the FTCO (weapons) or technology embedded in those items and that falls under Appended Table 1 of the FEO (programs), which were imported for use in Japan and are exported only for the purpose of return, repair, or replacement due to defects therein.
Specific bulk license for subsidiaries	A system to bulk license the export of certain products to subsidiaries of Japanese companies (more than 50 percent of capital).

Source: https://www.meti.go.jp/policy/anpo/guidance/guidance.pdf

If a bulk license is granted, an individual license is not needed. However, not only is a bulk license not applicable to all regions and goods, but the applicant must also establish internal regulations for export control and secure their reliable implementation.

Depending on the intended use (such as the development of nuclear weapons or when used for other military uses) and destination of the subject goods or technologies, the bulk license may expire, or it may be necessary to make a prior “notification” or follow-up “report” of an export made based on a bulk license to the Minister. Therefore, in practice, it is advisable to obtain an individual license.

(b) License Exceptions

(i) Goods

An exporter is not required to obtain a license from the Minister under FEFTA for:

- Goods such as fuel and ropes used on a specified vessels or aircraft;
- Aircraft on-board equipment for the safe arrival and departure of aircraft, which require repair or replacement;

- Goods sent by international organizations, which are exempted from regulations by treaties;
- Official goods sent to an Embassy of Japan;
- Goods free of charge (special exemption):
  - Goods imported and returned free of charge, such as when they are carried in and used by a person entering Japan temporarily;
  - Goods to be exported free of charge with a plan to import them free of charge at a later date, such as when they are carried in and used by a person leaving Japan temporarily.
- Goods in small amounts (special exemption):
  - Applicable when the total value of the goods listed in 5 to 13 and 15 of the Appended Table 1 of the ETCO) is 1 million yen or less; provided that in the case of goods that are listed in 3 of Attached Table 3 of the ETCO, the special exemption applies when the total value is 50,000 yen or less. However, this special exemption cannot be applied to the Catchall Control or to goods destined for Iran, Iraq, or North Korea.
- Components (special exemption):
  - Applicable when the goods intended to be exported contain a small component of regulated goods.

(ii) Provision of Technology

The cases where it is not necessary to obtain a license for the provision of technology are listed in Article 9 of the Ministerial Ordinance on Trade-Related Invisible Trade. The main examples include the following:

- Transactions that provide technology that is in the public domain or to provide technology to make said technology known to the public, and which fall under any of the following:
  - Providing technology that has already been released to an unspecified number of people through newspapers, books, magazines, catalogs, and files on telecommunications networks;
  - Providing technology available to an unspecified number of people, such as minutes of meetings of academic journals;
  - Providing technology available to or listened to by an unspecified number of people through factory tour courses, lectures, and exhibitions;

    - Providing a program with source code free to the public;
    - Designed for the purpose of making the relevant technology available or accessible to an unspecified number of people, through, for example, sending copies of presentations at academic conferences or copies of handouts at exhibitions or on other occasions, or by contributing articles to magazines.
- Transactions to provide technology in research activities in the field of basic science;
- Transactions to provide the minimum technology necessary for an application or registration of an industrial property right for the purpose of filing an application or registration thereof;
- Transactions to provide the minimum technology for use, which is provided in relation to the export of goods and for the installation, operation, maintenance, or repair of said goods (excluding programs and items specified by public notice);
- Transactions to provide the minimum technology for use, which is provided in association with the export of goods and is necessary for the installation, operation, maintenance, or repair of said goods (excluding programs and items specified by public notice);
- Programs specially designed for the use of goods, which are provided simultaneously with the relevant goods, where no source code is provided (excluding those specified by public notice);
- Transactions in technology imported in association with goods for assistance in a nuclear power disaster, and so on, and which is provided in association with the return of such goods;
- Transactions to provide cryptographic mechanisms or algorithms, or their reference codes, which are necessary in order to attend international conferences, make proposals, or express opinions for the development of international standards.

22.9 Penalties, Enforcement, and Voluntary Disclosure

(a) Administrative Penalties

Corporations that breach the requirements for licenses for the export of goods, or the provision of technology may be prohibited from exporting or transferring goods or technologies for not more than three years. An officer,

and so on, of a corporation that has been subject to administrative sanctions may be prohibited from activities such as exporting or importing as an officer, and so on, of another corporation that operates the same business as the business subject to the sanctions, or from newly starting the same business as an individual.

The corporation may also have its name published on the official website of METI, receive a warning from the Director-General, Trade and Economic Cooperation Bureau of METI, or be required to submit a report on unauthorized export of goods or provision of technologies, in which case the company name will not be published. In some cases, bulk licenses held by the corporation may be revoked.

(b) Criminal Penalties

Exporting or transferring controlled goods or technologies without obtaining a license is subject to punishment under the FEFTA as follows:

Subject Transactions	**Penal Provisions**	**Grounds for Provision**
Unauthorized technology transactions	Imprisonment for not more than seven years, a fine of the greater of not more than 20 million yen or five times the value of the transaction, or both	Article 69-6(1)(i)
Unauthorized intermediate transactions		Article 69-6(1)(i)
Unauthorized export of goods		Article 69-6(1)(ii)
Unauthorized technology transactions related to nuclear weapons	Imprisonment for not more than ten years, a fine of the greater of not more than 30 million yen or five times the transaction value, or both	Article 69-6(2)(i)
Unauthorized goods intermediate transactions related to nuclear weapons		Article 69-6(2)(ii)
Unauthorized export of goods related to nuclear weapons		Article 69-6(2)(ii)
Unauthorized export and sending overseas of technological documents and storage medium	Imprisonment for not more than five years, a fine of the greater of not more than 10 million yen or five times the transaction value, or both	Article 69-7(1)(ii)
Violation of administrative sanctions	Imprisonment for not more than three years, a fine of the greater of not more than 1 million yen or three times the transaction value, or both	Article 70(1)(xix) Article 70(1)(xxxii)
Obtaining license by		Article 70(1)(xxxvi)

illegal means		
Violation of compliance standards of exporters, etc.	Imprisonment for not more than six months or a fine of not more than 500,000 yen	Article 71(x)

(c) Enforcement

If it becomes clear that goods or technology regulated by the FEFTA have been exported without obtaining the permission of METI, an ex post facto review by METI will be conducted. The review procedure will commence when METI receives notification of a violation of the FEFTA from a third party or the violator. METI will clarify the facts, and if it is found that a violation of the FEFTA has occurred, it will draw up measures to prevent a recurrence of the violation. A decision on the penalty for the violation shall be made taking into consideration the degree of the violation, the possibility of a recurrence of the violation, and the degree of cooperation in the ex post facto review.

Criminal penalties may also apply.

(d) Voluntary Disclosures

Depending on the degree of noncompliance, an exporter that has violated export license requirements and who reports the violation may only be subject to guidance from METI to avoid a recurrence.

There is no formal criteria for METI accepting a voluntary disclosure, however, it is likely that METI will determine the degree of noncompliance by taking into account such factors as whether such actions are intentional, whether such actions are malicious, whether the consequences are serious, and so on.

22.10 Recent Export Enforcement Matters

Some recent enforcement actions for serious violations of export controls include the following:

- The export of regulated infrared cameras to China without the required export permits.
  - On January 22, 2018, a fine of 1 million yen was imposed on the exporter, and on April 24, 2018, an administrative penalty was

imposed to prohibit exports by the exporter of all goods to any and all regions for three months.

- The export of “vacuum suction pressure molding machines” (being a controlled product “induction furnaces”) to Iran, China, Thailand, and other countries without the required export permits.
  - On July 25, 2017, an administrative penalty was imposed to prohibit the exporting company from exporting any goods to any and all regions for three months.
- The export of carbon fiber, a regulated product, to China via Korea as a transit point without the required export permits.
  - On June 15, 2015, a fine of 1 million yen was imposed on a former employee of an exporting company, and a fine of 1 million yen was imposed on the exporting company. On January 20, 2016, an administrative penalty was imposed to prohibit the exporting company from exporting any goods to any and all regions for four months.

22.11 Special Topics

(a) Re-exports/Extraterritorial Application of Laws

FEFTA, ETCO, and FEO apply to the re-exporting of goods imported into Japan in the same manner as normal exports.

In addition, importing a U.S. product or product manufactured using U.S. technology from the U.S. into Japan and then re-exporting it to a third country is regulated by U.S. export control laws and export control regulation (Export Administration Regulations (EAR)) even within the territory of Japan. However, Japan’s export laws do not apply to the re-export of a Japanese product or a product manufactured using Japanese technology from the recipient country to a third country.

(b) Intangible Transfer of Technical Information

As explained in Section 22.4(b), the export of technology is regulated by Article 25, paragraph 1 of the FEFTA and the Appended Table of the FEO.

(c) Practical Issues Related to Export Control Clearance

The determination of whether or not the export of goods and technologies are regulated by the Appended Tables 1 and 2 of the ETCO, the FEFTA, or the Appended Table of the FEO, is referred to as nondetermination. In Japan, the issue is that it takes labor to perform such nondetermination. In addition, another issue is that the nondetermination is required at the time of export to overseas branches and subsidiaries and export for returned product.

(d) Recordkeeping

Exporters that export as a business must keep books that describe the product name, quantity, and price of the exported goods (excluding documents submitted to customs). Recordkeeping requirements include the following:

1. Books
    - Matters to be described. Product name, quantity, price, name (entity name) of exporter, date of export license, and the license number (it is possible to add the necessary items to existing books and purchase forms).
    - Storage period. Five years (starting from the day following the date of the export license).
2. Documents
    - Contents of documents. Documents prepared or received for transactions related to purchase orders and licensed goods.
    - Storage period. Five years (starting from the day following the date of the export license).
3. Storage of electronic records related to transaction information of electronic transactions
    - Contents of electromagnetic records. Transaction information when an electronic transaction (so-called EDI transactions, transactions on the internet, transactions that exchange transaction information by email, etc.) is conducted (matters usually described in order forms and contracts exchanged for transactions).
    - Storage Period. Five years (starting from the day following the date of the export license).

(e) How to Be Compliant When Exporting to Japan

When collecting foreign goods that have arrived in Japan, an import declaration has to be submitted to the customs office that has jurisdiction over the bonded area (a place designated by the Minister of Finance or a place permitted by the Director-General of Customs as a place to put goods to be exported or goods arriving from abroad) where the goods are stored.

If goods require an import license or approval under laws and regulations other than those related to customs duties, it must be obtained prior to obtaining the customs import license. (Customs Act, Article 67, Article 67-2, Article 70, and Article 72)

(f) How to Be Compliant When Exporting from Japan

Before exporting goods, an export declaration has to be submitted by the exporter (or a customs broker for the exporter) to the customs office that has jurisdiction over the location of the bonded area in which the goods are placed, the goods must pass any necessary inspection, and an export license is then obtained.

An export declaration may be made before the goods to be exported are brought into the bonded area, although it is usually issued afterwards.

When exporting goods that have export restrictions, such as requiring licenses and approvals under laws and regulations other than the Customs Act (e.g. military equipment as described above), it is necessary to submit the license or approval documents when submitting the export declaration to customs (Customs Act, Article 67, Article 67-2, and Article 70).

22.12 Encryption Controls

(a) General Comments

Export control on cryptographic equipment and the provision of cryptographic technology is also regulated by the FEFTA.

(b) Import Encryption Clearance Requirements

There are no specific regulations on cryptographic imports in Japan, though it is prohibited to import cryptographic equipment or components for

implementing cryptographic functions from North Korea under the general restrictions on imports from North Korea.

(c) Encryption Licensing Requirements

“Cryptographic equipment or components for implementing cryptographic functions” is subject to the List Control (Appended Table 1-9(7) of the ETCO). If the goods to be exported are “cryptographic equipment or components for implementing cryptographic functions” and also have the regulated specifications prescribed in Article 8, item 9 of the MOSG, export permission must be obtained from the Minister in advance.

In addition, providing cryptographic technology to a non-resident within or outside Japan (technologies listed in the Appended Table 9 of the FEO), requires obtaining export permission from the METI. For example, if selling a cryptographic program or application as software or providing it by email to a nonresident outside Japan, it is necessary to obtain prior export permission from the Minister unless the information is disclosed to an unspecified number of persons on the cryptographic program or cryptographic application home page.

(d) Penalties for Violation of Encryption Regulations

Any person who exports goods pertaining to cryptographic equipment without permission or provides cryptographic technology without permission is liable to imprisonment with labor for not more than seven years or a fine of the greater of not more than 20 million yen or five times the transaction value, or both. Any person who exports documents or data storage media related to cryptography or transmits such documents or data outside Japan without permission is liable to imprisonment with labor for not more than five years or a fine of the greater of not more than 10 million yen or five times the transaction value, or both.

22.13 Blocking Laws/Penalties for Compliance with Sanction Imposed by Other Countries

There are no blocking laws or penalties in Japan for compliance with sanctions imposed by other countries.

23

Export Controls and Economic Sanctions in Malaysia

Kuok Yew Chen and Tracy Wong[1]

23.1 Overview

(a) What Is Regulated?

The key legislation relating to export controls and economic sanctions in Malaysia include the following:

- Customs Act 1967 (CA)
- Strategic Trade Act 2010 (STA)
- Chemical Weapons Convention Act 2005 (CWCA)
- Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA)

Malaysia is a member of the Organization for the Prohibition of Chemical Weapons. However, Malaysia is not a member of the Wassenaar Arrangement, the Australia Group, the Missile Technology Control Regime, or the Nuclear Suppliers Group.

As a member of the United Nations, Malaysia implements resolutions adopted by the United Nations Security Council, such as the United Nations Security Council Resolution 1540 on nonproliferation of weapons of mass destruction, which is crystallized through the enactment and enforcement of the STA.

(b) Free Trade Agreements

At the time of writing, Malaysia has implemented seven bilateral free trade agreements (FTAs), which were entered into with the following countries:

- Australia
- Chile
- India
- Japan
- New Zealand
- Pakistan
- Turkey

In addition to bilateral FTAs, Malaysia, by virtue of being a member country of the Association of Southeast Asian Nations (ASEAN), is also party to the following regional FTAs:

- ASEAN-China Free Trade Agreement (ACFTA)
- ASEAN-Korea Free Trade Agreement (AKFTA)
- ASEAN-Japan Comprehensive Economic Partnership (AJCEP)
- ASEAN-Australia-New Zealand Free Trade Agreement (AANZFTA)
- ASEAN-India Free Trade Agreement (AIFTA)
- ASEAN Trade In Goods Agreement (ATIGA)
- ASEAN-Hong Kong Free Trade Agreement (AHKFTA)

The ACFTA, AKFTA, AJCEP, AANZFTA, and AIFTA are collectively known as the ASEAN Plus One FTAs.

Malaysia is a party to and has signed the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), but, at present, it is still pending ratification and entry into force. Malaysia is also currently undertaking two FTA negotiations, namely, the Malaysia-EU Free Trade Agreement (MEUFTA) and the Malaysia-European Free Trade Association Economic Partnership Agreement (MEEPA). Please see https://fta.miti.gov.my/index.php/pages/view/4?mid=23 for an updated list of the FTAs that Malaysia is a party to.

(c) Regional Comprehensive Economic Partnership (RCEP) in Malaysia

The RCEP represents the world's largest trade deal to date, creating a trade bloc that covers approximately 30 percent of the world's population and global gross domestic product. On January 21, 2022, the Ministry of International Trade and Industry (MITI) had issued a media release to announce that Malaysia's Instrument of Ratification has been submitted to the ASEAN Secretariat on January 17, 2022. With this, Malaysia became the twelfth signatory country, on March 18, 2022, to implement the RCEP. In gist, the objective of the RCEP is to establish a modern, comprehensive, high-quality, and mutually beneficial economic partnership that will facilitate the expansion of regional trade and investment and contribute to global economic growth and development.

Even though Malaysia has already signed bilateral and regional FTAs with each of the RCEP member states (see Section 23.1(b)), the RCEP plays a key role in consolidating and building on the existing ASEAN Plus One FTAs by improving key areas of trade, such as establishing a single rule of origin criteria across all RCEP member states and increasing the number of sectors open to foreign participation to improve market access. Among others, the RCEP also simplifies customs procedures, which facilitates quicker and more efficient administration of procedures as well as the clearance and release of goods.

(d) Where to Find the Regulations

Malaysian legislation is made available to the public on the Attorney General's Chambers of Malaysia's Official Portal available online at https://www.agc.gov.my, or the Malaysian Federal Legislation Portal available online at https://lom.agc.gov.my/index.php. Although these sources are official and maintained by the Malaysian government, they may not be complete and may not a contain up-to-date regulations or orders. As an alternative, the updated Malaysian legislation may also be obtained through various paid online legal subscription resources.

(e) Who Is the Regulator?

The Royal Malaysian Customs Department ("Malaysian Customs"), which is under the purview of the Ministry of Finance (MoF), is the main governing agency responsible for generally overseeing imports and exports from Malaysia. Specifically, in respect of the regulation of strategic items,

the Strategic Trade Secretariat (STS) division under MITI is the main authority that oversees the implementation of the STA and its regulations. The Central Bank of Malaysia or Bank Negara Malaysia (BNM) is the main regulatory body responsible for overseeing the compliance with anti-money laundering laws in Malaysia under the AMLA, where an element of the AMLA does include sanctions compliance.

(f) How to Get a License

Generally, the export of goods may be subject to licenses, permits, or approvals, depending on the type of goods to be exported and whether or not the exported goods fall within the scope of controlled goods or strategic goods. Further details of the licensing process are set out later in the chapter.

(g) Key Websites

The key website with the relevant information on general imports and exports is the Customs website: http://www.customs.gov.my/en. The key website with the relevant information on regulation of the STA is the MITI website: https://www.miti.gov.my/index.php/pages/view/2581.

23.2 Structure of the Laws and Regulations

As set out in Section 23.1(a), there are various statutes in Malaysian law that deal with different aspects of export control and economic sanctions. These statutes broadly cover the requirements of export control, such as the licenses and permits required for export of goods from Malaysia.

These statutes are supplemented by related subsidiary legislation, in the form of regulations and orders. These subsidiary legal instruments drill down into more granular details and provide further elaboration on the nature of the export controls and economic sanctions in Malaysia, as well as set out the offenses and penalties for failing to comply with these requirements. A non-exhaustive list of the crucial legislation, and the key subsidiary legislation, is set out next in Section 23.3.

As a UN member state, Malaysia has implemented domestic regulations to give effect to the decisions of the United Nations Security Council

(UNSC). A brief overview on the Malaysia sanctions regime is set out below in Section 23.10.

23.3 What Is Regulated: Scope of the Regulations

The legislation and subsidiary legislation in Malaysia are structured such that different aspects of export control and economic sanctions are covered by different statutes, as follows:

(a) The CA

The CA is the main legislation for the regulation and control of exports out of Malaysia. In particular, the Customs (Prohibition of Exports) Order 2017 ("Export Prohibition Order") is the main regulation setting out the specific license, permit, and/or approval requirements for the export of certain types of controlled goods.

(b) The STA

The STA is the main legislation that regulates the export, transshipment, transit, and brokering of strategic items and technology as well as activities that will or may facilitate the design, development, production, and delivery of weapons of mass destruction.

In particular, the Strategic Trade (Strategic Items) Order 2010 ("STA" Order) contains a full listing of the goods and technology that are deemed to be strategic items for the purpose of the STA, which essentially adopts the EU Control List of Dual-Use Items.

The Strategic Trade (United Nations Security Council Resolutions) Regulations 2010 ("UNSC Regulations") requires for certain measures, in accordance with the relevant resolutions of the United Nations Security Council, to be taken in relation to countries and persons designated under the Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010.

The STA also applies to "unlisted items," which refers to items that may be used in a restricted activity but are not prescribed as strategic items. As such, given that certain obligations under the STA also apply to "unlisted items" if the exporter does have knowledge that the unlisted item is capable

of being used in a restricted activity, then the STA obligations would also apply. It is important to note that there is an expectation from the regulator for exporters to conduct their own due diligence on the items being exported to determine whether the item is capable of being used in a restricted activity or not.

To further clarify, the STA defines “restricted activity” as “any activity that supports the development, production, handling, usage, maintenance, storage, inventory or proliferation of any weapon of mass destruction and its delivery systems; or participation in transactions with persons engaged in such activities.”

The STA also extends to intangible technology transfers (ITT), which is defined to mean the transmission or transfer of information and data, by any means, to a destination outside Malaysia, in any form, for the design, development, production, or use of another item. This includes transfer of technical data, technical assistance, and software.

In addition to the preceding, the Strategic Trade (Compounding of Offenses) Regulation 2022 was introduced on June 1, 2022, and prescribes that certain offenses under the STA may be compounded. It also prescribes the procedure for compounding, as well as the acceptance and payment of such compounds.

(c) The CWCA

The CWCA regulates, among other things, the export of certain controlled chemicals under the Chemical Weapons Convention.

Further, Malaysia is also a party to the following conventions under the World Trade Organization:

- Convention establishing a Customs Co-Operation Council
- Customs Convention on the ATA Carnet for the Temporary Admission of Goods (ATA Convention)
- International Convention on the Simplification and Harmonization of Customs Procedures (Kyoto Convention)
- International Convention on Mutual Administrative Assistance for the Prevention, Investigation and Repression of Customs Offenses (Nairobi Convention)
- Convention on the Valuation of Goods for Customs Purposes

23.4 Who Is Regulated

Any party who wishes to export goods from Malaysia will be regulated under the applicable statutes and their relevant subsidiary legislations. It is the exporter who will have to comply with the requirements of, among other things, obtaining the appropriate export permit for the export of goods from Malaysia.

23.5 Classification

(a) Harmonized System Codes

Classification of goods is based on the Harmonized Commodity Description and Coding System developed by the World Customs Organization ("HS Code"). Exporters should be aware of the classification system and should be able to classify their goods under the appropriate product code. This is to ensure that the exporter is able to accurately fill in the information required for the export declaration through DagangNet, and to allow the exporter to determine whether the goods are subject to control by any competent authorities.

Goods are classified in Malaysia according to a ten-digit tariff nomenclature, as set out under the Customs Duties Order 2022 (CDO). For example, butter would be classified under the code number 0405.10.00 00. This classification system is adopted from the ASEAN Harmonized Tariff Nomenclature (AHTN), which is an eight-digit classification system used by all ten ASEAN member countries. This is, in turn, based on the HS Code.

Exporters may easily determine the appropriate HS Codes for their products based on the following methods:

- Checking the HS Explorer website at http://mysstext.customs.gov.my/tariff/;
- Checking against the latest version of the CDO from the federal e-gazette website or paid online legal resources;
- Obtaining advice from the Technical Services Division of the Malaysian Customs; and

- Checking against free trade agreements that Malaysia is a party to (where applicable).

Once the HS Codes of the goods have been determined, the exporter may then use this to determine whether the goods are classified as controlled goods and therefore require the approval of the relevant competent authority before export by checking the code against the Export Prohibition Order. Some illustrations of the types of controlled goods, and their corresponding competent authorities, are set out here:

- Animals—competent authorities in Malaysia include the Department of Malaysian Quarantine and Inspection Services for exports from Peninsular Malaysia and Labuan, Department of Veterinary Services and Animal Industry, Sabah, for exports from Sabah; and State Veterinary Authority, Sarawak, for exports from Sarawak;
- Arms and ammunition (including paintball marker and/or paintball pellets for sporting and taser guns)—under the authority of the Chief Police Officer;
- Pesticides—competent authorities responsible include the Pesticides Board, and the Department of Agriculture; and
- Hazardous wastes—under the authority of the Director General of Environmental Quality.

(b) Strategic Items

Under the STA, Malaysia regulates the export, transshipment, transit, and brokering of strategic items and strategic technology, including ITT.

The list of strategic items is set out in the Schedule of the STA Order. It essentially regulates two types of goods: military goods and dual-use goods. Part I of the Schedule sets out the technical details of the type of military goods regulated, including items such as firearms, ammunitions, bombs, tanks, imaging devices, and chemicals. The list of military goods regulated as strategic goods is set out as follows:

Category Code	**Description**
ML1	Small-caliber arms
ML-2	Large-caliber weapons and projectors
ML-3	Ammunition and fuse setting devices
ML-4	Bombs, missiles, other explosive devices, and related equipment

ML-5	Fire control and related alerting and warning equipment
ML-6	Ground vehicles and components
ML-7	Chemical or biological toxic agents and related equipment
ML-8	Explosives, propellants, fuels, and related substances
ML-9	Naval vessels and components
ML-10	Military aircraft and components
ML-11	Electronic equipment for military use
ML-12	High-velocity kinetic energy weapons
ML-13	Armored or protective equipment
ML-14	Specialized equipment for military training
ML-15	Imaging or countermeasure equipment
ML-16	Unfinished products for use in military items
ML-17	Miscellaneous equipment and materials
ML-18	Production equipment for military items
ML-19	Directed energy weapon systems
ML-20	Cryogenic and “superconductive” equipment
ML-21	Specific software for military items
ML-22	Specific technology for military items

Part II of the Schedule then sets out the types of dual-use goods regulated as strategic goods. Dual-use goods essentially comprise goods that are designed for commercial applications, but which can have military applications, or which can potentially be used as precursors or components of weapons of mass destruction. A five-character alphanumeric code is used for the list of dual-use goods. The list is divided into the following ten broad categories:

Category Number	**Description**
0	Nuclear materials, facilities, and equipment
1	Special materials and related equipment
2	Materials processing
3	Electronics
4	Computers
5	Part 1 Telecommunications Part 2 Information security
6	Sensors and lasers
7	Navigation and avionics

8	Marine
9	Aerospace and propulsion

Each category of dual-use goods is then further sub-divided into five product groups, as follows:

Product Group	**Description**
A	Systems, equipment, and components
B	Test, inspection, and production equipment
C	Materials
D	Software
E	Technology

For example, Category Code “3A001” can be broken down as follows:

- The first numeral refers to the category, whereby “3” is for electronics;
- The second letter refers to the subcategory, whereby “A” is for systems, equipment, and components;
- The third numeral refers to the regime origin, whereby “0” is for the Wassenaar Arrangement; and
- The fourth and fifth numerals refers to the item’s individual entry code.

To ascertain whether the product comprises strategic items, the exporter must compare the product’s specifications against the possible item descriptions and notes in the STA Order. If there is no possible Category Code that matches the product’s specifications and description, then the product is not a strategic item. Even if the product meets the stated specifications, it will not be a strategic item if it fulfills the applicable exclusion notes, which can be found in the item descriptions and notes themselves.

Alternatively, exporters may refer to the Strategic Trade Item Finder, available at https://www.miti.gov.my/index.php/sti/sti_finder.

The STS provides assistance in the classification of items under the STA. Exporters may forward samples and specifications of the item to STS for evaluation. If only certain parts of a finished product are strategic items, an exporter should also forward the technical specifications of the parts that are strategic items to the STS for evaluation.

(c) Chemical Weapons Control

The CWCA was enacted to provide the Malaysian government with the legislative framework required to fulfill Malaysia's obligations under the Chemical Weapons Convention. Section 6 of the CWCA gives rise to the establishment of the National Authority in Malaysia ("National Authority"), which consists of 14 Malaysian ministries, including MITI, who in particular is tasked with the responsibility for the implementation of Malaysia's obligations under the Chemical Weapons Convention in terms of international trade.

The Chemical Weapons Convention contains three Schedules that classify toxic chemicals and their precursors, along with an additional category of unscheduled discrete organic chemicals (DOCs). The Schedules of the Chemical Weapons Convention are reflected within the CWCA under Schedules 1, 2, and 3, respectively (referred to as "Schedule 1 chemicals," "Schedule 2 chemicals," and "Schedule 3 chemicals," respectively). The Schedules are organized to reflect the risks posed by the chemical to the object and purpose of the Chemical Weapons Convention. A description of the types of chemicals listed in each Schedule is set out here.

Schedules	**Description**	**Examples of Chemicals**
1A & 1B	Chemicals that may be used as chemical weapons or as precursors in the final single technological stage of production of a chemical weapon	Saxitoxin
		Sarin
		Tabun
		Ricin
2A & 2B	Chemicals that may be used as chemical weapons or as precursors in one of the chemical reactions at the final stage of formation of a chemical listed in Schedule 1.	Arsenic trichloride
		Amiton
		Thiodiglycol
		Pinacolyl alcohol
3A & 3B	Chemicals that may be used as chemicals or that are important to the production of one or more chemicals listed in Schedules 1 or 2.	Cyanogen chloride
		Hydrogen cyanide
		Trimethyl phosphite
		Sulfur dichloride

Unscheduled DOCs are also regulated under the CWCA, as the facilities built for their production could have the potential of being converted to chemical weapons production facilities. Unscheduled discrete organic

chemicals refer to any chemical belonging to the class of chemical compounds consisting of all compounds of carbon, except for its oxides, sulfides, and metal carbonates.

Further information on identifying discrete organic chemicals is available at https://www.kln.gov.my/cwc/index.php?option=com_content&view=article&id=53&Itemid=62 under "Item 4: Flow Chart to Identify DOC's".

23.6 General Prohibitions/Restrictions/Requirements

As further elaborated next in Section 23.7, there are various licensing restrictions and requirements associated with the export of goods from Malaysia, depending on the type of goods that are intended to be exported.

(a) General Customs Prohibitions

Under the CA, and further to preceding Section 23.3(a), the Export Prohibition Order is the relevant order that prescribes an exhaustive list of goods that are either:

- Absolutely prohibited for export to all countries, such as certain poisonous chemicals and minerals; or
- Prohibited for export, except if under an export license and subject to the conditions specified under the export license.

Further details with regard to export licenses are described later in the chapter in Section 23.7(b).

(b) Strategic Items

The STA End-Users Order sets out a list of restricted and prohibited end users with regard to export control. The difference between a restricted and prohibited end user is that export relations with the former is possible through a special STA permit, while export to the latter is strictly forbidden. The prohibited end users listed are based on the sanctions imposed by the United Nations Security Council. An updated list can be found at the United Nations website at https://www.un.org/securitycouncil/content/resolutions.

To illustrate, the current restricted and prohibited end users are as follows:

End Users	Transit or Transshipment To	Remarks
Restricted (*Special Permit required*)	• Democratic Republic of Congo • Ivory Coast • Lebanon • Sudan • Libya	Embargoed and subject to transit permit for military items
	• Afghanistan • Iraq • Liberia • Rwanda • Somalia	Subject to transit permit for military items
	• Eritrea	Subject to transit permit for restricted military items
Prohibited	• Democratic People's Republic of Korea *As listed in the United Nations Security Council Resolution 1718 (2006)*	All export, transit, transshipment of strategic items or unlisted items are prohibited.
	• Islamic Republic of Iran *As listed in the United Nations Security Council Resolution 2231 (2015)*	

23.7 Licensing/License Exceptions

(a) Export Declaration

Generally, the CA requires exporters or customs agents to register with Malaysian Customs and submit a Customs Export Declaration Form before exporting goods from Malaysia, a process that can be done online on the DagangNet portal (http://www.dagangnet.com), the electronic permit application platform in Malaysia. All customs declarations should indicate a full and true account of the number and description of goods and packages, value, weight, measurement or quantity, and the country of final destination.

(b) Controlled Goods

As briefly stated in Section 23.6(a), if the goods to be exported are listed in the Export Prohibition Order, then the exporter would be required to apply for an export license, which is also known as an Approved Permit (AP).

While the CA is the legislation that regulates exports in general, APs are issued by several designated permit-issuing agencies in Malaysia (PIA). Please refer to the following table for a non-exhaustive list of PIAs.

No.	Permit Issuing Agencies (PIA)
1.	Ministry of Communications and Multimedia
2.	Ministry of Domestic Trade and Consumer Affairs
3.	Ministry of Health
4.	Ministry of International Trade and Industry (MITI)
5.	Ministry of Natural Resources and Environment

If the goods to be exported are strategic items, then an STA permit issued by MITI is required. This is further elaborated at Section 23.7(c).

Controlled goods can be subject to different forms of requirements in order to be exported from Malaysia, depending on the PIA regulating and overseeing the export of the specific controlled goods.

The first step in exporting controlled goods is to determine whether the goods to be exported are indeed controlled, and, if so, the specific competent authority which regulates it. For example, according to the Export Prohibition Order, some controlled exports and the respective PIAs with authority to issue permits for exporting these goods are as follows:

Controlled Export	PIA
Waste and scrap of iron, steel, copper, nickel, aluminum, lead, zinc, and toxic chemicals under the CWCA (see Section 23.5(c))	MITI
Certain minerals, ores, coal, lignite, and peat	Ministry of Natural Resources and Environment
Sugar and wheat flour	Ministry of Domestic Trade and Consumer Affairs
Military clothing, headgear, footwear, and other textiles articles	Ministry of Defence
Arms and ammunition including paintball markers, paintball pellets, and electroshock (e.g., Taser®) guns	Chief Police Officer

A more comprehensive determination as to whether the particular product is a controlled export can be obtained once the exporter has ascertained the HS Code of the product and checking against the Export Prohibition Order. Where unsure, an exporter can request a formal classification from Malaysian Customs itself, by contacting the Technical

Services Division (http://www.mobile.customs.gov.my/edirektori/portal-branch?x=8&km=865e62452a321157e796f056506478ac&lang=en).

Once the exporter has determined that the product it intends to export is a controlled export and identified the relevant PIA, the exporter will then have to comply with that PIA's requirements. Each PIA has different requirements. An application for a permit can also be completed online via the DagangNet portal (http://www.dagangnet.com).

(c) Strategic Items

Any party that wishes to export, transship, or bring in transit strategic items out of Malaysia is required to obtain an STA permit from MITI ("STA Permit"). This can be obtained through the DagangNet portal (http://www.dagangnet.com/trade-facilitation/epermit-sta/). STA permits are issued by four authorities:

- STS, MITI
- Atomic Energy Licensing Board
- Malaysian Communication and Multimedia Commission
- Pharmaceutical Services Division, Ministry of Health

There are four types of STA permits available:

- Single-use permit
- Bulk permit
- Multiple-use permit
- Special permit

The following table describes each STA permit accordingly:

No.	Permit Type	Permit Use	Permit Validity Period	Timeline to Obtain Permit
1.	Single-use	One-time export for a country or destination	6 months	working days
2.	Bulk	Multiple exports for a single country or destination	years	
3.	Multiple-use	Multiple exports for different countries or destinations		
4.	Special	Single-use export to a restricted end-user	1 year	

Note that the timeline of five working days is what is provided by MITI and it assumes complete documentation has been provided to MITI. In the event incomplete documentation is provided, MITI reserves the right to request additional information and the five-working day timeline will restart upon MITI's receipt of the documents requested.

In support of an application for STA permits, the following are some documents generally required to be submitted online. Similarly, these can also be submitted online through the DagangNet portal (http://www.dagangnet.com):

- End-use statement, that contains information on the end user and end use of the items that will be exported;
- Technical specifications of the goods;
- An undertaking by the exporter to provide a Delivery Verification within two months from the date of export (in the case of a single permit) or when requested (in the case of multiple and bulk permits);
- Purchase order;
- Customs Export Declaration Form (see Section 23.7(a));
- Invoice;
- Additional documents as may be required such as an (1) approval letter for multiple-use and bulk-permits and (2) approval letter from the Royal Malaysian Police in relation to military products; and
- Other documentation as may be required, such as information about the original manufacturer of the product to be exported, or about the key individuals in the applicant company's management.

Applications for bulk and multiple-use permits are only considered if the applicant company has an MITI-approved Internal Compliance Programme (ICP) in place. Briefly, an ICP is an internal set of procedures implemented within a company to ensure compliance with the requirements under the STA. To this end, MITI has come up with an ICP Checklist that indicates examples of best practices for companies to adhere to. The ICP Checklist was recently revised and it is available online at https://www.miti.gov.my/miti/resources/STA%20Folder/PDF%20file/Attachment_II_-_ICP_Checklist.pdf.

In addition, exporters who hold STA permits are subject to responsibilities, such as recordkeeping obligations and reporting obligations. Exporters are advised to refer to the STA and the STS website

(https://www.miti.gov.my/index.php/pages/view/sta2010#FAQ) for further information on the compliance requirements.

(d) Strategic Goods Export Permit Exceptions

Further to Section 23.3(b), the STA provides that a requirement to obtain a permit for the export of technology is waived to the extent that the export or transmission of strategic technology is necessary to facilitate:

- The installation, operation, maintenance, or repair of any items that have been exported;
- An application for a patent; or
- Research in such strategic technology, the results of which have no practical application.

(e) Chemical Weapons Convention

An authorization issued by the National Authority ("NA(CWC) Authorization") is required before the export of any of the Schedule 1 chemicals.

While the export of Schedule 2 and Schedule 3 chemicals do not require an NA(CWC) Authorization, the export of all Schedule 1, 2, and 3 chemicals requires an export permit from MITI. This means that the export of Schedule 1 chemicals requires an export permit from MITI in addition to an NA(CWC) Authorization.

Please note that controlled chemicals may also constitute strategic goods and be subject to the export control requirements under the STA.

In addition, certain restrictions apply where the controlled chemical is to be exported to states that are not a member of the Chemical Weapons Convention, depending on whether the controlled chemical is classified as a Schedule 1, Schedule 2, or Schedule 3 chemical.

Schedules	**Export to Nonmember States**
Schedule 1	Prohibited, unless: (a) the export is for research, medical, pharmaceutical, or protective purposes; (b) the types and quantities of the toxic chemicals are strictly limited to those that can be justified for such purposes; (c) the aggregate amount of such chemicals at any given time for such purposes is equal to or less than 10 kilograms for each facility in a

	calendar year; and (d) authorized by the National Authority. (collectively, “Specified Purposes”)
Schedule 2	Prohibited
Schedule 3	Allowed, subject to the submission of an end-user certificate issued by the National Authority.

The export of Schedule 1 chemicals will always require an NA(CWC) Authorization, pursuant to the CWCA.

However, the export of Schedule 2 and Schedule 3 chemicals without an NA(CWC) Authorization (but with an export permit from MITI) will be permitted where the export is to a member state of the Chemical Weapon Convention.

23.8 Penalties, Enforcement, and Voluntary Disclosures

(a) Penalties for Failure to Comply with Export Requirements

The CA provides that the following activities shall constitute offenses and shall be liable on conviction to the following penalties:

Prohibited Activity	**Penalty**
Failure to maintain records	Where the value of the goods can be ascertained, the importer will be liable to a fine not less than two times and not more than ten times the original value of the goods. With regards to goods for which value cannot be ascertained, the importer will be liable to a fine of not less than RM100,000 and not more than RM500,000. A fine not exceeding RM100,000 or to imprisonment for a term not exceeding five years or both.
Making incorrect declarations or falsifying documents	A fine not exceeding RM500,000 or to imprisonment for a term not exceeding seven years or both.
Refusing to answer questions or give information	Imprisonment for a term not exceeding five years or to a fine not exceeding RM100,000 or both.
Various smuggling offenses	First offense: A fine not less than ten times the amount of the customs duty or RM50,000, whichever is greater; and of not more than 20 times the amount of customs duty or RM500,000, whichever is greater. Second and subsequent offense: Fine not less than 20 times the amount of customs duty or RM100,000, whichever is the greater amount or to imprisonment for a term not exceeding seven years or both.

The STA provides that the exporting, transshipping, or bringing in transit strategic items without a permit shall constitute offenses and shall be liable on conviction to the following penalties:

Prohibited Activity	**Penalty**
In relation to strategic items that are arms or related material, where the act is done with the intent to unlawfully export, transship, or bring in transit strategic items that are arms or related material without a permit or with knowledge that the export, transshipment, or bringing in transit of such strategic items without a permit is unlawful.	Where death is the result of the act: • Individual: death or imprisonment for natural life; • Corporation: minimum fine of RM30 million. In any other case: • Individual: imprisonment for a term not exceeding ten years or with a fine not exceeding RM10 million or with both; • Corporation: a fine not exceeding RM20 million.
In relation to strategic items that are arms or related material, where the act is done without the intent to unlawfully export, transship, or bring in transit such strategic items without a permit or without knowledge that the export, transshipment, or bringing in transit of such strategic items without a permit is unlawful.	Individual: imprisonment for a term not exceeding five years or with a fine not exceeding RM5 million or with both; Corporation: fine not exceeding RM10 million.
In relation to strategic items other than arms or related material, where the act is done with the intent to unlawfully export, transship, or bring in transit such strategic items without a permit or with knowledge that the export, transshipment, or bringing in transit of such strategic items without a permit is unlawful.	Individual: imprisonment for a term not exceeding ten years or with a fine not exceeding RM10 million or with both; Corporation: fine not exceeding RM20 million.
In relation to strategic items other than arms or related material, where the act is done without the intent to unlawfully export, transship, or bring in transit such strategic items without a permit or without knowledge that the export, transshipment, or bringing in transit of such strategic items without a permit is unlawful.	Individual: imprisonment for a term not exceeding five years or with a fine not exceeding RM5 million or with both; Corporation: fine not exceeding RM10 million.

The STA provides that the exporting, transshipping, or bringing in transit strategic items or unlisted items to a restricted end user without a special permit shall constitute offenses and shall be liable on conviction to the following penalties:

Prohibited Activity	**Penalty**
In relation to strategic items or unlisted items that are arms or	Where death is the result of

related material, where the act is done with the intent to unlawfully export, transship, or bring in transit such items without a special permit or with knowledge that the export, transshipment, or bringing in transit of such strategic items without a special permit is unlawful.	the act: • Individual: death or imprisonment for natural life; • Corporation: a minimum fine of RM30 million. In any other case: • Individual: imprisonment for a term not exceeding ten years or with a fine not exceeding RM10 million or with both; • Corporation: fine not exceeding RM20 million.
In relation to strategic items or unlisted items that are arms or related material, where the act is done without the intent to unlawfully export, transship, or bring in transit such items without a special permit or without knowledge that the export, transshipment, or bringing in transit of such strategic items without a special permit is unlawful.	Individual: imprisonment for a term not exceeding five years or with a fine not exceeding RM5 million or with both; Corporation: fine not exceeding RM10 million.
In relation to strategic items or unlisted items other than arms or related material, where the act is done with the intent to unlawfully export, transship, or bring in transit such items without a special permit or with knowledge that the export, transshipment, or bringing in transit of such strategic items without a special permit is unlawful.	Individual: imprisonment for a term not exceeding ten years or with a fine not exceeding RM10 million or with both; Corporation: a fine not exceeding RM20 million.
In relation to strategic items or unlisted items other than arms or related material, where the act is done without the intent to unlawfully export, transship, or bring in transit such items without a special permit or without knowledge that the export, transshipment, or bringing in transit of such strategic items without a special permit is unlawful.	Individual: imprisonment for a term not exceeding five years or with a fine not exceeding RM5 million or with both; Corporation: a fine not exceeding RM10 million.

The STA provides that the exporting, transshipping, or bringing in transit strategic items to a prohibited end user shall constitute offenses and shall be liable on conviction to the following penalties:

Prohibited Activity	**Penalty**
In relation to strategic items or unlisted items that are arms or related material, where the act is done with the intent to unlawfully export, transship, or bring in transit such items without a special permit or with knowledge that the export, transshipment, or bringing in transit of such strategic items without a special permit is unlawful.	Where death is the result of the act: • Individual: death or imprisonment for natural life; • Corporation: a minimum fine of RM30 million. In any other case: • Individual: imprisonment for a term not exceeding ten years or with a fine not

	exceeding RM10 million or with both; • Corporation: fine not exceeding RM20 million.
In relation to strategic items or unlisted items that are arms or related material, where the act is done without the intent to unlawfully export, transship, or bring in transit such items without a special permit or without knowledge that the export, transshipment, or bringing in transit of such strategic items without a special permit is unlawful.	Individual: imprisonment for a term not exceeding five years or with a fine not exceeding RM5 million or with both; Corporation: fine not exceeding RM10 million.
In relation to strategic items or unlisted items other than arms or related material, where the act is done with the intent to unlawfully export, transship, or bring in transit such items without a special permit or with knowledge that the export, transshipment, or bringing in transit of such strategic items without a special permit is unlawful.	Individual: imprisonment for a term not exceeding ten years or with a fine not exceeding RM10 million or with both; Corporation: fine not exceeding RM20 million.
In relation to strategic items or unlisted items other than arms or related material, where the act is done without the intent to unlawfully export, transship, or bring in transit such items without a special permit or without knowledge that the export, transshipment, or bringing in transit of such strategic items without a special permit is unlawful.	Individual: imprisonment for a term not exceeding five years or with a fine not exceeding RM5 million or with both; Corporation: fine not exceeding RM10 million.

The STA also provides that the act of brokering any strategic items without being registered as a broker under the STA shall constitute offenses and shall be liable on conviction to the following penalties:

Prohibited Activity	**Penalty**
In relation to strategic items or unlisted items that are arms or related material, where death is the result of the act:	• Individual: death or imprisonment for natural life; • Corporation: a minimum fine of RM30 million.
In relation to strategic items or unlisted items that are arms or related material, in any other case where death is not the result of the act:	• Individual: imprisonment for a term not exceeding ten years or with a fine not exceeding RM10 million or with both; • Corporation: fine not exceeding RM20 million.
In relation to strategic items or unlisted items other than arms or related material	• Individual: imprisonment for a term exceeding five years or with a fine not exceeding RM5 million or with both; • Corporation: fine not exceeding RM10 million.

In addition, the CWCA provides that any person who commits the following prohibited activities shall be liable for the following penalties:

Prohibited Activity	Penalty
Export of Schedule 1 chemicals except for the Specified Purposes	Fine not exceeding RM150,000 or imprisonment for a term not exceeding seven years or both.
Export of Schedule 2 chemicals	
Export of Schedule 3 chemicals without an end-user certificate	Fine not exceeding RM100,000 or imprisonment for a term not exceeding five years or both.

Where any offense against the CWCA has been committed by a body corporate, any person who at the time of the commission of the offense was a director, manager, secretary, or other similar officer of the body corporate or was purporting to act in any such capacity, or was in any manner or to any extent responsible for the management of any of the affairs of such body corporate, or was assisting in such management, shall also be guilty of that offense unless the person proves that the offense was committed without their knowledge, consent, or connivance and that the person exercised all such due diligence to prevent the commission of the offenses as they thought to have exercised, having regard to the nature of theit functions in that capacity and to all the circumstances.

Please note that the list of prohibited activities outlined earlier is non-exhaustive. Other prohibited activities, and their penalties, may be found in the CA, and in other applicable statutes and their subsidiary legislation.

(b) Voluntary Disclosure Programme

There is no voluntary disclosure program currently in place under the STA.

On December 31, 2021, the Malaysian Customs introduced a temporary Voluntary Disclosure and Amnesty Program (“VA Program”). The VA Program was launched on January 1, 2022, and ended on September 30, 2022.

The VA Program seeks to encourage taxpayers to come forward and voluntarily declare any indirect taxes, duties, or levies that have been underpaid or erroneously reported, as well as to voluntarily settle any outstanding debts due and owing to Malaysian Customs.

The VA Program is divided into two categories:

1. Voluntary Disclosure Programme—this covers any duty/tax/levy/penalty/surcharge liabilities (“Customs Debt”) that have arisen and remain outstanding on or before October 31, 2021. For the avoidance of doubt, any Customs Debt that is being or has

been investigated by the Enforcement Division of Malaysian Customs, and companies/individuals who have been approved for duty/tax/levy remissions by the Ministry of Finance are excluded from this program.

2. Amnesty Programme—this covers any offenses committed by a company/individual where such offenses were discovered by Malaysian Customs and for which a Bill of Demand has been issued or will be issued.

The incentives offered by Malaysian Customs under the VA Program include a remission of penalty/surcharge of up to 100 percent, and no audit will be conducted on applications approved during the program except where fraud has been proven.

23.9 Enforcement and Developments

Apart from encouraging traders to practice self-compliance methods (e.g., through the ICP) and having audit practices in place, Malaysia also continuously ensures that the export requirements are satisfied by exporters through an active awareness and educational program, where the STS division of MITI regularly conducts seminars to educate businesses on compliance with strategic trade regulations and/or export controls.

In respect of enforcement under the Customs Act, the case of *Acedeck Sdn Bhd v. The Customs Appeal Tribunal* [2020] 1 LNS 209 is highlighted as follows:

> March 2020: a High Court in Malaysia decided in favour of the Malaysian Customs (more specifically, the Customs Appeal Tribunal) against a local company engaged in the export of sawn timbers that did not possess a legitimate export license and had instead borrowed a license from a third-party exporting company, under the pretext that it was recognised practice in the timber industry. Without an export license of its own, the local company was found to have underpaid the tax due and was ordered to settle the outstanding amount accordingly with the Malaysian Customs.

In terms of export controls pursuant to the STA and CWCA, there have been no relevant published cases in respect of noncompliances with the STA and the CWCA.

23.10 Special Topics

The authority to issue orders to give effect to UNSC resolutions lies with the Minister of Home Affairs (MOHA), pursuant to the powers granted under the AMLA.

MOHA is empowered under the AMLA to, among others, declare individuals and entities whom the MOHA is satisfied to have knowingly committed, attempted to commit, participated in committing, or facilitated the commission of a terrorist act or is knowingly acting on behalf of, at the direction of, or in association with such individuals or entities, to be "specified entities." Currently, only one order has been made under the AMLA that recognizes the entities specified in UNSC's 1267 List and 1988 List as specified entities.

Under the AMLA, Malaysian citizens and body corporates incorporated in Malaysia are prohibited from conducting certain acts relating to specified entities, including knowingly providing or making available property or financial services to the specified entities. The penalty for contravening this requirement is a fine not exceeding RM3 million, or imprisonment for a term not exceeding five years, or both.

Other than UNSC resolutions, MOHA is also empowered to maintain a domestic sanctions list by way of an order published in the *Gazette*, where, as at the time of writing, the latest order published is the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities (Declaration of Specified Entities and Reporting Requirements) (Amendment) Order 2022, which came into force on April 25, 2022.

---

1. Kuok Yew Chen, Partner, Christopher & Lee Ong; Tracy Wong, Partner, Christopher & Lee Ong.

24

Export Controls and Economic Sanction in Mexico

Turenna Ramirez Ortiz[1]

24.1 Overview

(a) What Is Regulated?

Export Controls were incorporated into the Mexican regulatory framework almost 20 years ago. Initially, this concept was introduced through various specific agreements published in the Federal Official Gazette of Mexico, which established a series of requirements necessary for the export of goods that could be used to manufacture and promote conventional weapons and/or weapons of mass destruction.

In addition to the preceding, the "General Export Control Agreement"[2] was published in the Federal Official Gazette on June 16, 2011, and amended on December 13, 2011; June 7, 2012; October 22, 2012; February 8, 2013; March 13, 2014; and February 9, 2016, all of which likewise were published in the Federal Official Gazette, in order to implement Mexico's accession to the Wassenaar Arrangement.

Thus, by way of the General Export Control Agreement published on June 16, 2011, and its subsequent amendments, the Mexican government prescribed that the export of ammunition, software, technology, equipment, materials, software, precursor chemicals, and any other dual-use goods that could be intended for the manufacture or composition of weapons, is

subject to the issuance of prior export licenses by the Mexican Ministry of Economy, specifically by the General Directorate for Foreign Trade.

(b) Where to Find the Regulations

The regulatory framework for export controls in Mexico can be found in various statutory/regulatory instruments and publications of the Mexican government.

The General Export Control Agreement and its subsequent amendments can be found on the website: https://www.snice.gob.mx/cs/avi/snice/control_exportaciones.html.

Likewise, the website of the Mexican Chamber of Deputies can be very useful in finding all the laws and regulations related to export controls: http://www.diputados.gob.mx/LeyesBiblio/index.htm.

Finally, the Mexican Ministry of Economy has a website dedicated to export controls and all its forms and procedures. This site includes useful information aimed at explaining the steps to follow in detail: http://www.siicex.gob.mx/portalSiicex/CONTROL%20DE%20EXPORTACIONES/inicio.html.

(c) Who Is the Regulator?

Pursuant to Mexican law, the bodies responsible in the first place for supervising and monitoring compliance with the export control measures are the Ministry of Economy and the Tax Administration Service.

The Ministry of Economy, through its various departments, is the body in charge of determining what types of goods require an export permit, in accordance with the General Export Control Agreement published in the Federal Official Gazette on June 16, 2011, and its subsequent amendments.

Likewise, the Ministry of Economy is the competent export permit issuing authority. It receives and analyzes the permit applications submitted by exporters seeking to export goods and related technical data, listed in the General Export Control Agreement. The specific entities within the Ministry of Economy charged with this responsibility are the General Directorate for Foreign Trade; the Directorate of Export Control; and the Committee for the Control of Exports of Dual-Use Goods, Software and Technologies.

It is important to note that in addition to the export permits provided for in the General Export Control Agreement, there are other permits determined by other Mexican authorities, such as the Ministry of National Defense, the Ministry of Energy, the Ministry of Environment and Natural Resources, among others.

Once the corresponding export permit has been obtained, it is important to note that the authority in charge of carrying out the customs clearance of the goods is the Tax Administration Service, which requires the Mexican exporter to have a permit issued by the Ministry of Economy prior to exporting the goods in question and will be in charge of imposing sanctions in the event exports are carried out without the required permit.

(d) How to Get a License

In order to obtain an export permit, Mexican legislation and regulations establish a series of steps that the applicant must follow. To obtain an export permit required by the General Export Control Agreement, the first requirement prescribed by Mexican legislation is that the exporter must have an approved End-User/End-Use Statement. This Statement is obtained by filling out a form as prescribed by the Ministry of Economy, which includes general information on the exporter; the exporter's legal representative; information related to the final user to whom the goods are destined; the end user's business activity and address; and the country of export.

Once this Statement is submitted, the Ministry of Economy has ten business days to approve or reject the Statement. The ten-day period may be extended up to 60 business days in case the authority requires more time or information to make a decision on the Statement.

When no reliable information is presented, or when the requirements of the authority are not adequately met, the Ministry of Economy will reject the End-User/End-Use Statement and a fresh application must be submitted.

The Ministry of Economy provides a blank End-User/End-Use Statement on its website at https://www.gob.mx/se/acciones-y-programas/se-03-080-manifestacion-de-uso-y-usuario-final-para-obtener-el-permiso-previo-de-exportacion-de-armas-convencionales-bienes-de-uso-dual.

Once an approved End-User/End-Use Statement is obtained, exporters must request from the Ministry of Economy an export permit known as a Prior Export Control Permit, which will be granted or rejected within 15 business days from the business day following the date of its submission.

In order to obtain the permit, the applicant must present certain information to the Mexican authority, including the following:

- Product to be exported, indicating whether the product is new or used.
- Export regime
- Regime classification
- Description of goods
- Tariff item
- Amount and value of the invoice in dollars
- Unit of measure
- Specific use of the goods
- Export justification and business purpose.

Once this information has been declared, the applicant must attach the previously obtained End-User/End-Use Statement to the Prior Export Control Permit.

Having carried out the preceding steps, and if there are no irregularities in the information provided by the applicant, the Mexican authority issues its resolution granting the Prior Export Control Permit so that the interested party can undertake the corresponding export.

It is important to mention that the validity period of the Prior Export Control Permits in question shall be up to one year, which can be extended for an equal period, as long as all the authorization criteria continue to be met.

However, it is of the utmost importance to remember that in addition to the Prior Export Control Permits stipulated in the General Export Control Agreement and its amendments, there are other “Regulatory Agreements” within the Mexican legal framework that also establish the need to process prior export permits for various goods.

Thus, in order to obtain such permits, a procedure similar to the one just described must be followed before the competent authorities.

It should be noted that the Regulatory Agreements that also prescribe prior permits for the export of certain goods, are:

- The Agreement establishing the classification and coding of goods whose import or export is subject to regulation by the Ministry of National Defense.[3]
- The Agreement establishing the classification and coding of goods whose import and export are subject to regulation by the agencies that form the Inter-secretarial Commission for the Control of the Process and Use of Pesticides, Fertilizers and Toxic Substances.[4]
- The Agreement establishing the classification and coding of goods whose import and export is subject to prior authorization by the Ministry of Energy.[5]
- The Agreement establishing the classification and coding of goods whose import, export, entrance, or exit is subject to sanitary regulation by the Ministry of Health.[6]

(e) Key Websites

The key websites for locating the Mexican laws and regulations related to export control are the following:

- The Mexican Ministry of Economy: https://www.gob.mx/se/
- The National Foreign Trade Information Service: https://www.snice.gob.mx/
- The General Export Control Agreement: http://www.diariooficial.gob.mx/nota_detalle.php?codigo=5672276&fecha=24/11/2022#gsc.tab=0
- The Directorate of Export Control of the Ministry of Economy of Mexico: http://www.siicex.gob.mx/portalSiicex/CONTROL%20DE%20EXPORTACIONES/inicio.html

24.2 Structure of the Laws and Regulations

The Mexican legal framework for export controls consists of a series of provisions and regulations that should be read and interpreted together. This national legal framework implements various international treaties and agreements to which Mexico is party. Therefore, a correct analysis of the provisions governing Mexico's export control regime requires an

understanding of the international instruments the regime is designed to implement.

(a) International Treaties

As noted, Mexico has signed a number of international treaties related to export controls. It is important to mention that these treaties are commonly used for interpretive guidance on the national regulatory framework. In particular, the following international treaties related to export control have been signed by Mexico:

1. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies
2. The Treaty on Non-Proliferation of Nuclear Weapons
3. The Amendment to the Convention on the Physical Protection of Nuclear Material
4. The Nuclear Suppliers Group
5. The Zangger Committee
6. The Australia Group
7. The Missile Technology Control Regime (pending)
8. The Nuclear Security Convention

(b) Mexico National Laws and Regulations on Export Controls

Mexican export controls depend mostly on various secondary legislation that have their origin in the Mexican Political Constitution. In this regard, it is worth mentioning that Article 131 of the Federal Constitution states that the Executive Branch of the Federation has the power to increase, decrease, or eliminate export and import tariff fees, and to restrict and prohibit imports and exports. These powers are exercised through the Foreign Trade Law and its Regulation.

Thus, the Foreign Trade Law clearly stipulates that nontariff regulatory and restrictive measures may be imposed on the export of goods in accordance with the international treaties or agreements to which Mexico is a party. This is further supported by several articles of the regulations adopted under the aforementioned law.[7]

Similarly, the Foreign Trade Law[8] itself contemplates that such goods subject to nontariff restrictions or regulations (such as the Prior Export

Control Permit discussed) shall be identified in terms of their tariff classification and nomenclature, in accordance with the Tariff of the General Import and Export Tax Law.

For its part, the Mexican Customs Law[9] expands on the stipulations of the Foreign Trade Law by prescribing that, when exporting goods, interested parties must comply with any and all of the nontariff restrictions or regulations that apply to the goods. In this way, we can see that Mexican Export Controls are based on the Political Constitution of the United Mexican States, as well as on the Foreign Trade Law, the Customs Law, and their corresponding regulations. However, while such laws provide for the possibility of determining export control measures, in the Mexican system, these measures are determined by means of general Agreements published in the Federal Official Gazette by the Ministry of Economy and other agencies. So, it is through the General Export Control Agreement published on June 16, 2011, and its subsequent amendments, that the corresponding export controls are concretely established.

It should be noted that, in addition to the Agreement referred to in the previous paragraph and as indicated in Section 24.1 of this chapter, the Mexican legal framework also has other instruments, such as various regulatory agreements, that provide for additional export control mechanisms for specific goods.

(c) Controlled Lists

The lists of goods that are subject to export controls are found in the General Export Control Agreement and its corresponding amendments, as well as the Regulatory Agreements. It should be noted that these lists are divided into various items, as follows:

- List corresponding to dual-use goods (Annex I to the General Export Control Agreement dated June 11, 2011, and its amendments);
- List of ammunition and weapons (Annex II to the General Export Control Agreement dated June 11, 2011, and its amendments);
- List of software and technology (Annex III to the General Export Control Agreement dated June 11, 2011, and its amendments);
- List of dual-use equipment, materials, and software in the nuclear field and related technology (Annex VI to the General Export Control Agreement dated June 11, 2011, and its amendments);

- Control list for precursor chemical substances, facilities and equipment for manufacturing dual-use chemical substances and technology and associated information systems, dual-use biological equipment and technology and associated information systems, biological agents, plant pathogens, and animal pathogens (Annex VII to the Agreement dated June 11, 2011 and its amendments);
- List of the Agreement establishing the classification and coding of goods whose import or export is subject to regulation by the Ministry of National Defense, published in the Federal Official Gazette on June 30, 2007;
- List of the Agreement establishing the classification and coding of goods whose import and export are subject to regulation by the agencies that form the Inter-secretarial Commission for the Control of the Process and Use of Pesticides, Fertilizers and Toxic Substances, published in the Federal Official Gazette on May 26, 2008;
- List of the Agreement establishing the classification and coding of goods whose import and export is subject to prior authorization by the Ministry of Energy, published in the Federal Official Gazette on June 30, 2007;
- List of the Agreement establishing the classification and coding of goods whose import, export, entrance, or exit is subject to sanitary regulation by the Ministry of Health, published in the Federal Official Gazette on September 27, 2007.

24.3 What Is Regulated: Scope of the Regulations

The Mexican Export Control system controls trade in goods covered by the Agreements discussed in the previous section. This includes conventional weapons, their parts and components, dual-use goods, software, and technologies subject to use in the manufacture and proliferation of conventional weapons and weapons of mass destruction, as well as their parts and components.

Goods are also subject to export controls when (1) the exporter has been informed by the competent Mexican authorities that the goods may be subject to division or could be used for military end-use or be destined in whole or in part to activities related to the proliferation of weapons, or (2) when the acquiring country or the country of final destination is subject to

an embargo by a resolution of the United Nations Security Council, or (3) where the exporter has been informed by the competent authorities that the goods to be exported may be destined in whole or in part to military use. Mexico's sanctions regime is discussed in greater detail in section 24.11.

24.4 Who Is Regulated

According to the Mexican regulatory framework, any individual who intends to export a good, input, or item regulated by the Agreements discussed previously must observe and comply with the requirements of the export control system. Notwithstanding this, it is important to note that in accordance with national provisions, among others, the following are exempted from the formalities related to export control:

- Goods to be used by the Mexican government in foreign maneuvers or missions for humanitarian, peacekeeping, and peace support operations.
- Goods whose final destination is a state that has an agreement with Mexico for the reciprocal recognition of the export control system.
- Goods sent by Mexican companies to the United States of America and Canada.
- Subject to certain exceptions, minimum technology necessary for the installation, operation, maintenance, and repair of uncontrolled materials.
- Software in the public domain or available to the general public.

24.5 Classification

(a) Classification of Dual-Use Items

According to the General Export Control Agreement, dual-use goods are subclassified into several categories as follows:

Category 1: Special materials and related equipment
Category 2: Processed materials
Category 3: Electronics
Category 4: Computers

Category 5: Telecommunications
Category 6: Sensors and lasers
Category 7: Navigation and avionics
Category 8: Navy
Category 9: Aerospace and propulsion

It should be noted that each of the categories mentioned here is also made up of different groups in which the goods subject to the corresponding export permits are specified. In addition, the aforementioned Agreement also has a list of nuclear and related technology dual-use equipment, materials, and software that are subject to a prior export permit in terms of the lists developed in "The Nuclear Suppliers Group," and a control list for precursor chemical substances, facilities, and equipment for manufacturing dual-use chemical substances and technology and associated information systems, dual-use biological equipment and technology and associated information systems, biological agents, plant pathogens, and animal pathogens, subject to prior export permit, under the terms of the lists developed in the Australian Group.

As in other country lists, in Mexico's dual-use goods classification lists, the goods in question can be identified both by their description and by their tariff classification, so exporters will be able to clearly verify whether or not a specific good is subject to prior export permits in accordance with Mexican export control policies.

The lists mentioned in this section can be viewed at http://www.diariooficial.gob.mx/nota_detalle.php?codigo=5672276&fecha=24/11/2022#gsc.tab=0.

(b) Classification of Military Items

In relation to military goods, the list in question is specifically included in the Regulatory Agreement named "Agreement Establishing the Classification and Coding of Goods Whose Import or Export Is Subject to Regulation by the Ministry of National Defense" (hereinafter the National Defense Agreement) and its amendments published on October 6, 2014, and January 13, 2016. (https://www.dof.gob.mx/nota_detalle.php?codigo=5608886&fecha=27/12/2020#gsc.tab=0)

This list includes goods such as tanks and other armored combat vehicles, planes, helicopters, landing gear, air combat simulators, warships,

military grade lasers, rocket launchers, flamethrowers, grenade launchers, torpedo launchers, cannons, and other goods.

24.6 General Prohibitions/Restrictions/Requirements

As indicated throughout this chapter, the objective of Mexico's export control system is that exporters who intend to export various goods that, due to their use, purpose, or composition could be used to manufacture and promote conventional weapons and/or weapons of mass destruction, must first obtain a Prior Export Control Permit from the Ministry of Economy or from any other agency as required by Mexican regulations.

24.7 Licensing/Reasons For Control

(a) Types of Export Control Licenses and Permits for Dual-Use Items

Mexican export permits can be divided into those set through the General Export Control Agreement and those set by the Regulatory Agreements issued by authorities other than the Ministry of Economy. As already explained, the permits issued in accordance with the General Export Control Agreement are issued for a period of one year, which can be extended. With regard to the permits issued under the Regulatory Agreements, they can also be issued for a specific period, and, on occasion, depending on the concerned good, can be issued on a specific-shipment basis.

(b) Import and Export Licenses for Military Items

The National Defense Agreement specifically determines which goods to be imported to or exported from Mexico shall comply with the permit procedure before the Ministry of National Defense. This permit procedure stipulates that those interested in importing or exporting the goods referred to in the Agreement must submit an application for an ordinary permit for import and/or export of military goods before the Ministry of National

Defense. The application must contain, among other things, the following information:

- Information on the foreign supplier where the goods are imported
- Information on the end user to which the export is destined
- Information on the importer or exporter
- Information that demonstrates why the import or export operation is being carried out

(c) Independent Expert Examination

It is common that the Mexican authorities and exporters face situations in which, due to the complexity or specific characteristics of the goods to be exported, there is no full knowledge as to whether they are or are not subject to export controls. In this case, the General Export Control Agreement provides for the possibility of a consultation before the Committee for the Control of Exports of Dual-Use Goods, Software and Technologies, which depends on the Ministry of Economy.

It should be noted that this consultation can be made at the request of the exporter, or at the request of the authorities. Once the consultation is presented, the Committee deliberates and decides on the principle of majority vote.

24.8 Penalties, Enforcement, and Voluntary Disclosures

The failure to comply with the requirement to obtain an export permit is a violation of Mexican law. It is important to note that the Mexican regulatory framework also stipulates that once an export permit is granted, it may be canceled in the following cases:

- When the exporter violates the obligations established in the permit
- When the initial conditions under which the permit was granted are altered
- When the End Use Statement or the permit application contains an omission, alteration, or falsification
- When the exporter lacks the documentation that covers the export of the regulated goods, when it presents inconsistencies with what was declared in the application, or when it is verified that the regulated

goods were not exported to the final destination provided for in the permit
- When the Ministry of Economy observes that the exports were not destined to the end use or the destination provided in the application
- When the fiscal address declared by the exporter is nonexistent
- When the Mexican authorities determine that the name or fiscal address of the recipient or buyer abroad is false, inexistent, or untraceable.

(a) Administrative Penalties

The following administrative monetary penalties are provided for under Articles 178 and 185 of the Customs Law:[10]

- For failing to have the required export permit at the time of customs clearance: A fine of 70 percent to 100 percent of the commercial value of the goods to be exported may be imposed.
- For omitting to transmit, or transmitting in an untimely manner, the document that proves the processing of the export permit: A fine of $3,730 to $5,590 Mexican pesos (a fine of approximately between $170 and $270 U.S. dollars).
- Similarly, if the omission is proven prior to the export of the goods, the Mexican customs authority may place an embargo on the goods to be exported.

(b) Criminal Penalties

The failure to comply with export controls in Mexico not only results in the imposition of administrative fines. The Federal Fiscal Code, in article 102,[11] section II, and article 104, section IV, prescribes among other things that exporting or importing goods without the necessary permits constitutes the federal crime of smuggling, which is punishable by three to six years in prison.[12]

(c) Voluntary or Self-Disclosure

The Mexican legislation allows entities or individuals to carry out their obligations spontaneously and thus prevent the updating of the fines

stipulated by law. Derived from this, it is recommended that in case of having committed the infringement of not presenting the Prior Export Control Permit for the export of goods, the individual has the opportunity to correct spontaneously and process such export permit (before the authorities trigger an official procedure against the individual).

It should be noted that the spontaneous fulfillment of such an obligation can be seen as a factor of goodwill and mitigation before any action of criminal or administrative nature by the Mexican authority is initiated.

24.9 Mexican Encryption Controls

Regarding export controls on cryptographic goods, the Mexican regulatory framework is not as robust or as specific as the legislations of some other countries. This type of technology is regulated by the General Export Control Agreement, specifically, in the list corresponding to dual-use goods in Categories 4 “Computers” and 5 “Systems, equipment and components.” The export license process regarding these technologies is the same as other goods controlled under the General Export Control Agreement. Likewise, the same penalties for noncompliance apply.

24.10 Special Topics

(a) Practical Issues Related to Export Control Clearance

Although export control is regulated consistently at the national level, due to the significant number of Customs offices in the country, there may be local variations in the application and interpretation of the rules. As such, it is recommended that prior to the export that exporters have sufficient records proving the reason why such goods are subject to the export permit.

It is also very important that exporters be mindful of the expiration dates of their export permits, and whether the circumstances in force at the time of obtaining it continue. The preceding would allow a timely request of the renewal or extension of the corresponding permit before the Mexican authorities.

(b) Recordkeeping

According to Mexican laws, individuals or companies who must obtain any kind of prior export permit shall have in their custody records confirming the fulfillment of their obligations for a period of five years. This considers that the Mexican authorities have an equal period of time (five years) to subject individuals to verification procedures or audits of compliance regarding export control compliance.

(c) Intangible Transfer of Technical Information

The General Export Control Agreement prescribes that the export of software, technologies, or dual-use goods, including transmissions containing data processing programs or data delivery telecommunications by electronic means, fax, telephone, satellite transmission, or any other means of communication, susceptible to deviation, will be assimilated to any tangible export operation, and, therefore, the exporter is required to obtain a prior export permit from the Ministry of Economy. In other words, technical data related to export controlled goods is likewise export controlled.

(d) How to Be Compliant When Exporting to Mexico

First, it must be verified whether or not in order to export the goods in question to Mexico, compliance is required with an export control regime in the country of origin; if this is the case, the exporting entity shall apply for the corresponding license in accordance with the legislation applicable in that country. In view of this, and in accordance with Mexican laws, in order to import certain goods or merchandise, importers must comply with various regulations and nontariff restrictions, including import licenses. In this sense, before shipping goods to Mexico, importers and exporters should be aware of all the regulations and nontariff restrictions to which the good in question is subject.

It is generally recommended that, when exporting goods subject to export controls in Mexico, an analysis of national regulations should be carried out beforehand so that the import process is efficient and is not affected by the lack of compliance with a prior import permit requirement.

(e) How to Be Compliant When Exporting from Mexico

In order to carry out the export of goods from Mexican territory, the exporter must first carry out the tariff classification of the goods to be exported.

Once this classification has been made, a study will have to be conducted to verify whether the export of the mentioned good is subject to an export license requirement in accordance with Mexico's export control regime. If so, the exporter must apply for and obtain the appropriate permit according to the procedure described earlier in this chapter.

24.11 International Economic Sanctions

(a) Mexico and UN Security Council Sanctions

Mexico does not have a specific statutory instrument for the implementation of United Nations Security Council sanctions. That said, once a sanction is established by the Security Council, a presidential order is published in the Federal Official Gazette, and it thus forms part of the Mexican regulatory system. This is because, in accordance with Article 133 of the Political Constitution of the United Mexican States, all treaties signed by Mexico form part of its regulatory framework and must therefore be respected.

In addition, once the United Nations Security Council issues sanctions and they are published in the Federal Official Gazette, the Ministry of Foreign Affairs of Mexico publishes them on its website[13] and, as discussed in the following section, the Ministry of Economy incorporates them into a Restriction Measures Agreement.

(b) Mexico National Laws on Economic Sanctions and Sanctioned Parties Lists

Upon their publication in the Federal Official Gazette, the Mexican government carries out a series of measures to implement and monitor compliance with said sanctions. These measures include the publication of the "Agreement establishing measures to restrict the export or import of various goods to the indicated countries, entities, and individuals" (hereinafter Import/Export Restriction Agreement) published on November 29, 2012, which has been modified several times.

Through this Import/Export Restriction Agreement, Mexico issues a list of goods through which such exports are strictly prohibited to countries such as the Somali Democratic Republic, Islamic Republic of Afghanistan, Republic of Iraq, Democratic Republic of Congo, Republic of Sudan, and Democratic People's Republic of Korea (North Korea), among others.[14]

Under this Agreement, the Ministry of Economy summarizes the resolutions adopted by the United Nations Security Council, listing the states and individuals subject to sanctions and the scope of such sanctions.

These express prohibitions cannot be subject to export permits, failure to comply with this regulation implies the seizure of the intended products to be exported, as well as the cancellation of the exporter's registries, as a penalty of 100 percent of the value of the goods, Article 151, 176 III, 178 III of the Customs Law.

Mexico has not adopted the figure of deemed exports and has no controls of re-exports.

---

1. Turenna is the Managing Partner of the Mexico City office at Sánchez Devanny Eseverri Law Firm. She joined Sánchez Devanny to head the International Trade and Customs practice in 2009. She has more than 20 years of experience advising multinational and national companies on foreign trade and customs strategic planning, trade compliance, startups settings, customs official and preventive audits, international treaties, tariff and nontariff regulations, customs regimes, rules of origin, etc.

2. General Export Control Agreement by which the export of conventional weapons, their parts and components, dual-use goods, software and technologies susceptible to diversion for the manufacture and proliferation of conventional weapons and of weapons of mass destruction. *See* www.dof.gob.mx/2020/SEECO/SEECO_27122020_n5.pdf.

3. https://www.snice.gob.mx/cs/avi/snice/sedena.html.

4. https://www.snice.gob.mx/cs/avi/snice/cicoplafest.html.

5. http://www.siicex.gob.mx/portalSiicex/SICETECA/Acuerdos/Regulaciones/SENER/senerx.htm.

6. http://www.siicex.gob.mx/portalSiicex/SICETECA/Acuerdos/Regulaciones/SSA/SSAx.htm.

7. Articles 15 and 17 of the Foreign Trade Law: http://www.diputados.gob.mx/LeyesBiblio/pdf/28.pdf.

8. www.diputados.gob.mx/LeyesBiblio/pdf/LAdua.pdf.

9. Articles 36-A, II, and 56, www.diputados.gob.mx/LeyesBiblio/pdf/28.pdf.

10. www.diputados.gob.mx/LeyesBiblio/pdf/LAdua.pdf.

11. https://www.diputados.gob.mx/LeyesBiblio/pdf/CFF.pdf.

12. *Id.*

13. https://www.gob.mx/sre/es/archivo/acciones_y_programas.

14. https://www.snice.gob.mx/~oracle/SNICE_DOCS/TI_Embargos_PDF-Acuerdo-Embargos_20180615-20180615.pdf.

25

Export Controls in Russia[1]

Alexander Bychkov, Vladimir Efremov, and Andrey Gavrilov

25.1 Overview

(a) What Is Regulated?

Russian regulations on export controls were established about 30 years ago, and are based on international treaties aimed at combating terrorism and nonproliferation of weapons of mass destruction. Russian export control regulations have been constantly changing and developing in order to meet international trends and standards.

Russian export controls establish rules for Russian individuals and legal entities on international cooperation in the sphere of development and trade in products and technologies classified as dual-use and military items. Dual-use and military items include a wide range of goods and technologies that may be used for or in connection with the creation of weapons of mass destruction. The controlled items include results of intellectual activity, including IP rights, along with performance of works and provision of services. Russian export controls restrict the transfer of controlled items to any foreign persons and establish special procedures for Russian exporters for licensing export control operations, reporting and recordkeeping, as well as penalties for violation of such procedures.

(b) Where to Find the Regulations

Generally, all Russian laws and regulations are available on the official website of legal information in the Russian language at http://pravo.gov.ru/ips/.[2]

The Russian export control regulations are also placed on the website of the main governmental body responsible for export controls at www.fstec.ru.

Information on the Russian legislation is also available in legal databases provided by private companies (in English and Russian languages). The most popular among them are Consultant Plus (http://www.consultant.ru/) and Garant (http://www.garant.ru/).

(c) Who Is the Regulator?

The main Russian body is the Federal Service for Technical and Export Controls (the FSTEC). The FSTEC is responsible for (1) issuance of export control licenses, permits, official confirmation letters or "comfort" letters; (2) field (on-site) audits of Russian exporters/foreign trade participants; and (3) accreditation of test laboratories performing independent expert examination of dual-use goods and technologies. The central office of the FSTEC is located in Moscow. The FSTEC has seven territorial subdivisions located in Saint Petersburg (the North-Western Federal District), Rostov-on-Don (the Southern and North-Caucasian Federal District), Nizhny Novgorod (the Volga Federal District), Yekaterinburg (the Urals Federal District), Novosibirsk (the Siberian Federal District), and Khabarovsk (the Far Eastern Federal District).

The Federal Customs Service (official website: www.customs.ru)[3] is responsible for customs clearance and customs control over the controlled items at the customs border, including post-clearance customs control and customs audits.

The FSTEC and the Russian Ministry of Defense (the MoD) cooperate with a number of other Russian federal executive governmental bodies, including security, enforcement, and intelligence authorities that provide them with the relevant support and assistance in the sphere of export controls, including the performance of certain types of expert examination of controlled items and foreign trade transactions, participation in the export licensing procedures and approval, and so on (e.g., the Russian Federal Security Service, various governmental commissions, etc.).

Foreign trade in arms and military items is within the sphere of competence of the MoD, along with the following competent authorities:

- The Russian President—issues permits to import/export military items;
- The Commission for Military-Technical Cooperation—implements state policy;
- The Russian MoD—coordinates all foreign transactions with military items;
- The Federal Service for Military-Technical Cooperation—issues export licenses and official import/export permits for potentially controlled items.

Foreign trade in military items can be performed only by the following specifically authorized organizations:

- "Rosoboronexport" JSC—the main governmental corporation authorized to sell military equipment and technologies;
- State corporation "Rostechnologii"—authorized to advertise, exhibit, and market military items;
- Russian legal entities—developers/manufacturers of military products and technologies should be specifically authorized by the Russian president to perform foreign trade activity with certain types of military items (e.g., spare parts, technical documentation, provision of works and services, etc.).

(d) How to Get a License

Russian export controls apply to all Russian individuals and legal entities. In order to obtain an export control license and transfer dual-use items to a foreign person, a Russian seller (applicant) should prepare and execute an application for a license together with a standard set of documents, pay state duty, and apply to the FSTEC. Generally, it should be possible to apply with the FSTEC electronically, via the main web portal of governmental services at https://www.gosuslugi.ru/structure/10000001025. Practically, it is more preferable for the FSTEC to receive submissions on paper.

(e) Key Websites

FSTEC's website is available at www.fstec.ru and provides texts of regulations, export control licensing procedures, and controlled lists. All information is published in the Russian language only, however. A limited English version of the website is also available (http://fstec.ru/en/).

The MoD website is http://mil.ru/, and an English version is also available (http://eng.mil.ru/en/index.htm).[4]

25.2 Structure of the Laws and Regulations

(a) International Treaties

As mentioned earlier, Russia participates in a number of international treaties on export controls, and its national regulations are based on such treaties. In particular, Russia participates in the following:

- The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1995)
- The Treaty on Non-Proliferation of Nuclear Weapons (NPT, 1968)
- The Convention on Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (1993)
- The Convention on Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (1972)
- The Nuclear Suppliers Group (NSG)
- The Zangger Committee (ZC)
- The Missile Technology Control Regime (MTCR)

These treaties were incorporated into Russian national legislation.

Russia does not participate in the Australia Group, which is a multilateral export control regime (MECR).

(b) Russia and the Commonwealth of Independent States (CIS)

Russia is a party of the Commonwealth of Independent States (CIS). The member states of the CIS are Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, Ukraine, Armenia, Turkmenistan, and Uzbekistan. Ukraine has a rather uncertain status in the CIS. In 2014, the country

announced its intention to withdraw from the CIS. Although, so far, Ukraine has not applied for withdrawal, and the country has very limited participation in the work of the CIS. Each member state of the CIS has its own export control regulations, which are similar to Russian export control regulations.

(c) Russia and the Eurasian Economic Union (EAEU)

From January 1, 2015, Russia has been a member of the Eurasian Economic Union (EAEU), an international organization of regional economic integration. The EAEU is the successor of the Customs Union that was created in 2010 and included the member states of Russia, Belarus, and Kazakhstan. Currently, the EAEU includes the following member states: Russia, Belarus, Kazakhstan, Armenia, and Kyrgyzstan.

Among other integration aspects, the EAEU has a unified customs territory providing free movement of goods, works, and services between the EAEU member states (i.e., no customs borders and customs control). The EAEU member states still have their own (national) export control regulations, which have not been unified at the EAEU level. Therefore, transfer of controlled items between the EAEU member states would still be subject to general export control clearance procedures. At present, the EAEU member states are working on the unification of export control regulations, but the expected timelines are unknown.

(d) Russia as a Permanent Member of the UN Security Council

Russia is a permanent member of the UN Security Council. The UN Security Council has imposed a number of foreign trade sanctions restricting supplies of specific types of products, works, services, and technical support in the sphere of military cooperation and arms, dual-use items, nuclear items, as well as blocking accounts and the financing of transactions of designated persons and/or blacklisting designated persons (i.e., entry/transit ban). Russia traditionally does not itself go beyond the UN sanctions, except for the arms embargo imposed on Georgia in 2009 and the food embargo introduced in 2014 as a response to Ukraine-related sanctions. Russia’s foreign trade sanctions are imposed by presidential decrees based on Federal Law No. 281-FZ, dated December 30, 2006, On Special Economic Measures; Federal Law No. 164-FZ, dated December 8,

2003, On the Basics of State Regulation of Foreign Trade Activity; and Federal Law No. 127-FZ, dated June 4, 2018, On Measures (Countermeasures) in Response to Unfriendly Actions of the USA and (or) Other Foreign States. Currently, Russia applies the following resolutions of the UN Security Council, which constantly change:

- UN Resolutions No. 1388 (2002) and No. 1390 (2002) on Al-Qaida and the Taliban (Decree No. 393, dated April 17, 2002);
- UN Resolutions No. 1556 (2004) and No. 1591 (2005) on the Republic of Sudan (Decrees No. 1379, dated October 22, 2004; and No. 719, dated June 24, 2005);
- UN Resolution No. 1807 (2008) on Congo (Decree No. 1490, dated October 17, 2008);
- UN Resolution No. 1844 (2008) on Somali (Decree No. 516, dated April 24, 2010);
- UN Resolution No. 1907 (2009) on Eritrea (Decree No. 933, dated July 22, 2010);
- UN Resolutions No. 1970, No. 2009 (2011), and No. 1973 (2011) on Libya (Decree No. 1092, dated August 12, 2011; Decree No. 588, dated June 6, 2012; Decree No. 286, dated March 9, 2011);
- UN Resolutions No. 2127 (2013) and No. 2134 (2014) on the Central African Republic (CAR), implemented by Decree No. 626, dated September 10, 2014;
- UN Resolutions No. 1718 (2006), No. 2094 (2013), and No. 2270 (2016) on North Korea (Decree No. 665, dated May 27, 2007; Decree No. 871, dated December 2, 2013; and Decree No. 729 of December 29, 2016), etc.
- UN Resolution No. 2321 (2016) on North Korea (Presidential Decree No. 484, dated October 14, 2017)
- UN Resolution No. 2231 (2015) on Iran (Presidential Decree No. 109, dated March 11, 2016)

The consolidated list of individuals and organizations that are subject to the preceding listed sanctions is provided on the FSTEC website in the Russian language.[5]

(e) Russian National Laws and Regulations on Export Controls

Russian laws on export controls are primarily based on the Wassenaar Arrangement, but differ in some details. The main Russian laws on dual-use items include the following:

- Federal Law No. 183-FZ, On Export Controls, dated July 18, 1999 (the "Law on Export Controls"). This is the main legal act that establishes the basic principles of Russian export control and implements regulations on export control licensing and supervision.
- Governmental Decree No. 973, dated December 15, 2000, On Exportation and Importation of Nuclear Materials, Equipment, Special Non-Nuclear Materials and Relevant Technologies.
- Governmental Decree No. 447, dated June 7, 2001, On the Establishment of Regulations on Control over Foreign Trade Activity with Dual-Use Goods and Technologies That May Be Used for the Creation of Arms and Military Equipment.
- Governmental Decree No. 462, dated June 14, 2001, On the Establishment of Regulations on Performance of Control over Foreign Trade Activity with Dual-Use Equipment and Materials as Well as Relevant Technologies Applied in the Nuclear Sphere.
- Governmental Decree No. 294, dated April 16, 2001, On Establishment of Rules for State Expert Examination of Foreign Trade Transactions with Goods, Works, Services and Results of Intellectual Activity (IP Rights) Subject to Export Control.
- Governmental Decree No. 477, dated June 21, 2001, On the System of Independent Identification Expert Examination of Goods and Technologies Performed for the Purposes of Export Control.
- Governmental Decree No. 691, dated September 15, 2008, On Establishment of Regulations on Licensing Foreign Trade Operations with Goods, Works, Services and Results of Intellectual Activity (IP Rights) Subject to Export Control.

A separate set of regulations is applied to foreign trade in military items based on Federal Law No. 114-FZ ,dated July 19, 1998, On the Military-Technical Cooperation of Russia with Foreign States.

(f) Controlled Lists

Russian lists of dual-use and other controlled items are established by a number of presidential decrees. Currently Russia applies the following lists

of controlled dual-use and military items:

- The List of Dual-Use Items established by Governmental Decree No. 1299, dated 19 July 2022 (entered into force on July 22, 2022);
- The List of Nuclear Materials, Equipment and Special Non-Nuclear Materials and Relevant Technologies Subject to Export Control (Governmental Decree No. 1285, dated July 16, 2022, entered into force on July 19, 2022);
- The List of Equipment and Materials of Dual Use and Relevant Technologies Used in the Nuclear Sphere and Subject to Export Control (Governmental Decree No. 1286, dated July 16, 2022, entered into force on July 19, 2022);
- The List of Equipment, Materials and Technologies that Can Be Used for Creation of Missile Weapons and Are Subject to Export Control (Governmental Decree No. 1288, dated July 16, 2022, entered into force on July 19, 2022);
- The List of Chemicals, Equipment and Technologies that Can Be Used for Creation of Chemical Weapons and Are Subject to Export Control (Governmental Decree No. 1284, dated July 16, 2022, entered into force on July 19, 2022);
- The List of Microorganisms, Toxins, Equipment and Technologies Subject to Export Control (Governmental Decree No. 1287, dated July 16, 2022, entered into force on July 19, 2022).

Additionally, the List of Military Items was established by Presidential Decree No. 1062, dated September 10, 2005, Issues of Military and Technical Cooperation between Russia and Foreign States.

25.3 What Is Regulated: Scope of the Regulations

Pursuant to Section 1 of the Law on Export Controls, the controlled items may include raw materials, materials, equipment, scientific and technical information (i.e., technology), results of intellectual activity and IP rights, performance of works, provision of services that, by virtue of their specifics and peculiarities, can have a substantial impact on the creation of weapons of mass destruction, delivery means, other types of arms and military equipment. Thus the scope of items is very broad.

Russian export controls apply to any items falling under the lists of controlled items mentioned in Section 25.2(f). Exportation of such items from Russia would be subject to special export control clearance, that is, the exporter of record would need to obtain an export control license (or other type of authorization) issued by a competent body responsible for export control clearance of the particular products (for more details please refer to Section 25.4). In certain specific cases, the importation of dual-use products might also be subject to export control requirements (for example, for military items or sensitive items; for more details please see Sections 25.5 and 25.7).

Russian export controls also provide a "catchall" clause, when the Russian exporters of record must obtain an export control license for items that do not fall under any of the controlled lists, but the exporters understand that the end user will or could apply such items for military end-use purposes.

Russian export control requirements apply to any type of transfer of the controlled items to any foreign persons (i.e., individuals or legal entities), which may include any types of tangible and intangible transfer. This may include physical shipments of dual-use goods, including dual-use technology on documents and other fixed media (irrespective of the origin of goods/technology); hand carries by individuals; intangible transfers by means of electronic correspondence, intranet, electronic downloads, fax, telephone (if relevant controlled parts are read out or described), even via video conferencing, and so on.

If a product by its description, HS classification, technical characteristics, or purpose of use may potentially fall under Russian export control regulations, it must undergo special export control identification and testing in order to determine whether special export control clearance is required (i.e., export control license, permit, or end-use certificate issued by the FSTEC for the importation/exportation of the products). In order to avoid delays during customs clearance, or even penalties for violation of export control requirements, it is important to precisely determine whether items are controlled or not well in advance of their exportation/importation or transfer to foreign persons.

In order to determine whether a product or technology is subject to Russian export control and, if yes, what type of clearance is required (i.e.,

export license or export permit), the product should undergo a special state expert examination. Therefore, it is recommended to:

- determine whether the products in question are likely to fall under Russian dual-use export control regulations; and
- instruct your Russian counterpart to make the required arrangements and legal actions in order to comply with Russian export controls (i.e., perform the required expert examination, obtain permit documents, etc.).

25.4 Who Is Regulated

As mentioned in Section 23.3, Russian export control regulations must be observed by all Russian persons, which includes legal entities incorporated under the laws of the Russian Federation, as well as individuals who are Russian citizens or who have permanent residence in Russia, including those who are registered in Russia as private entrepreneurs.

25.5 Classification

(a) Classification of Dual-Use Items

The lists of controlled items provided in Section 25.2 (f) (except for military items) provide a general description of goods and their HS classification. HS codes are listed for information purposes only, so the exporter should mainly consider the description of goods/technologies and their technical characteristics.

The Dual-Use List is the main document on export controls and is very similar to the Wassenaar List but differs in some slight details. The Dual-Use List includes the following sections:

- Section 1 of the Dual-Use List (Categories 1–9):
  - Category 1 Special materials and related equipment and ammunition;
  - Category 2 Material processing items;
  - Category 3 Electronics;
  - Category 4 Computer equipment;

    - Category 5 Telecommunications and information security items;
    - Category 6 Sensors and lasers;
    - Category 7 Navigation and avionics;
    - Category 8 Marine items;
    - Category 9 Aviation-and-space industry.
- Sections 2 and 3: Sensitive and very sensitive items.
- Section 4: Items controlled for reasons of national security.
- Section 5: Controlled imports (e.g., radio-location products, aerial vehicles, riot control devices, industrial explosives, special protection equipment, etc.).
- Subcategories for each category—1 (systems, equipment and components), 2 (test, inspection and production items), 3 (materials), 4 (software), 5 (technology)—are equal to subcategories A, B, C, D, and F of the Wassenaar List.

Other lists of controlled items (i.e., on missile weapons, chemical and biological items) also provide descriptions and HS classifications.

(b) Classification of Military Items

Presidential Decree No. 1062 dated September 10, 2005, Issues of Military and Technical Cooperation between Russia and Foreign States, established the List of Military Items. Military items are listed in accordance with their description and designation. The list of military items provides broad classification of military items into the following sections:

- Tanks and other self-moving machines;
- Military vehicles;
- Military items for engineering supplies of the army;
- Planes, helicopters, and other flying apparatus of military application;
- Military marine equipment and submarine equipment, etc.;
- Arms/munitions, bombs and other military explosives, etc.

The military list includes machines/goods, parts/spare parts, technical documentation, and works/services. The military list is not classified by HS codes, that is, the exporter should instead refer to the description of goods/technologies and purposes of their application and end use. Both imports and exports of military items are controlled.

25.6 General Prohibitions/Restrictions/Requirements

Every case of exportation or transfer of controlled items by Russian companies and individuals to any foreign persons must pass through the export control formalities. Otherwise the Russian exporter may face negative consequences related to law-enforcement activities performed by the competent governmental bodies and/or penalties for violation of export control regulations. This may happen even with respect to products/services/information that do not fall under export control requirements but could potentially be controlled.

25.7 Licensing/Reasons For Control

(a) Types of Export Control Licenses and Permits for Dual-Use Items

There are two types of export control licenses: (1) general license and (2) one-shot license. General licenses are considered in Section 25.8.

A one-shot license is issued for one contract and an exact quantity of controlled items. A one-shot license indicates the country of final destination, the shipper (seller), and the buyer (recipient). The issuance of one-shot licenses requires a preliminary state expert examination of the transaction by the FSTEC. The maximum validity term of a license is one year and may be extended for an additional one-year term.

In addition to export control licenses, depending on the specifics of a particular transaction, any of the following permit documents may be required: export permit, re-export permit, and end-user import certificate.

(b) Export Control Licensing Procedure

The following documents should be submitted by an applicant to the FSTEC when applying for a license:[6]

- A written application together with a cover letter with the details of the applicant (name, address, etc.);
- Document providing precise information on the controlled items with attached copies of documents (if needed), confirming their technical

characteristics and area of application;

- Cover letter indicating the type of license requested, as well as the full name, location, main state registration number of the legal entity or main state registration number of an individual entrepreneur, tax identification number;
- Copy of the foreign trade contract including all addenda and appendices;
- Document confirming whether the controlled products or technologies constitute or contain information related to state secrets;
- Document issued by the Russian Federal Service for Intellectual Property (Rospatent) confirming that the contemplated transaction will not include or relate to any IP rights belonging to the state;
- Written obligations of the foreign recipient (end user) that the controlled products or technologies will not be used for illegal purposes (i.e., support of terrorism, etc.). Relevant special wording could be alternatively included in the foreign trade contract with the end user. In certain cases, the FSTEC could request the applicant to provide relevant obligations to be covered by official letters of the authorized state bodies of the end user—or certified by such state bodies;
- Applicant's constituent documents;
- Copies of contracts between the applicant and the manufacturer (owner) of the controlled goods or technologies (if the applicant is not the manufacturer/owner);
- Document confirming payment of the state duty (RUB 7,500, approx. US$125) (due to the constant fluctuations in the exchange rate, the equivalent amounts in U.S. dollars indicated in this chapter may differ on a given date);
- Other documents may be required depending on the type of transaction or type of products or technologies (e.g., for nuclear materials—documents confirming their ownership, for technology—documents describing the technology).

A one-shot export license should be issued within 12 business days after the receipt of the application by the FSTEC. If the set of documents is incomplete, the FSTEC will request the applicant to provide the missing documentation. In this case, consideration of the application will be suspended.

A general export license should be issued within six business days after the receipt of the application by the FSTEC. Issuance of general export licenses requires the prior approval of the Russian government. The total period for preparing the draft decisions on the issuance of general export licenses, their approval, and consideration by the Russian government can be up to 60 days.

(c) Import and Export Licenses for Military Items

Licenses may be issued only to Russian manufacturers/developers of military items that have special authorization to perform foreign trade activity with certain types of military items. In order to obtain authorization, a Russian developer/manufacturer of military items must file an application form with the Russian government enclosing:

- Accounting and audit reports;
- Constituent documents (including certificate of tax registration, statistics letter, share register for joint stock companies, etc.);
- Recommendation letters issued by the Ministry of Justice, Ministry of Foreign Affairs, Ministry of Defense, Federal Security Service, External Intelligence Service, etc.;
- Documents confirming that the applicant has special internal departments dealing with:
  - performance of the authorized activities, and
  - control and security of the authorized activities.

Import and export licenses are issued by the Federal Service for Military and Technical Cooperation. Licenses are issued for the term of the contract. Issuance of military licenses must be coordinated with various Russian governmental authorities including the MoD.

(d) Export Permits and Independent Expert Examination

Export licenses, export permits, or “comfort” letters should be provided to the Russian customs authorities during customs clearance of the exported goods. The Russian customs authorities perform identification of the controlled items against the permit documents issued by the FSTEC during their customs clearance and allow exportation (and in certain specific cases, importation).

Very often the Russian exporters and the customs authorities cannot exactly know whether the products in question are subject to export controls or not. In order to give a precise response and avoid any related compliance issues, the Russian exporter of record may arrange a special export control expert examination of such products. The examination could be performed by the FSTEC on a free of charge basis (timeline: 30 calendar days).

The exporter may also engage an independent test laboratory accredited with the FSTEC. The list of independent test laboratories is provided on the FSTEC website.[7] Independent test laboratories charge fees for their services but the main advantage of using them is the short time required for the expert examination. Expert reports issued by independent laboratories and confirming that products do not require an export control license should be accepted by the Russian customs authorities.

25.8 General Licenses/License Exceptions

(a) General License

Issuance of general licenses is governed by Section 19 of the Law on Export Controls. A general license is issued for a particular type of controlled items, for a maximum possible quantity of controlled items. A general license indicates the country of final destination, but does not indicate the buyer (recipient). General licenses are available only for Russian legal entities that have established an *internal program for export control* and obtained special state accreditation with the FSTEC. Issuance of general licenses requires the prior approval of the Russian government. General licenses are issued for an unlimited term (depending on the quantity/volume of items).

The establishment of special internal programs on export controls is governed by Article 15 of the Russian Law on Export Controls and allows one to facilitate export control clearance formalities. Internal programs can be established by any Russian legal entity. These programs are mandatory for organizations involved in scientific and manufacturing activities related to meeting state needs in the sphere of national defense capabilities and systematically receiving income from foreign trade operations with

controlled items and technologies. An intercompany program must be accredited by the FSTEC.

(b) License Exceptions

An export control license is not required in the following cases:

1. Temporary exports of controlled goods and technologies without their transfer to any foreign persons, for example, for exhibition purposes or for internal use by the Russian exporter of record; however, this still requires prior approval of the Governmental Commission on Export Controls;
2. Imports and exports of controlled goods designated for the repair or replacement of equipment that was earlier imported into Russia, if such imports and exports are set forth under contractual guarantee obligations;
3. Exports of foreign controlled items that were earlier imported into Russia, if such items are returned back to the initial owner;
4. Exports of controlled products designated for technical maintenance or repair of Russian sea vessels or aircraft.

Any of these transactions should be approved by the FSTEC.

25.9 Penalties, Enforcement, and Voluntary Disclosures

(a) Administrative Penalties

Administrative penalties are set forth in the Russian Code on Administrative Violations (the “Administrative Code”) and are applied to Russian legal entities or individuals (usually the responsible managers of Russian legal entities).

Part 1 of Article 14.20 of the Administrative Code establishes penalties for the performance of foreign trade activities with dual-use items without special authorization (i.e., license or permit, etc.), or in violation of special conditions set forth by an authorization, as well as when an authorization was obtained illegally (for example, on the basis of invalid documents or inaccurate information). The penalties are in the form of a fine amounting to the price of products involved in the violation, with or without their

confiscation. Part 2 of Article 14.20 establishes penalties for the improper or inaccurate recordkeeping on export control operations and are in the form of a fine for the responsible managers of up to RUB 2,000 (approx. US$30) and for legal entities of up to RUB 20,000 (approx. US$300).

The period of the statute of limitations for this type of violation is one year.

(b) Criminal Penalties

Article 189 of the Russian Criminal Code establishes penalties for deliberate illegal exportation from Russia or transfer to a foreign company or its representative of raw materials, equipment, technologies, scientific and technical information, or illegal performance of works or provision of services in favor of such foreign organization/its representative that could be used for or in connection with the creation of arms and military equipment and are subject to export control. Thus, the essential element of the crime is that the guilty person should have known about the designation or end-use of the products.

Depending on aggravating circumstances, the maximum possible penalties include up to seven years imprisonment with a fine of up to RUB 1 million (approx. US$16,500) and confiscation of the controlled items. The maximum period of the statute of limitations is ten years.

Article 226.1 of the Russian Criminal Code establishes penalties for the smuggling of dual-use or military items. Depending on aggravating circumstances, the maximum possible penalties include up to 12 years imprisonment with a fine of up to RUB 1 million (approx. US$16,000) and confiscation of the controlled items. In order to be considered a crime, the cost of the goods in question should exceed RUB 1 million (approximately US$14,000) (RUB 100,000 (approximately US$1,400) in relation to specific goods determined by the government of the Russian Federation). The maximum period of the statute of limitations is 10 years.

Criminal responsibility can be applied only to individuals (e.g., the responsible managers).

(c) Enforcement

Administrative penalties are enforced by the FSTEC. If the penalties include confiscation of goods, a final decision must be taken by a court (i.e.,

state courts of general jurisdiction or state arbitrazh courts).

Criminal investigations are initiated by the Russian Federal Prosecution Service and conducted by the Investigation Committee. Criminal penalties may be imposed only by a state court.

According to the recent statistics available, in 2021 the customs authorities initiated two criminal cases under Article 189 of the Russian Criminal Code and 704 criminal proceedings under Article 226.1 of the Russian Criminal Code. In 2022 the customs authorities initiated three cases under Article 189 of the Russian Criminal Code and 742 cases under Article 226.1 of the Russian Criminal Code. According to court statistics, in 2021 the Russian courts issued two verdicts under Article 189 of the Criminal Code; in both cases the guilty persons were sentenced to conditional imprisonment. During the same period of 2021 the Russian courts passed 377 verdicts under Article 226.1 of the Russian Criminal Code, including 63 sentenced individuals, 241 individuals put under conditional deprivation, two cases of compulsory work, and 23 criminal fines.

(d) Voluntary Disclosure

Russian entities or individuals are not legally required to report any discovered violation of Russian laws. There are no penalties in Russian law for nondisclosure or failure to report.

Voluntary self-disclosure does not exempt one from criminal liability and penalties, but self-disclosure could be viewed as an alleviating circumstance in an administrative case, and the Criminal Code provides for the possibility of exemption from criminal penalties for active repentance.

According to court practice on administrative cases, if an exporter immediately (i.e., within several days after the mistake is unveiled) corrects a mistake and correctly reports the fact to the customs, there are high chances of proving in court that the exporter took all possible measures to act in a bona fide fashion and, therefore, cannot be held administratively liable.

Therefore, voluntary self-disclosure could be viewed as a strong mitigating factor for responsibility and penalties on administrative and criminal offences. However, use of the self-disclosure option must be

carefully considered on a case-by-case basis and should take into account all the peculiarities of the given situation.

25.10 Recent Export Enforcement Matters

As mentioned in Section 25.9(c), according to CaseLook database, there were 37 lawsuits related to challenging administrative sanctions imposed for violation of export control regulations (i.e., Article 14.20 of the Administrative Code) in 2020. According to CaseLook database, there were eight court decisions on criminal cases initiated under Article 189 of the Russian Criminal Code in 2020.

Almost all administrative and criminal cases have common corpus delicti. Russian exporters did not check whether the products they intended to transfer to foreign persons were subject to export controls. As a result they transferred controlled items without prior authorization of the FSTEC. The FSTEC or the Russian customs unveil such cases and initiate administrative and/or criminal investigations.

25.11 Special Topics

(a) Re-export

Re-export of controlled items is subject to special clearance under Russian export controls (i.e., an end-user certificate is required). Re-export is the transfer of controlled items by the initial end user to any third parties, including in the territory of Russia. Any re-export must be approved by the FSTEC or MoD.

(b) Practical Issues Related to Export Control Clearance

Prior to exporting any potentially controlled items the Russian exporter is recommended to perform a preliminary expert examination by approaching:

1. The FSTEC (free of charge), statutory timeframes: 1–2 months; or
2. Independent test laboratories accredited by the FSTEC (for a fee), statutory timeframes: 1 week to 1 month; at the end the laboratory issues an official statement letter (conclusion).

An official statement of the FSTEC or an independent test laboratory confirming that the items at issue do not fall under export controls should be legal grounds to claim that an export license is not required. Note that in some cases the customs require not only letters issued by the FSTEC/independent test laboratories but also “comfort” letters from the MoD confirming that the products are not viewed as military items.

(c) Special Customs Entry Points and Transit

Goods are in transit when they pass through a territory before reaching their final (export) destination. Transit through Russia of goods originating from third countries is subject to export control regulations. Some types of goods require a transit permit.

Transit may be prohibited if items are/may be intended for the manufacture or use of a weapon of mass destruction. Some specific types of dual-use products must be imported/exported into Russia only at special customs entry/exit points. For example, this relates to chemical, biological, nuclear goods, and waste.

In cases of intangible transfer of controlled information/technology, the Russian exporter of record must also obtain preliminary approval of the FSTEC for each such transfer (usually the FSTEC formalizes this by making the relevant note in the export control license or an attachment to it).

(d) Recordkeeping

Russian export control regulations require exporters to keep documents and records related to export control operations for at least three years. The exporters must properly and in a timely fashion compile records and report on the controlled transactions, otherwise they might be subject to administrative penalties in the form of a fine and/or cancellation of the export control license.

(e) Intangible Transfer of Technical Information

Russian export control regulations do not provide clear guidance on intangible transfer of controlled items (for example, provision of technical documentation via the internet). In practice, the FSTEC requires copies of

technical information before it is sent offshore. The current legislation does not provide special documents for formalization of such transfers. Export licenses usually also do not have any special appendices or enclosures. The FSTEC still has a formal right to establish additional requirements for the exportation of technical information and to require provision of technical documentation. Without provision of the technical documentation to the FSTEC, the export license could be viewed as invalid and export of the technical information under such export license is unlikely to be permitted, and if it is attempted, this would constitute an administrative violation.

The law does not set any requirements regarding storage conditions (i.e., terms and timing) of the technical documentation that is provided by the applicant within the export licensing procedure. However, based on general statutory rules, the FSTEC should guarantee its secrecy and should not disclose such information to any third parties.

(f) How to Be Compliant When Exporting to Russia

Note that for import of certain controlled items, a Russian importer of record is required to obtain an export control license. In this regard, prior to starting shipping to Russia of items that are subject to export controls in the United States or any other country, the following step plan would be recommended:

1. Classify products, software, and technology by requesting the Russian importer to determine if the delivery could be restricted or prohibited under Russian laws. In cases of doubt:
   - examine questionable items to see whether they are subject to Russian export control or not (in disputable cases expert reports are compulsory);
   - the testing can be performed either by the FSTEC or by independent test laboratories accredited by the FSTEC.
2. On the basis of the test results, the Russian importer should:
   - apply to the FSTEC for an export control license, if required (i.e., importation into Russia of certain types of items requires an export control license);
   - apply to the FSTEC for an import certificate (end-user certificate) and provide the certificate to your company;

- report to the FSTEC when necessary on the controlled import/export operations with the imported items; and
- properly record any transactions with the imported items (documents must be kept for three years).

(g) How to Be Compliant When Exporting Out of Russia

1. The Russian exporter should classify the item:
   - determine if the delivery could be restricted or prohibited (by comparing description/key words/HS codes with the dual-use/military lists) under Russian law;
   - in cases of doubt:
   - examine questionable items to see whether they are subject to Russian export control or not (in disputable cases expert reports are compulsory);
   - note: during the testing/examination product samples might be required;
   - the testing can be performed either by the FSTEC or by independent test laboratories accredited by the FSTEC.
2. On the basis of results of classification, the Russian exporter should:
   - if items are subject to export control, apply for an export license;
   - for re-exportation of items subject to export control, apply for a re-export permit;
   - if items are not subject to export control, obtain and use a written conclusion (export permit) of the FSTEC/test laboratory for customs clearance purposes;
   - provide a timely report to the FSTEC on the controlled export operations, and properly record export control transactions (documents must be kept for three years).

25.12 Russian Encryption Controls

(a) General Comments

The Russian encryption regulations are divided into the following two parts: (1) import encryption regulations that control importation and exportation of encryption-based products, and (2) local encryption licensing

requirements that are the two separate sets of regulations that should be applied independently from the Russian export control. The main governmental regulatory and law enforcement body in the sphere of encryption is the Licensing Center of the Russian Federal Security Service (FSS). The official website of the FSS: http://clsz.fsb.ru/.

(b) Import Encryption Clearance Requirements

The importation to or exportation from Russia of the listed goods may be subject to the import/export encryption clearance requirements that are set forth at the supranational level of the Eurasian Economic Union (Russia, Belarus, Kazakhstan, Kirgizstan, and Armenia). The main legal act is Resolution of the EAEU Commission No. 30, dated April 21, 2015, On Non-Tariff Regulations ("Non-Tariff Regulations"). Section 2.19 of the Non-Tariff Regulations established the list of goods that normally include encryption technology (almost all types of IT products). The list includes HS codes and product description.

Electronic (intangible) cross-border transmission of data (e.g., via internet) is not controlled. Depending on the encryption-based characteristics and type of data that is encrypted by the product, the import encryption clearance can require one the following types of permission documents:

- An import encryption license,
- An import encryption permit, or
- A registered notification.

An *import encryption license* is generally required for B2B products with "heavy" encryption functions that can encrypt customer/business data "at rest" or "in flight" with encryption keys exceeding 56 bits for symmetric (or 512 bits for asymmetric) cryptographic algorithms.

Import encryption licenses are issued by the Russian Ministry for Industry and Trade (MIT) on the basis of a standard set of documents attached to a formal application. The term of consideration of applications should not exceed 15 business days. The MIT issues one-shot licenses that can be valid within a one-year term. An applicant for import encryption license could be only a Russian legal entity that must also have a valid local (domestic) encryption license (issued by the FSS); foreign companies and

their local branches or representative offices cannot act in the legal capacity of licensee.

Before applying for an import encryption license, the applicant should first apply to the FSS for an official license approval. The statutory term for obtaining a license approval with the FSS should not exceed 30 calendar days, and certain additional time is required for the preparation and delivery of the documents to the FSS. The applicant should provide to the FSS a standard set of documents, including corporate documentation on the legal entity, a copy of foreign trade contract, contract with the end user, as well as technical characteristics of the products (the regulations specifically exempt the applicants from a necessity to provide source codes).

An *import permit* can be issued with respect to "heavy" encryption-based products, if such products are imported for certain specific purposes, including temporary importation (e.g., for exhibition purposes), or for the internal needs of the importer of record. The applicant can be any person, including Russian legal entities and individuals, as well as local representative or branch offices of foreign companies. The procedure of issuance of import permits is very similar to the issuance of an import license approval. The import permits are issued by the FSS based on a standard set of documents that should include a guarantee letter of the applicant confirming the designation of the products and an obligation that the products would not be subsequently transferred to any third parties or used for the provision of encryption-based services.

A *notification procedure* can be applied with respect to products that fall under any of the 12 exemption categories of "mass market" goods that are primarily designated for use by individuals, or certain specific types of goods with limited encryption capabilities. If all encryption-based functions of products fall under the 12 exemption categories, such functions would be out of scope of the local encryption licensing requirements. Generally, the preceding 12 statutory exemption categories do not apply to B2B products with "heavy" encryption functions that can encrypt customer/business data "at rest" or "in flight" with encryption keys exceeding 56 bits for symmetric (or 512 bits for asymmetric) cryptographic algorithms.

Notifications can be registered by Russian legal entities or individuals acting as authorized representatives of foreign manufacturers. Authorization documents issued by the manufacturers must be respectively notarized and legalized (apostilled) in the country of issue. The notification form includes

sections on the full product name (including model name and SKU/part numbers), product description, information on the manufacturer and the applicant, full description of encryption functionalities (including names of cryptographic algorithms, key lengths, implementing protocols, and designation of encryption functions), as well as term of validity of the notification set by the applicant. The notifications are registered by the FSS. The term of consideration of the notifications should not exceed ten business days following the date of submission. All registered notifications are published at the EAEU website: http://www.eurasiancommission.org/ru/docs/Lists/List/AllItems.aspx.

When the notification has been registered, the products can be freely imported to Russia/EAEU by any persons. Therefore, the registration of notifications is viewed as one of the simplest types of import encryption clearance procedure. However, in practice, the process of registration of notifications can be complicated (the applicants often have to amend, re-execute and re-submit the notifications for registration several times in order to address certain specific questions raised by the FSS).

(c) Local Encryption Licensing Requirements

Russian encryption licensing requirements are set forth by Governmental Decree No. 313, dated April 16, 2012 ("Decree No. 313"). Decree No. 313 establishes a list of 28 types of licensing activities that generally include all possible activities related to the:

1. Development and manufacturing of encryption-based products;
2. Distribution/transfer of encryption-based products;
3. Maintenance, servicing, and repair of encryption-based products;
4. Provision of encryption-based services to third parties.

Generally, the development of any encryption-based products/technology requires a local encryption license.

Local encryption licenses are issued by the FSS to Russian legal entities only. To get a local encryption license, the applicant should perform certain technical preparations and arrangements. The main licensing requirements include the following: to establish an internal division responsible for the licensed activities, to hire at least two to three engineers that would be responsible for the management/operation of the division, to get and prepare licensed premises and equip them with certain IT equipment, to

arrange a certain specific level of security of the licensed premises, and so on. The timelines for the issuance of a local encryption license is normally three to six calendar months, plus a certain time required for the aforementioned preparations. Local encryption licenses are termless.

Decree No. 313 established 12 exemption categories of "mass market" goods that are very similar to the 12 exemption categories of goods set forth by the import encryption regulations for the notification procedure. Another statutory exemption under Decree No. 313 applies to encryption-based activities performed for the internal needs of the legal entity, without transfer/distribution of encryption-based products or provision of encryption-based services to any third parties. In all such cases, a local encryption license is not required.

(d) Penalties for Violation of Russian Encryption Regulations

(i) Administrative Penalties

A failure to obtain an import encryption license/permit or to register a notification for encryption-based products before their importation to Russia can be viewed as an administrative violation of nontariff regulations under Article 16.2(3) or Article 16.3 of the Administrative Code. Penalties are in the form of a fine of RUB 50,000–300,000 (approx. US$800–5,000) per shipment, with or without confiscation of the imported products, or confiscation of the products. Confiscation of products could be performed only on the basis of a court decision. Responsible managers of the importers of record could be subject to an administrative fine of RUB 10,000–20,000 (approx. US$160–320). The statute of limitations period for customs violations is two years.

Performance of local (domestic) encryption activities without a local license (for example, if a Russian company develops encryption-based technology or products without a local license) may be viewed as an administrative violation under Article 13.13 of the Administrative Code. Penalties are in the form of a fine for legal entities of RUB 10,000–20,000 (approx. US$150–300) with or without confiscation of the encryption-based products. Responsible managers of the company may be subject to an administrative fine of RUB 2,000–3,000 (approx. US$30–50), with or without confiscation of the encryption-based products. The statute of

limitations period is two months, or three months if the case is considered by a court.

(ii) Criminal Liability

Conducting business activity without a license/authorization when such license/authorization is required per se, may incur criminal liability under Article 171 of the Russian Criminal Code if and when the proceeds from such activity exceed RUB 2.25 million (approx. US$36,000). The penalty for a crime under Article 171 of the Criminal Code includes up to five years of imprisonment. The statute of limitations period depends on the gravity of the crime and may be up to ten years. Article 171 of the Criminal Code can be similarly applied to the violations in the sphere of both import encryption clearance and local encryption licensing requirements.

25.13 Recent and Expected Developments

(a) Developments in Russian National Laws and Regulations on Export Controls

Starting from March 2020, new export restrictions were introduced in response to the Covid-19 pandemic. However, as of January 2021, these export restrictions no longer remained in force (e.g., on various medical items and food products).

On October 15, 2020, the Russian government adopted a new Roadmap on Business Climate Transformation, which included the following measures aimed at simplifying export control clearance:

1. To allow multiple uses of conclusions issued by FSTEC/test laboratories for export of goods/technologies that cannot cause damage to national security;
2. To extend the list of goods that are not subject to restrictions of the Russian export control regulations;
3. To reduce time and financial costs of exporters on export control compliance; and
4. To optimize the list of dual-use goods and technologies subject to export control that are controlled for national security reasons.

From November 23, 2022, the Russian government adopted Decree No. 313 establishing a list of dual-use products temporarily prohibited from export to so-called “hostile” countries, which have imposed foreign trade measures against Russia (i.e., the U.S., EU, Australia, Canada, Japan, Taiwan, Singapore, New Zealand, etc.). The dual-use products covered by Decree No. 313 should be identified using the provided description, and HS codes are indicated for ease of reference only. The list primarily covers various types of arms, explosives, machinery, equipment, and spare parts. The export ban on dual-use products should be in force until December 31, 2023, unless further extended.

(b) Russian Export Restrictions

On March 9, 2022, prior to aforementioned Decree No. 313, the Russian government adopted Decrees Nos. 311 and 312 establishing the following temporary export restrictions and prohibitions, as follows:

1. Decree No. 311 established a list of goods temporarily prohibited from export outside Russia and Belarus to any foreign countries, except for other EAEU countries (i.e., Armenia, Kazakhstan, and Kirgizstan, as well as certain other local territories). The list of restricted goods includes machinery, equipment, vehicles, and IT products. The restricted goods are listed by customs classification (HS) codes.
2. According to Decree No. 312, the exportation of the same goods (listed under Decree No. 311) to the EAEU countries of Armenia, Kazakhstan, and Kirgizstan requires a special export permit from the competent authorities (depending on the type of goods). For example, export permits for vehicles, manufacturing, and IT equipment should be issued by the Ministry of Industry and Trade (MIT). The export of telecoms equipment should be authorized by the Russian Ministry of Digital Development, Communications and Mass Media (Mincifra), and so on.

The key purpose of Decrees Nos. 311–312 is to temporarily prevent physical extrication of products from Russia so that such export does not affect the Russian economy.

The procedure for obtaining an export permit is set out in implementing regulations issued by the competent authorities (i.e., MIT, Mincifra, etc.)

and includes preparation and submission of a standard set of commercial and shipping documents to the appropriate governmental body, and completion of an application form. The time lines for consideration of the application should not exceed two to three business weeks.

The issuance of an export permit under Decree No. 312 can be denied in the following two cases: (1) incorrect completion of the application, or absence of certain supporting documents (in such case the application can be corrected, re-executed and re-submitted), or (2) critical shortage of the goods on the local market (this aspect is considered by the authority on a case-by-case basis).

1. Decree No. 313, in addition to the list of dual-use items, established a separate list of wood products, steel materials, and steel wastes, which cannot be exported outside Russia to the aforementioned "hostile" countries.

Decrees Nos. 311–313 establish a number of statutory exemptions, which could be applied in certain specific cases, for example including goods originating from Russia and covered by certificates of origin, temporary importation under ATA carnets, or goods exported by individuals and designated for their personal use, and so on.

Importantly, export restrictions under Decrees Nos. 311–313 apply to any goods that have been physically brought to Russia, including temporarily imported products, which have the legal status of "foreign" goods.

The export restrictions imposed by Decrees Nos. 311–313 should be in force until December 31, 2023, unless further extended.

(c) Russian Law on Exclusive Jurisdiction of Russian Courts over Sanctions Disputes

On June 19, 2020, a new Russian Law No. 171-FZ, dated June 8, 2020, known as the Lugovoy Law entered into force. It includes a number of changes into the Russian Arbitrazh Procedural Code:

1. Most important, Russian state commercial courts (also called "arbitrazh" courts) were granted exclusive jurisdiction over sanctions disputes. Sanctions disputes include (1) disputes involving sanctioned parties (Russian persons and/or their foreign affiliates) as

well as (2) disputes between Russian and/or foreign parties if the sanctions are a cause of their dispute.

2. Parties may still agree to resolve their sanctions disputes outside of Russia, but Russian courts will have jurisdiction over such disputes if a sanctioned party cannot access the justice system because of sanctions.
3. If a party is sued or is about to be sued in a foreign court or arbitration institution in breach of the Lugovoy Law, this party may request an anti-suit injunctive order from a Russian court. Any party breaching such injunction may be fined by the Russian court for the full amount of the claim plus the opponent's legal costs.

(d) Criminal penalties for calls for introducing sanctions against the Russian Federation

On March 4, 2022, the Russian Parliament adopted a law introducing the new Article 284.2 of the Russian Criminal Code, establishing criminal liability for calls to introduce foreign trade sanctions against the Russian Federation. The maximum possible penalties include up to 3 years of imprisonment with a fine of up to RUB 200,000 (approximately, US$2,800). The maximum period of the statute of limitations is two years.

The same law introduced the new Articles 207.3 and 280.3 of the Russian Criminal Code, establishing penalties for public dissemination of knowingly false information about the use of the armed forces of the Russian Federation and for public discrediting of the armed forces of the Russian Federation. The maximum possible penalties may include up to 15 years of imprisonment. The maximum period of the statute of limitations is 15 years.

---

1. Prepared by Alexander Bychkov (partner, Baker McKenzie, Moscow), Vladimir Efremov (partner, Baker McKenzie, Moscow), and Andrey Gavrilov (senior associate, Baker McKenzie, Moscow).
2. Access to this link could be restricted in your jurisdiction.
3. Access to this link could be restricted in your jurisdiction.
4. Access to this link could be restricted in your jurisdiction.
5. https://fstec.ru/normotvorcheskaya/eksportnyj-kontrol/283-reestry-perechni.
6. As mentioned (in Section 25.1(d)), legally, submissions could be filed electronically via a web-link: https://www.gosuslugi.ru/structure/10000001025.
7. https://fstec.ru/eksportnyj-kontrol/nezavisimaya-identifikatsionnaya-ekspertiza/294-reestr-organizatsij-i-predpriyatij (URL access could be restricted in certain jurisdictions due to foreign trade

sanctions).

26

Export Controls and Economic Sanctions in Singapore

Kala Anandarajah[1]

26.1 Introduction

(a) What Is Regulated?

The key legislation relating to export controls and economic sanctions in Singapore includes the following:

1. Customs Act 1960 (CA)[2]
2. Regulation of Imports and Exports Act 1995 (RIEA)[3]
3. Strategic Goods (Control) Act 2022 (SGCA)[4]
4. Chemical Weapons (Prohibition) Act 2000 (CWPA)[5]
5. United Nations Act 2001 (UNA)[6]
6. Monetary Authority of Singapore Act 1970 (MASA)[7]
7. Terrorism (Suppression of Financing) Act 2002 (TSOFA)[8]

Singapore is a member of the following multilateral export control treaties and free trade agreements (FTAs[9]):

1. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (1993) ("Chemical Weapons Convention")[10]

2. Basel Convention on the Control of Transboundary Movement of Hazardous Wastes and Their Disposal (1989)[11]
3. Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)
4. European Union-Singapore Free Trade Agreement (EUSFTA)
5. ASEAN-Australia-New Zealand FTA
6. ASEAN-China FTA
7. ASEAN-Hong Kong, China FTA
8. ASEAN-India FTA
9. ASEAN-Japan Comprehensive Economic Partnership
10. ASEAN-Korea FTA
11. ASEAN FTA
12. EFTA-Singapore FTA
13. GCC-Singapore FTA
14. Regional Comprehensive Economic Partnership
15. Pacific Alliance Singapore FTA
16. Trans-Pacific Strategic Economic Partnership

Singapore is not a member of the Wassenaar Arrangement, the Australia Agreement, the Missile Technology Control Regime, or the Nuclear Suppliers Group. Although Singapore is not a member of the Wassenaar Arrangement, it updates its export control regime for military and dual-use goods from time to time to comply with the Wassenaar Arrangement's List of Dual-Use Goods and Technologies and Munitions List.

Separately, Singapore is also party to numerous bilateral agreements with a number of countries, such as China, India, Japan, Korea, New Zealand, Panama, Peru, Australia, Costa Rica, Jordan, Sri Lanka, Turkey, United Kingdom, and United States.

Singapore is also in the process of negotiating the MERCOSUR-Singapore FTA and the EAEU-Singapore FTA. Singapore has substantively concluded negotiations on the MERCOSUR-Singapore FTA on July 21, 2022, while negotiations on the EAEU-Singapore FTA have likely been put on hold due to the Russia-Ukraine war.

(b) Where to Find the Regulations:

All the aforementioned regulations can be found on Singapore statutes online at: http://sso.agc.gov.sg, as well as the other sources in the footnotes.

(c) Who Is the Regulator?

Multiple government ministries and agencies share the responsibility for administering and enforcing export controls and economic sanctions in Singapore.

1. Singapore Customs administers and enforces export controls and trade sanctions relating to goods imported into, exported from, transhipped in, or in transit through Singapore.
2. The Monetary Authority of Singapore (MAS) administers and enforces financial sanctions.
3. The Ministry of Foreign Affairs (MFA) and Ministry of Home Affairs (MHA) are members of the Inter-Ministry Committee on Terrorist Designation, which has the authority to designate specific individuals and organisations as terrorists subject to sanctions under the TSOFA.
4. The Commercial Affairs Department (CAD) of the Singapore Police Force and Attorney-General's Chambers are responsibility for investigating and prosecuting sanctions violations.

(d) How to Get a License

In summary, any party exporting goods from Singapore is required to obtain an export permit from Singapore Customs. This can be obtained through TradeNet®, Singapore's National Single Window for trade declaration, at https://www.ntp.gov.sg/public/government-services. In addition, further licenses, permits, or approvals may be required if the exported goods fall within the scope of controlled goods, strategic goods, or controlled chemicals. Further details of the licensing process are set out later in the chapter.

(e) Key Websites

The key website with the relevant information on export controls and economic sanctions is Singapore Customs' website, which can be found at http://www.customs.gov.sg, and the MAS's website, which can be found at http://www.mas.gov.sg.

26.2 Structure of the Laws and Regulations

As listed earlier in Section 26.1(a), there are various statutes in Singapore that deal with different aspects of export control and economic sanctions. These statutes broadly cover the requirements of export control, such as the licenses and permits required for an export of goods from Singapore, and the offences and penalties for failing to comply with these requirements.

The statutes are supplemented by related subsidiary legislation, in the form of regulations and orders. These regulations and orders drill down into more granular details and provide further elaboration on the nature of the export controls and economic sanctions in Singapore. A non-exhaustive list of the more crucial legislation, and the key regulations and orders, is set out in the following section.

26.3 What Is Regulated: Scope of the Regulations

The legislation and subsidiary legislation in Singapore are structured such that different aspects of export control and economic sanctions are covered by different statutes, as follows:

- The CA broadly establishes Singapore Customs as the regulator and sets out its powers.
- The RIEA provides for the regulation, registration, and control of imports and exports in Singapore, including but not limited to the import and export of goods to and from sanctioned regions.
  - In particular, the Regulation of Imports and Exports Regulations (RIER)[12] sets out the general export licensing requirements in Singapore, including the requirement to obtain approvals from the relevant competent authorities for the export of certain types of controlled goods.
  - The Seventh Schedule and Eighth Schedule to the RIER also sets out a specific list of prohibited imports from and exports (including transshipped goods and goods in transit bound for) to sanctioned countries.
- The SGCA regulates the transfer and brokering of strategic goods and strategic goods technology. In particular, the Strategic Goods (Control) Order 2021 contains a full listing of the goods and

technology that are deemed to be strategic goods and strategic goods technology for the purposes of the SGCA.

- The CWPA regulates, among other things, the export of certain controlled chemicals under the Chemical Weapons Convention.
- The UNA enables the Ministry of Home Affairs to enact domestic regulations that implement trade sanctions imposed by United Nations Security Council (UNSC) resolutions. The full list of specific trade sanctions can be found in the Seventh Schedule to the RIER, the Eighth Schedule to the RIER, and subsidiary legislation under the UNA.
- The MASA enables the MAS to enforce domestic regulations that implement UNSC resolutions against financial institutions that do not comply with sanctions against designated individuals/entities in sanctioned countries. A full list of these regulations and the designated individuals/entities, which are updated from time to time, can be found at https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/lists-of-designated-individuals-and-entities.
- The TSOFA regulates, amongst others, financial transactions to suppress the financing of terrorism, in accordance with the International Convention for the Suppression of the Financing of Terrorism.

26.4 Who Is Regulated?

Any party who wishes to export goods from Singapore will be regulated under the applicable statutes and the relevant subsidiary legislation. It is the exporter (i.e., the party issuing the commercial invoice to the overseas customer) who will have to comply with the requirements of, among other things, obtaining the appropriate export permit for the export of goods from Singapore.

For re-exportation of goods, an export permit is also required for the re-export of goods that are imported under the Temporary Import Schedule (TIS). More information on the TIS can be found at https://www.customs.gov.sg/businesses/importing-goods/temporary-import-scheme.

On the extraterritorial application, it is not explicitly stated in the RIEA and SGCA (e.g., brokering of strategic goods) whether the prohibitions in the acts will apply to Singapore persons/entities while they are outside of Singapore; it is merely stated that the prohibitions apply to a "person." The term "person" is not defined, suggesting that on a literal reading there is extraterritorial application.

Note, however, *section 6 of the UNA specifically creates extraterritorial jurisdiction over Singapore citizens*: "the provisions of this Act have effect, *in relation to citizens of Singapore, outside as well as within Singapore*, and where an offence under this act or any regulations made under this act is committed by a citizen of Singapore in any place outside Singapore, the citizen may be dealt with in respect of that offence as if it had been committed within Singapore." In short, given section 6 of the UNA, the UNA applies to *Singapore citizens (whether within or outside Singapore) and any person in Singapore*. This includes not just an individual but also any company or association or body of persons, corporate or unincorporate, where incorporated or registered in Singapore or present in Singapore (and where the violation takes place in Singapore).

26.5 Classification

(a) Harmonized System Codes

Before exporting goods from Singapore, exporters should be aware of the classification system, and should be able to classify their goods under the appropriate product code. This is to ensure that the exporter is able to accurately fill in the information required for the export permit through TradeNet®, and to allow the exporter to determine whether the goods are subject to control by any competent authorities.

Goods are classified in Singapore according to an eight-digit tariff nomenclature, as set out under the Singapore Trade Classification, Customs and Excise Duties (STCCED). For example, butter would be classified under the code number 04051000. This classification system is adopted from the ASEAN Harmonized Tariff Nomenclature (AHTN), which is also an eight-digit classification system used by all ten ASEAN member countries. This is, in turn, based on the Harmonized System (HS) developed by the World Customs Organization.

Exporters may easily determine the appropriate HS codes for their products by referring to the latest online version of the STCCED, which can be found at https://www.customs.gov.sg/files/businesses/STCCED%202018_Feb%2021.pdf.

Once the HS codes of the goods have been determined, the exporter may then use this to determine whether the goods are classified as controlled or strategic goods and require the approval of the relevant competent authority before export. Some illustrations of the types of controlled goods, and their corresponding competent authorities, are set out here:

- Sand and granite—Building and Construction Authority (BCA);
- Controlled substances (as defined in the Misuse of Drugs Act 1973) —Central Narcotics Bureau (CNB);
- Rice and rubber, including rubber latex—Enterprise Singapore (ESG);
- Therapeutic products, medical devices, cell, tissue and gene therapy products, Chinese proprietary medicines, psychotropic substances, oral dental gums, substances specified as “poisons”—Health Sciences Authority (HSA);
- Publications, recorded sound media, imported telecommunication equipment—Info-communications Media Development Authority (IMDA);
- Human and zoonotic pathogens and selected toxins regulated under the Biological Agents and Toxins Act—Ministry of Health (MOH);
- Fruit machines, jackpot machines, remote gambling activities—Ministry of Home Affairs (MHA);
- Goods containing any of the ingredients listed in Part I of the Second Schedule of the Environmental Protection Management Act 1999, pesticides, waste batteries, chlorofluorocarbons—National Environment Agency (NEA)
- Plants, plant materials, live animals, birds, veterinary biologics, animal feed and products—National Parks Board (NParks);
- Petroleum and flammable materials—Singapore Civil Defence Force (SCDF);
- Chewing gum, items classified as “strategic goods,” mastering equipment and replicating equipment for the manufacture of CD, CD-

Rom, VCD, DVD, and DVD-Rom—Singapore Customs;
- Animals, fish, meat for human consumption, fresh fruit and vegetables, processed food—Singapore Food Agency (SFA);
- Arms and explosives, handcuffs, toy guns—Singapore Police Force (SPF).

Further details on the process of obtaining the approval of the competent authority for controlled goods are set out in the following section.

(b) Strategic Goods

Under the SGCA, Singapore regulates the export, transshipment, transit, and brokering of strategic goods and strategic goods technology, as well as the intangible transfer of technology. An intangible transfer of technology is defined as "the electronic transmission of controlled strategic goods technology in Singapore" or "the act of making the controlled strategic goods technology available in Singapore on a computer or server" such that it becomes "accessible to a person in a foreign country."[13] While there is no absolute clarity on this, it is likely for the intangible transfer of technology to exclude "deemed exports," where technology is revealed to a non-Singaporean national in Singapore. The question is whether the recipient of the intangible transfer of technology is based in a foreign country, that is, his location is outside of Singapore.

Exporters should be aware that the HS Codes used for the classification of general goods is insufficient to determine conclusively if a particular product falls under the Strategic Goods Control List. This is because in determining whether a product constitutes strategic goods, factors such as the end use and technical specifications of the product need to be taken into consideration.

As such, before anything else, it must first be determined whether the product that is intended to be exported falls under the Strategic Goods Control List, as set out in the Schedule to the Strategic Goods (Control) Order 2021. Goods that meet the technical specifications as described in the Strategic Goods Control List will be classified as strategic goods, and subject to control under the SGCA.

The Strategic Goods Control List essentially regulates two types of goods: military goods and dual-use goods. Part I of the Strategic Goods Control List sets out the technical details of the type of military goods

regulated, including items such as arms, ammunitions, bombs, tanks, imaging devices, and chemicals. The list of military goods regulated as strategic goods are set out as follows:

Category Code	Description
ML1	Small-caliber arms
ML2	Large-caliber weapons and projectors
ML3	Ammunition and fuse setting devices
ML4	Bombs, missiles, other explosive devices and related equipment
ML5	Fire control, surveillance, and related alerting and warning equipment
ML6	Ground vehicles and components
ML7	Chemical, biological toxic agents, radioactive materials and related equipment
ML8	Explosives, propellants, fuels and related substances
ML9	Naval vessels and components
ML10	Military aircraft and components
ML11	Electronic equipment for military use
ML12	High velocity kinetic energy weapons
ML13	Armoured or protective equipment
ML14	Specialized equipment for military training
ML15	Imaging or countermeasure equipment
ML16	Unfinished products for use in military items
ML17	Miscellaneous equipment and materials
ML18	Production equipment for military items
ML19	Directed energy weapon systems
ML20	Cryogenic and “superconductive” equipment
ML21	Specific software for military items
ML22	Specific technology for military items

Part II of the Strategic Goods Control List then sets out the types of dual-use goods regulated as strategic goods. Dual-use goods essentially comprise goods that are designed for commercial applications, but that can have military applications or that can potentially be used as precursors or components of weapons of mass destruction. A five-character alphanumeric code is used for the list of dual-use goods. The list is divided into the following ten categories:

Category Number	Description

0	Nuclear materials, facilities, and equipment
1	Special materials and related equipment
2	Materials processing
3	Electronics
4	Computers
5	Part 1 Telecommunications Part 2 Information security
6	Sensors and lasers
7	Navigation and avionics
8	Marine
9	Aerospace and propulsion

Each category of dual-use goods is then further sub-divided into five product groups, as follows:

Product Group	**Description**
A	Systems, equipment, and components
B	Test, inspection and production equipment
C	Materials
D	Software
E	Technology

To ascertain whether the product comprises strategic goods, the exporter must first identify the nature of the product; its intended use, function, and application; and whether it is a complete system, equipment, or raw material. The exporter must then compare the product's specifications against the possible categories of goods. If there is no possible category code, then the product is not a strategic good. Even if the product meets the stated specifications, it will not be a strategic good if it fulfills the applicable exclusion notes, which can be found in the Strategic Goods Control List itself.

Further information on the classification of products as strategic goods can be found in the Guidebook on the Determination of Strategic Goods, at https://www.customs.gov.sg/businesses/strategic-goods-control/resources.

If the exporter is still unable or unsure as to the proper classification of a product, an application for determination of strategic goods may be submitted to Singapore Customs, to obtain advice as to whether the product

would constitute strategic goods and be regulated under the SGCA. The exporter will have to provide the following information:

- Particulars of the applicant;
- Particulars of the product manufacturer;
- Technical specification(s), datasheet(s), brochure(s) of the product;
- Safety Data Sheet (SDS) or Certificate of Analysis (COA);
- Export license(s) or authorization(s); and
- Intended end use of the product.

The exporter must provide the following supporting documents:

- Technical specifications of the strategic goods (for example, operating instructions, manuals, brochures, data sheets, catalogues);
- Business transaction documents (for example, contract, purchase order, invoice, tender requirements);
- End-user statement;
- Export license (and its English translation) from the originating country or a confirmation from the originating country that they do not control the re-export of the goods;
- Company profile/websites of relevant parties (exporter, consignee, end user); and
- Other relevant supporting documents.

(c) Chemical Weapons Control

The CWPA was enacted to provide the Singapore government with the legislative framework required to fulfill Singapore's obligations under the Chemical Weapons Convention. The Chemical Weapons Convention contains three Schedules of toxic chemicals and their precursors, along with an additional category of unscheduled discrete organic chemicals. The Schedules are organized to reflect the risk posed by the chemical to the object and purpose of the Chemical Weapons Convention. A description of the types of chemicals listed in each Schedule are set out as follows.

Schedules	**Description**	**Examples of Chemicals**
1A & 1B	Chemicals that may be used as chemical weapons or as precursors in the final single technological stage of production of a chemical weapon	Saxitoxin
		Sarin
		Tabun

		Ricin

2A, 2A* & 2B	Chemicals that may be used as chemical weapons or as precursors in one of the chemical reactions at the final stage of formation of a chemical listed in Schedule 1.	Arsenic trichloride
		Amiton
		Thiodiglycol
		Pinacolyl alcohol
3A & 3B	Chemicals that may be used as chemicals or that are important to the production of one or more chemicals listed in Schedules 1 or 2.	Cyanogen chloride
		Hydrogen cyanide
		Trimethyl phosphite
		Sulfur dichloride

Unscheduled discrete organic chemicals are also regulated under the CWPA, as the facilities built for their production could have the potential of being converted to chemical weapons production facilities. Unscheduled discrete organic chemicals refer to any chemical belonging to the class of chemical compounds consisting of all compounds of carbon, except for its oxides, sulfides, and metal carbonates. However, unscheduled discrete organic chemicals do not include:

- Oligomers and polymers whether or not containing phosphorous, sulfur, or fluorine;
- Chemicals containing only carbon and metal;
- Carbon monoxide and carbon dioxide; and
- Carbon disulfide or carbonyl sulfide.

Further details on the classification of controlled chemicals under the Chemical Weapons Convention can be found at https://www.customs.gov.sg/files/businesses/GuidetoNACWCLicensewithSchChemList.pdf.

26.6 General Prohibtions/Restrictions/Requirements

As detailed in Section 27.7, there are various licensing restrictions and requirements associated with the export of goods from Singapore, depending on the type of goods that are intended to be exported.

Apart from these licensing restrictions and requirements, under the RIER, exporters are strictly prohibited from exporting certain types of

goods to countries that are sanctioned by the UNSC. A non-exhaustive list of the types of goods is provided next. An updated list can be found at the United Nations (UN) website.[14]

Country	Prohibited Goods
Central African Republic	• Arms and related material
Democratic People's Republic of Korea	• Arms and related material • All items, materials, equipment, goods, and technology relating to nuclear programs, ballistic missile programs, and other weapons of mass destruction programs • Luxury goods including the following: cigars, wines and spirits, fur products, leather bags and clothes, perfumes and cosmetics, plasma televisions, personal digital music players, luxury cars, luxury motorboats and yachts, motor vehicles, watches of metal clad with a precious metal, carpets, works of art, precious jewellery, musical • instruments Graphite designed or specified for use in Electrical Discharge Machining machines • Para-aramid fiber, filament, and tape Certain specified nuclear items, missile items and chemical weapons items in Annex III of Resolution 2094 (2013)
Democratic Republic of Congo	• Arms and related material
Iran	• All items, materials, equipment, goods, and technology that could contribute to enrichment-related, reprocessing, or heavy water-related activities, or to the development of nuclear weapon delivery systems • Arms and related material, and their means of production
Iraq	• Arms and related materials and their means of production
Lebanon	• Arms and related material
Libya	• Arms and related material
Somalia	• Arms and related material • Explosive materials and mixtures, explosive related goods, and technology required to produce explosive materials and mixtures and explosive related goods
South Sudan	• Arms and related material
Sudan	• Arms and related material to all the territory of Darfur, including the new states of Eastern and Central Darfur
Syria	• Chemical weapons

The RIER has been amended to include a new Eighth Schedule, which strictly prohibits exporters from exporting military and dual-use goods to Russia with effect from March 16, 2022, as a result of the Russia-Ukraine War.[15] Further details on the economic sanctions imposed by Singapore on Russia are set out later in the chapter.

(a) Advance Export Declaration

As stated earlier, the RIER requires exporters to obtain an export permit from Singapore Customs for the export of all goods from Singapore. As part of this, Singapore Customs has implemented the Advance Export Declaration requirement, which requires all declarations to be submitted before the goods are exported.

The export declaration must be submitted by either the exporter or the appointed declaring agent via TradeNet®, as soon as possible before the goods are exported. In order to do so, the exporter must first register as a trader by activating its Customs Account[16] at least one working day before the advance export declaration is submitted. After the exporter has registered as a trader, it can then submit the export declarations by either:

- Subscribing as a TradeNet® user, and subsequently declaring its imports on its own or
- Appointing a local declaring agent to make declarations and apply for permit applications to Singapore Customs on its behalf.

Please note that Singapore Customs recommends that the export declaration be submitted before the goods are handed over to the seaport operators or the air cargo handling agents.

The purpose of the Advance Export Declaration system is to enhance Singapore's supply chain security, as the advance information allows Singapore Customs to conduct risk assessments before high-risk items are exported. It also assists the implementation of Mutual Recognition Arrangements to strengthen supply chain security between Singapore and overseas authorities.

(b) Controlled Goods

In addition to the export permit, certain types of controlled goods may be subject to additional regulatory requirements. Controlled goods are goods that are specified in the First Schedule of the RIER, or any goods for which a permit, license, or any form of approval or sanction is required under any legislation in Singapore. This is a long list.

Controlled goods can be subject to different forms of requirements in order to be exported from Singapore, depending on the competent authority regulating the export of the specific controlled goods.

The first step in exporting controlled goods is to determine whether the goods to be exported are indeed controlled and, if so, the specific competent authority that regulates it.

A more comprehensive determination as to whether the particular product is a controlled export can be obtained once the exporter has ascertained the HS Code of the product. A search can then be conducted in Singapore Customs' database,[17] using either the description of the product, HS code, or CA product code. If a product is a controlled export, the "Export" column of the search result will indicate the relevant competent authority that regulates the product.

Once the exporter has determined that the product it intends to export is a controlled export and identified the relevant competent authority, the exporter will then have to comply with that competent authority's requirements. Each competent authority has different requirements. For example, where arms and explosives are to be exported, the Police Licensing & Regulatory Department of the Singapore Police Force requires the consignment to be sent for inspection, and supporting documents to be submitted, before the export will be approved.

(c) Strategic Goods

Strategic goods and strategic goods technology, as set out in the Strategic Goods Control List, are regulated under the SGCA. In addition, even if the product is not listed in the Strategic Goods Control List, it will still be regulated under the SGCA if the exporter has been notified, is aware, or has reasonable grounds to suspect that the product is intended or likely to be used wholly or in part, for or in connection with an activity relating to nuclear, chemical, or biological weapons, or missiles capable of delivering these weapons (i.e., the "catchall" provision).

As part of this regulation under the SGCA, a strategic goods permit must be obtained from Singapore Customs prior to every export, re-export, transshipment, bringing in transit, intangible transfer, electronic transmission (via email, fax, or internet), or brokering of strategic goods or strategic goods technology in the Strategic Goods Control List or of items

covered under the “catchall” provision. There is no requirement to apply for a re-export permit to export the goods from the first country it has been exported to.

In Singapore, strategic trade control is administered under the Strategic Trade Scheme. Under the Strategic Trade Scheme, two kinds of strategic goods permits can be obtained: bulk permits and individual permits. To qualify for a strategic goods permit, the exporter must be a registered trader with Singapore Customs. The difference between the two types of permits is as follows:

- Individual permits are applied for by the exporter on a per transaction basis. They must be applied for at least five working days prior to the loading of the strategic goods. The validity of the individual permit is 22 working days. Where necessary, the validity of the individual permit may be extended up to 66 working days via TradeNet®, subject to conditions if the movement authorized by the permit has not taken place.
- Bulk permits are applied for by the exporter on a longer-term basis. Singapore Customs provides a single approval for the export of strategic goods, so long as the strategic goods are covered within the scope of the bulk permit. The bulk permit has a validity period of three years from the date of the approval.

In addition, for strategic goods software or technology, an intangible transfer of technology (ITT) permit is required before transmitting the technology. There are two types of ITT permits, including:

- Individual permits are applied for by the exporter and are valid for one year on approval. They must be applied for at least seven working days before the transmission of the strategic goods technology.
- Bulk permits are applied for by the exporter on a longer-term basis. The bulk permit has a validity period of three years from the date of the approval.

In support of an application for an individual permit, the following documents must also be submitted:

- End-user statements or certificates;

- Export licenses from the supplying or exporting country (if applicable);
- Import authorization from the importing country (if applicable);
- End-user company profile or website;
- Technical specifications of the strategic goods, such as their operating instructions, manuals, brochures, data sheets, and so on; and
- Business transaction documents such as order forms, contracts, invoices, bills of lading, air waybills, and transaction-related communications;
- Other relevant supporting documents.

Additional criteria will apply if the exporter intends to obtain a bulk permit under the Strategic Trade Scheme. In particular, the exporter will be required to satisfy stringent compliance requirements, as follows:

- Maintain a good trade compliance record with Singapore Customs;
- Implement an effective Internal (Export Control) Compliance Program; and
- Achieve at least the "Enhanced" band under the TradeFIRST Framework.

This is because the bulk permit is intended to be for exporters who are able to commit the necessary resources to implement and maintain a sufficiently robust internal compliance program; who export strategic goods to multiple end users regularly; and who have short order fulfillment times.

In addition, exporters who hold strategic goods permits are subject to responsibilities, such as recordkeeping obligations. Bulk permit holders are required to abide by further obligations, including monthly reporting obligations. Further information on the requirements to obtain a bulk permit, and the responsibilities applicable to strategic goods permit holders, can be found in the Strategic Trade Scheme Handbook at https://www.customs.gov.sg/files/businesses/SEB/STS%20Handbook%20-%20May%202022%20.pdf.

(d) Chemical Weapons Convention

A National Authority (Chemical Weapons Convention) (NA(CWC)) license is required before the export of any controlled chemical under the CWPA to member states of the Organization for the Prohibition of Chemical

Weapons. The full list of member states can be found at https://www.opcw.org/about-opcw/member-states/.

In addition to the NA(CWC) license, as with the export of all goods from Singapore, an approved export permit is required prior to the export of the controlled chemical. Please note that controlled chemicals may also constitute strategic goods and be subject to the export control requirements under the SGCA.

However, different restrictions apply in obtaining a NA(CWC) license where the controlled chemical is to be exported to nonmember states, depending on whether the controlled chemical is classified as a Schedule 1, a Schedule 2, or a Schedule 3 chemical.

Schedules	**Export to Nonmember States**
Schedule 1	Prohibited
Schedule 2	Allowed, subject to the following conditions: • Product must contain no more than 1 percent (by weight) of a mixture of a Schedule 2A or Schedule 2A* chemical • Product must contain no more than 10 percent (by weight) of a mixture of a Schedule 2B chemical • Product must be identified as consumer goods packaged for retail sale for personal use or packaged for individual use • End-User Certificate must be submitted prior to any permitted exports of Schedule 2A, 2A* or 2B chemicals to nonmember states
Schedule 3	Allowed, subject to the following conditions • End-User Certificate must be submitted prior to any permitted exports of Schedule 3 chemicals to nonmember states. However, this will not be required if the product contains no more than 30 percent of a Schedule 3 chemical, and it is identified as consumer goods packaged for retail sale for personal use or packaged for individual use

26.8 General Licenses/License Exceptions

(a) Export Permit Exemptions

The RIER provides for certain exemptions from the requirement to obtain an export permit. In particular, an export permit will not be required if the goods in question are not controlled exports and are:

- Personal or household effects, other than motor vehicles, that accompany passengers, crew, or employees of transport undertakings by land, sea, or air; are not being transported for sale but are intended for the personal or household use of such passengers, crew, or employees of transport undertakings; and where the household effects are being transported for the purpose of a transfer of residence of the owner;
- Being exported by parcel post;
- Diplomatic correspondence;
- Being exported by the joint defence force (including the Singapore Armed Forces, the Singapore Police Force and the Singapore Civil Defence Force), including personal and household effects of its officers but excluding civilian motor vehicles; or the Ministry of Foreign Affairs, including personal and household effects of its officers but excluding motor vehicles;
- Used motor vehicles covered by Carnet de Passage, which are endorsed by the Automobile Association of Singapore;
- Trade samples, specimens for analysis or test, and gifts, the total value of which does not exceed S$400;
- Commercial, shipping, or airline documents; press photographs or negatives; news write-ups, news clippings, news films or news transcription tapes;
- Human corpses, human remains, human bones, or cremated ashes; or
- Human transplant materials.

In addition, an export permit will also not be required where the goods in question are not controlled exports, have a total value that does not exceed S$1,000, and are being exported by air as manifested cargoes or hand-carried goods. However, an export permit is required before goods can be exported under the Hand-Carried Exports Scheme (HCES), regardless of the value and quantity of goods. Further information on the HCES can be found at https://www.iras.gov.sg/taxes/goods-services-tax-(gst)/general-gst-schemes/hand-carried-exports-scheme-(hces).

(b) Strategic Goods Permit Exemptions

The SGCA provides that strategic goods permits are not required for any contract for the acquisition, disposal, or transmission of any technology, or

of any document in which any technology is recorded, stored, or embodied, or for the transmission of any technology, to the extent that this is necessary to facilitate:

- The installation, operation, maintenance, or repair of any goods that have been exported, transshipped, or brought in transit (where a permit has been obtained or is not required for such export, transshipment, or bringing in transit);
- An application for a patent; or
- Any research in the technology the results of which have no practical application.

Further, under the Strategic Goods (Control) Regulations, the prohibition against the export of strategic goods or strategic goods technology without a strategic goods permit will not apply to:

- Any act authorized by or carried out for or on behalf of the government;
- The export, transshipment, or bringing in transit of any goods or document that is brought into Singapore by a military, naval, or air force of a foreign government (not being a visiting force) in the course of duty, or the transmission of any technology that is brought into Singapore or received by that force from its government;
- The export, transshipment, or bringing in transit or transmission of any goods, document, or technology by or on behalf of a visiting force in the course of duty; or
- Diplomatic correspondence.

(c) Chemical Weapons License Exemption

The export of Schedule 1 chemicals will always require a NA(CWC) license, pursuant to the CWPA.

However, under the Chemical Weapons (Prohibition) Regulations 2007, the export of Schedule 2 and Schedule 3 chemicals without a license will be permitted where the export is to a member state, and the mixture to be exported contains not more than the following concentrations of controlled chemicals:

- Thirty percent or less by weight of a chemical specified in item B of Part 2 of the Schedule to the Act; and

- Thirty percent or less by weight of a Schedule 3 chemical.

26.9 Penalties, Enforcement, and Voluntary Disclosures

(a) Penalties for Failure to Comply with Export Requirements

The RIER provides that the following activities shall constitute offences and shall be liable on conviction to the following penalties:

Prohibited Activity	**Penalty**
The export of goods out of Singapore without the requisite permit	• First conviction: fine not exceeding S$100,000 or three times the value of the goods in respect of which the offence was committed (whichever is greater), or imprisonment for a term not exceeding two years, or both • Second or subsequent conviction: fine not exceeding S$200,000 or four times the value of the goods in respect of which the offence was committed (whichever is greater), or imprisonment for a term not exceeding three years, or both
The export of prohibited goods, as sanctioned by the UNSC	
The despatch of goods by the exporter without the prior submission of the export permit	
The failure to return the permit within the requisite time period after the goods have been exported	
The counterfeiting or falsification of a permit, or use of a counterfeited or falsified permit	
The knowing or reckless making of statements that are false or misleading in a material particular, in applications for export permits	

Similarly, the SGCA provides that any exporter who exports strategic goods without the requisite strategic goods permit shall be guilty of an offence and liable on conviction to:

- For a first conviction, a fine not exceeding S$100,000 or three times the value of the goods or technology in respect of which the offence was committed (whichever is greater), or imprisonment for a term not exceeding two years, or both; and
- For a second or subsequent conviction, a fine not exceeding S$200,000 or four times the value of the goods or technology in respect of which the offence was committed (whichever is greater), or imprisonment for a term not exceeding three years, or both.

In addition, the CWPA provides that any person who commits the following prohibited activities shall be liable for the following penalties:

Prohibited Activity	**Penalty**
Transfer (e.g., export) of Schedule 1 chemicals for a permitted purpose without the requisite license	Fine not exceeding S$100,000 or imprisonment for a term not exceeding ten years, or both
Export of Schedule 2 or Schedule 3 chemicals without the requisite license	Fine not exceeding S$10,000 or imprisonment for a term not exceeding two years, or both

Please note that the list of prohibited activities outlined here is non-exhaustive. Other prohibited activities, and their penalties, may be found in the CA, the RIER, or other applicable statutes and their subsidiary legislation.

(b) Voluntary Disclosure Program

1. Singapore Customs offers a nonstatutory Voluntary Disclosure Programme (VDP) for traders to voluntarily come forward to disclose errors and omissions or contraventions with the applicable laws. This facilitates voluntary compliance, by encouraging traders to take an active role in identifying and remedying problems.
2. In order to be eligible for the VDP, the individual or company must meet the following requirements:
    - The disclosure must be complete with all the relevant information pertaining to the error or omission in question; and
    - The disclosure must be made before any notice of commencement of an audit or investigation by Singapore Customs.

A VDP submission must be made using the VDP form. In addition, the following relevant supporting documents must also be submitted:

- The permit;
- The invoice;
- The packing list;
- The bill of lading/air waybill; and
- Any other applicable documents.

For noncompliance relating to strategic goods, additional information is required. Further information on this, and the respective VDP forms, can be

found at https://www.customs.gov.sg/businesses/compliance/voluntary-disclosure-programme.

26.10 Recent Export Enforcement Matters

Apart from encouraging traders to practice self-compliance methods (e.g., via the VDP) and having post-clearance audit practices in place, Singapore Customs also continuously ensures that the export requirements are satisfied by exporters through an active enforcement program. Several recent published cases have been highlighted:

- August 31, 2022: A former director of scrap metal trading companies was fined a sum of S$558,000 for furnishing false statements when applying for Preferential Certificates of Origin (PCO) for exported goods.[18]
- June 28, 2022: A director of a freight forwarding company was fined a sum of S$7,000 for failing to retain the trade documents relating to the export of goods between March and June 2021.[19]
- March 14, 2022: A director of 3 companies pleaded guilty to charges relating to the violation of the Democratic People's Republic of Korea regulations under the UNA by supplying luxury items to North Korea. The director was sentenced to 6 weeks' imprisonment. The fines imposed on the three companies amounted to S$363,000 in total.[20]
- October 4, 2021: A director of a freight forwarding company was fined a sum of S$105,000 for fraudulent evasion of Goods and Services Tax and for abetting another person to furnish false information to Singapore Customs.[21]
- May 3, 2019: A former company director of a freight forwarding company was fined a sum of S$109,000, or more than 20 months' jail in default, for submitting incorrect customs declarations in respect of the shipping company, goods description, and quantity of goods. The former company director had also breached permit conditions requiring dutiable goods to be stored in a place approved by Singapore Customs if they were not exported.[22]

26.11 Special Topics

There are no special topics to be covered in relation to export controls and economic sanctions in Singapore.

26.12 International Economic Sanctions Imposed by Singapore

Singapore has a dual approach sanction regime. Singapore, as a member of the UN, implements sanctions imposed by UNSC resolutions through the UNA, whilst regulating financial institutions through section 27A of MASA. The UNA was enacted to enable Singapore to fulfill its obligations respecting Article 41 of the Charter of the United Nations (UN Charter).

Each sanctioned state is provided for through subsidiary legislation (listed here), and is detailed in the Seventh Schedule of the RIER.

- United Nations (Freezing of Assets of Persons—Sudan) Regulations 2006;
- United Nations (Sanctions—Central African Republic) Regulations 2020;
- United Nations (Sanctions—Democratic People's Republic of Korea) Regulations 2010;
- United Nations (Sanctions—Democratic Republic of the Congo) Regulations 2006;
- United Nations (Sanctions—Iran) Regulations 2019;
- United Nations (Sanctions—Libya) Regulations 2021;
- United Nations (Sanctions—Mali) Regulations 2020;
- United Nations (Sanctions—Somalia) Regulations 2021;
- United Nations (Sanctions—South Sudan) Regulations 2019; and
- United Nations (Sanctions—Yemen) Regulations 2015.

Apart from implementing UN sanctions, Singapore also imposed sanctions and restrictions against Russia on March 5, 2022, which aim to constrain Russia's capacity to conduct war against Ukraine.[23] Specifically, Singapore has imposed export controls on items that can be directly used as weapons to inflict harm on or to subjugate the Ukrainians, as well as items that can contribute to offensive cyber operations. In this regard, Singapore has imposed a ban on the transfer to Russia of (1) all items in the Military Goods List and (2) all items in the "Electronics," "Computers," and

“Telecommunications and Information Security” categories of the Dual-Use Goods List of the Strategic Goods (Control) Order 2021. Singapore has also imposed financial measures targeted at designated Russian banks, entities and activities in Russia, and fund-raising activities benefiting the Russian government. These measures apply to all financial institutions in Singapore, including banks, finance companies, insurers, capital markets intermediaries, securities exchanges, and payment service providers.

26.13 Brokering Controls

Brokering controls in Singapore are provided for under the SGCA[24] and are enforced by Singapore Customs. Any person who is brokering (i.e., arranging, negotiating, or doing any act to facilitate the arrangement or negotiation of) goods or technology that the person has been notified, knows, or has reasonable grounds to suspect are intended, or likely, to be used, wholly or in part, for or in connection with the development, production, handling, maintenance, storage, detection, identification or dissemination of any nuclear, chemical, or biological weapon, or development, production, maintenance, or storage of missiles capable of delivering any nuclear, chemical, or biological weapons will need a brokering permit from Singapore Customs. Do exercise caution as the broad phrasing of “know or have reasonable grounds to suspect,” implies that the obligation to acquire a brokering permit applies even if the goods are not listed strategic goods.

Other categories of strategic goods requiring a brokering permit pursuant to the Strategic Goods (Control) (Brokering) Order 2021 include goods within ML1 to ML4, and ML8, and strategic goods technology prescribed under ML21 and ML22.

Brokering permit applications will require particulars of the Company and any other parties who will be involved in the transactions, information on the goods, and end-user’s information and the intended end use of the goods. The application is accessible here: https://form.gov.sg/#!/5d09da39be47a30011f73872.

Lastly, all registered brokers in Singapore are required to submit a half-yearly report on brokering activities that have been carried out during that period by the 30th day of June and December annually. The report must include:

- Contract reference;
- Dates;
- Description of item;
- Strategic goods product code;
- Quantity;
- Value; and
- The name and address of supplier and end user.

As added compliance, Singapore Customs may request an audit and verification of records by an authorized officer at any time.

26.14 Blocking Statutes

Singapore does not have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes.

---

1. Head, Competition & Antitrust and Trade, Rajah & Tann Asia Singapore LLP.
2. Singapore Statutes Online, Customs Act 1960, https://sso.agc.gov.sg/Act/CA1960.
3. Singapore Statutes Online, Regulation of Imports and Exports Act 1995, https://sso.agc.gov.sg/Act/RIEA1995.
4. Singapore Statutes Online, Strategic Goods (Control) Act 2002, https://sso.agc.gov.sg/Act/SGCA2002.
5. Singapore Statutes Online, Chemical Weapons (Prohibition) Act 2000, https://sso.agc.gov.sg/Act/CWPA2000.
6. Singapore Statutes Online, United Nations Act 2001, https://sso.agc.gov.sg/Act/UNA2001.
7. Singapore Statutes Online, Monetary Authority of Singapore Act 1970, https://sso.agc.gov.sg/Act/MASA1970.
8. Singapore Statutes Online, Terrorism (Suppression of Financing) Act 2002, https://sso.agc.gov.sg/Act/TSFA2002.
9. See https://www.enterprisesg.gov.sg/non-financial-assistance/for-singapore-companies/free-trade-agreements/ftas/singapore-ftas for the list of multilateral FTAs.
10. United Nations, Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (1993), https://treaties.un.org/doc/Treaties/1997/04/19970429%2007-52%20PM/CTC-XXVI_03_ocred.pdf.
11. Basel Convention, Basel Convention on the Control of Transboundary Movement of Hazardous Wastes and Their Disposal (1989), https://www.basel.int/Portals/4/Basel%20Convention/docs/text/BaselConventionText-e.pdf.
12. Singapore Statutes Online, Regulation of Imports and Exports Regulations, https://sso.agc.gov.sg/SL/RIEA1995-RG1.
13. https://www.customs.gov.sg/businesses/strategic-goods-control/permit-and-registration-requirements/intangible-transfer-of-technology-itt/.
14. https://www.un.org/securitycouncil/content/un-sc-consolidated-list.
15. Singapore Statutes Online, Regulation of Imports and Exports (Amendment) Regulations 2022, https://sso.agc.gov.sg/SL-Supp/S183-2022/Published/20220315.
16. https://www.tradenet.gov.sg/TN41EFORM/tds/sp/splogin.do?action=init_acct.

17. https://www.tradenet.gov.sg/tradenet/portlets/search/searchHSCA/searchInitHSCA.do.
18. Singapore Customs (31 August 2022) *Media Release: Director fined $558,000 for making false statements in applications for Preferential Certificates of Origin*, https://www.customs.gov.sg/files/Singapore_Customs_Press_Release_31_Aug_Final.pdf.
19. Singapore Customs (28 June 2022) *Media Release: Director of Freight Forwarding Company Fined $7,000 for Failing to Retain Documents*, https://www.customs.gov.sg/files/Singapore_Customs_Press_Release_28_June_Final.pdf.
20. Public Prosecutor v Sindok Trading Pte Ltd and other appeals [2022] SGHC 52.
21. Singapore Customs (4 October 2021) *Media Release: Director of Freight Forwarding Company Fined $105,000 for Offences under Customs Act*, https://www.customs.gov.sg/news-and-media/media-releases/2021-10-04-Media-Release.pdf.
22. Singapore Customs, (9 May 2019) *Media Release: Former Company Director Fined $109,000 for Incorrect Customs Declarations and Breach of Permit Condition*, https://www.customs.gov.sg/news-and-media/media-releases/2019-05-09-Media-Release.pdf.
23. Ministry of Foreign Affairs, (5 March 2022) Sanctions and Restrictions Against Russia in Response to Its Invasion of Ukraine, https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/03/20220305-sanctions.
24. Strategic Goods (Brokering) (Control) Order 2019, https://sso.agc.gov.sg/SL/SGCA2002-S534-2019?DocDate=20190801.

27

Export Controls and Economic Sanctions in South Korea

Andrew Park

27.1 Overview

(a) What Is Regulated?

South Korea is a member of the Wassenaar Arrangement and the Australia Group, but is not a party to the Missile Technology Control Regime or the Nuclear Suppliers Group. The South Korean licensing authority for dual-use items is the South Korean Ministry of Trade, Industry and Energy (MOTIE).

According to MOTIE, laws relevant to South Korea's export control system include the Foreign Trade Act; the Defense Acquisition Program Act; the Nuclear Safety Act; and the Act on the Control of the Manufacture, Export and Import of Specific Chemicals and Chemical Agents for the Prohibition of Chemical and Biological Weapons (Prohibition of Chemical and Biological Weapons Act).

An exporter needs to obtain an export license if a product and/or technology involved in the transaction is classified as "strategic item." Strategic items include a wide variety of items specifically categorized as industrial dual-use items, nuclear energy exclusive items, and military goods. The individual list and confirmations on whether an item is a strategic item can be found at https://www.yestrade.go.kr/search/search.do?method=intro.

It should be noted that the Korean government operates a comprehensive online export control system called Yestrade. All export control-related tasks, including applying for export licenses, can be processed online through Yestrade. The key services provided by Yestrade include application for export licenses, searches for application status, and issuance of export license.

(b) Where to Find the Regulations

The Korea Law Translation Center's (KLTC's) website is available at https://elaw.klri.re.kr/kor_service/main.do and provides texts of laws and regulations that are published in both Korean and English. An English version of the website is also available at https://elaw.klri.re.kr/eng_service/main.do. However, accessing the English version of the website will only allow access to the English translations of the Korean laws and regulations, while the Korean version will allow access to the Korean laws and regulations in the original Korean version as well as the English translations of the same. Information on relevant regulations are also placed on the website of the Yestrade (only available in Korean).

(c) Who Is the Regulator?

The Financial Services Commission is the central government body responsible for financial policy and supervision. Financial Supervisory Service is the regulator responsible for the supervision of financial institutions. MOTIE is the regulator responsible for the Foreign Trade Act with regard to Arms Embargo and related restrictions. The Ministry of Justice is the regulator responsible for travel bans. The Ministry of Unification is the regulator responsible for the travel ban with regard to North Korea.

(d) How to Get a License

Any person or entity that intends to export "strategic items" must obtain "export permission" from the pertinent government agencies. For any person or entity that intends to export goods that do not fall within the category of any strategic items but have high potential of being

appropriated for manufacturing, developing, using, or storing weapons of mass destruction or missiles as carriers of such weapons, the person or entity must obtain "situational permission." Details on the license are prescribed in the Public Notice on Trade of Strategic Goods (Public Notice). Application for an export license can be processed online through Yestrade.

(e) Key Websites

- Yestrade website is available at https://www.yestrade.go.kr/. Yestrade is a portal for exports control related tasks including filing application for export permits of strategic items and application for classification of goods. The website is only available in the Korean language.
- Korea Strategic Trade Institute (KOSTI) website is available at https://www.kosti.or.kr/intro.do. KOSTI was established to oversee the implementation of the exports controls and support the exporter and importers.
- Korea International Trade Association's (KITA's) website is available at http://kita.org/.
- Korea Customs Service provides information on import and export clearance and customs clearance procedures and other valuable information relating to the customs administration, and an English version of the website is available at https://www.customs.go.kr/english/cm/cntnts/cntntsView.do?mi=8056&cntntsId=2732.

27.2 Structure of the Laws and Regulations

(a) International Treaties

South Korea participates in multilateral export control regimes on strategic items including the Wassenaar Arrangement (WA), the Nuclear Suppliers Group (NSG), the Missile Technology Control Regime (MTCR), the Australia Group (AG), and the treaties including the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (CWC); the Biological Weapons Convention (BWC); and the Arms Trade Treaty (ATT).

(b) South Korea's National Laws and Regulations on Export Controls

(i) Customs Act

According to Article 241 of the Customs Act, all goods entering or leaving South Korea's border must undergo customs clearance procedures, which include making import or export declaration to, and acceptance of, such declaration by the head of the Korea Customs Service (KCS).

However, exporting of strategic items, including the dual-use and military items listed in Appendix 2 and 3, respectively, of the Public Notice on Trade of Strategic Goods and Technologies ("Public Notice") requires approval from the relevant authorities to maintain international peace and security in accordance with multilateral export control regimes on strategic items (Article 1 and 2 of the Public Notice).

(ii) Foreign Trade Act

The Foreign Trade Act is the main pillar for regulating all matters concerning trade. This includes the exportation and importation of goods, services, and intangible goods in electronic form.

According to Article 19 of the Foreign Trade Act, MOTIE is given the authority over the export of strategic items. An approval from the head of the MOTIE is required for exporting dual-use items that fall under the Category 1 to 9 on Appendix 2 of the Public Notice, which are listed in Section 27.2(c).

(iii) Defense Acquisition Program Act

According to Article 57 of the Defense Acquisition Program Act, the Defense Acquisition Program Administration (DAPA) is given the authority to regulate the export of certain defense industry materials or dual-use items that are intended to be used for military purposes and an approval from DAPA is required for exporting certain defense industry materials or dual-use items. These items are listed in Appendix 3 of the Public Notice, and are considered strategic items.

(iv) Nuclear Safety Act

The Nuclear Safety and Security Commission (NSASC) is given the authority under Article 107 of the Nuclear Safety Act to control exports of atomic-related materials listed in Category 10 in Appendix 2 of the Public Notice.

(v) Act on the Control of the Manufacture, Export and Import of Specific Chemicals and Chemical Agents for the Prohibition of Chemical and Biological Weapons ("Prohibition of Chemical and Biological Weapons Act")

Article 11 of this act regulates the export of certain chemicals and biological agents or toxins that can be used in the manufacture of chemical weapons and biological weapons.

(vi) Act on Safety Management of Guns, Swords, Explosives, Etc.

Article 9 of this act regulates the export of guns, swords, explosives, gas sprayers, electroshock weapons, and crossbows that have no military use, which may contribute to the maintenance of public safety.

(vii)Chemicals Substances Control Act

Article 21 of this act regulates the export of restricted and prohibited chemicals to prevent risks posed by chemicals to people's health and the environment, and to protect the lives and property of the people or the environment.

(viii)Narcotics Control Act

Article 6-2 of this act regulates the export of narcotic drugs, psychotropic drugs, marijuana, or other basic substances to contribute to improving the health of the general public and prevent harm or danger to the public health from misuse or abuse of such substances.

(ix) Plant Protection Act

Article 28 of this act requires inspections of plants and plant material exports to conserve the natural environment by providing for matters necessary for phytosanitary measures for agricultural and forestry production.

(x) Wildlife Protection and Management Act

Articles 16 and 21 of this act regulates the export of endangered and certain non-endangered wildlife and endangered species to prevent the extinction of wildlife and maintain the ecosystem in equilibrium.

(xi) Inter-Korean Exchange and Cooperation Act

Article 13 of this act requires approval from the Ministry of Unification for any exchange of items, or trading with North Korea.

(xii)Transboundary Movement, etc. of Living Modified Organisms Act

Article 20 of this act requires notification in advance to the head of the relevant central administrative agency for persons who intend to export living modified organisms prescribing the items, quantity, and exporting country.

(c) Controlled Lists

- The list of dual-use items provided in Appendix 2 (dual-use items) of the Public Notice:
  Category 1—Special Materials and Related Equipment
  Category 2—Materials Processing
  Category 3—Electronics
  Category 4—Computers
  Category 5—Telecommunications and Information Security
  Category 6—Sensors and Lasers
  Category 7—Navigation and Avionics
  Category 8—Marine
  Category 9—Aerospace and Propulsion
  Category 10—Nuclear Materials, Facilities and Equipment
- The list of military items provided in Appendix 3 (military items) of the Public Notice.
- Both lists are made publicly available in both Korean and English at https://www.yestrade.go.kr

(d) South Korea and UN Security Council Sanctions

South Korea is a member state of the UN and supports and carries out measures taken by the UN. Article 2 of the Guidelines on Payments and Receipts for the Fulfilment of Obligations for International Peace and Security Maintenance (the "Guidelines") provides a sanctions list, as follows:

1. Fourteen of the UN Security Council (UNSC) Resolutions
   - UN Resolutions No. 751 (1992) and No. 1907 (2009) on Somalia and Eritrea
   - UN Resolutions No. 1267 (1999), No. 1989 (2011), and No. 2253 (2015) on ISIL and Al-Qaeda
   - UN Resolution No. 1518 (2003) on the Hussein government of Iraq
   - UN Resolution No. 1521 (2003) on Liberia
   - UN Resolution No. 1533 (2004) on DR Congo
   - UN Resolution No. 1572 (2004) on Côte d'Ivoire
   - UN Resolution No. 1591 (2005) on Sudan
   - UN Resolution No. 1718 (2006) on Democratic People's Republic of Korea (DPRK)
   - UN Resolution No. 2231 (2015) on Iran
   - UN Resolution No. 1970 (2011) on Gaddafi government Libya
   - UN Resolution No. 1988 (2011) on the Taliban in Afghanistan
   - UN Resolution No. 2127 (2013) on the Central Africa Republic
   - UN Resolution No. 2140 (2014) on Yemen
   - UN Resolution No. 2206 (2015) on South Sudan
2. Three U.S. Executive Orders
   - U.S. Executive Order: EO 13324 on Terrorism
   - U.S. Executive Order: EO 13382 on Iranian Financial Sanctions Regulations (IFSR)
   - U.S. Executive Order: EO 13573 and 13582 on Syria
3. Sanctioned Parties by the Council of the European Union
4. Other persons designated by the Minister of Economy and Finance according to the Guidelines after consultation with the heads of related central administrative agencies, including the Minister of Foreign Affairs; Minister of Unification; Minister of Trade, Industry and Energy; and the Chairman of the Financial Services Commission, to protect the safety of the nation and the lives of people.

5. Any individual residing in or an organization located in Iran, except for those subject to economic sanctions as listed in Subsections (1) to (4).

The Guidelines are available in Korean at: http://www.law.go.kr/행정규칙/국제평화및안전유지등의의무이행을위한지급및영수허가지침/(2017-39,20171228)

(e) South Korea's National Laws on Economic Sanctions

South Korea implements the UNSC's resolutions through its existing laws and regulations, such as the Foreign Trade Act, the Foreign Exchange Transactions Act, and the Customs Act, as well as by enacting enforcement decrees or notices to implement specific measures.

(i) Criminal Economic Sanctions

- Act on Prohibition Against the Financing of Terrorism and Proliferation of Weapons of Mass Destruction ("Prohibition of Financing Terrorism Act")

  Under Article 6 of this act, any person who violates this act may be punished by imprisonment with labor for not more than ten years or by a fine not exceeding 100 million won.
- Foreign Exchange Transactions Act

  Under Article 27-2 of the act, any person who violates this act may be punished by imprisonment with labor for not more than three years or by a fine not exceeding 300 million won, so long as the 300 million won does not exceed triple the value of the object related to the violation.
- Foreign Trade Act

  Under Article 53 of the act, a person in violation of this act may be punished by imprisonment with labor for not more than seven years or by a fine not exceeding five times the value of goods that are exported, transit, transshipped, or brokered.

  For criminal economic sanctions offences, the prosecution and the police investigate, the prosecution files charges, and the court decides the final punishment according to the Criminal Procedure Act.

(ii) Civil Economic Sanctions

Under Article 7 of the Prohibition of Financing Terrorism Act, any financial company that makes a negligent transaction, may be punished by a fine not exceeding 20 million won.

The Financial Services Commission is authorized to investigate and enforce civil economic sanctions violations.

(f) South Korea's Sanctioned Parties Lists

The Ministry of Economy and Finance maintains a list of sanctioned parties, which was last released on December 2, 2016. The list reflects the UN and OFAC's lists of sanctioned parties, and such list is available in Korean at: http://www.moef.go.kr/com/bbs/detailComtPolbbsView.do?menuNo=5020200&searchBbsId1=MOSFBBS_000000000039&searchNttId1=MOSF_000000000006720#

27.3 What Is Regulated: Scope of the Regulations

In accordance with section 3 of the Foreign Trade Act, the Foreign Trade Act serves as the general act on import and export of strategic items. The Nuclear Safety Act; the Defense Acquisition Program Act; the Inter-Korean Exchange and Cooperation Act; and the Act on the Control of the Manufacture, Export and Import of Specific Chemical Substances and Biological Agents for the Prohibition of Chemical and Biological Weapons regulate the import and export of the relevant goods respectively.

In accordance with Article 26 of the Foreign Trade Act, the aforementioned acts are implemented by the Public Notice. Korean export controls apply to any items falling under the lists of controlled items mentioned in Section 27.3. The list of controlled items in the Appendix 2 and 3 of the Public Notice include all items regulated by the aforementioned acts.

Exportation of such items from Korea are subject to special export control clearance, that is, the exporter would need to obtain an export control license (or export permit). In certain cases the importation of dual-use products might also be subject to export control requirements. Determination and application for permit may be done online on Yestrade website.

According to Articles 5 through 12 of the Public Notice, exporters may apply for an advanced determination of items to confirm whether an item is classified as a controlled item by the pertinent government agency. If the item is determined to be a controlled item, the exporter must obtain export permit. This process may be conducted online on the Yestrade website.

27.4 Who Is Regulated?

According to Article 2 of the Foreign Trade Act, South Korea's laws and regulations on export control must be observed by all traders regardless of their citizenship who are importing or exporting the goods into South Korea's border.

27.5 Classification

(a) Classification of Dual-Use Items

As stated in Section 27.2(c), Dual-Use Items subject for export control are listed in Appendix 2 of the Public Notice.

(b) Classification of Military Items

As stated in Section 27.3, Classification of Military Items subject for export control are listed in Appendix 3 of the Public Notice.

27.6 General Prohibitions/Restrictions/Requirements

As explained in Section 27.2(b)(i), an importer or exporter must file an import or export declaration for all goods to be imported or exported in accordance with the Customs Act and must follow import or export clearance procedures. Noncompliance with the relevant laws or regulations on import or export controls may result in civil or criminal penalties (refer to Section 27.9).

27.7 Licensing/Reasons for Control

(a) Types of Export Control Licenses and Permits for Dual-Use Items

As stated in Section 27.1(d), export permits/licenses related to strategic items are as follows:

- Individual permit (Articles 19 to 26 of the Public Notice): Individual export permits are given to a confirmed amount of controlled items;
- Comprehensive permit (Articles 28 to 40 of the Public Notice): Exporters who are designated by the pertinent government agencies as having established the "Internal Compliance Program" pursuant to Article 79 may apply for a comprehensive permit that allows the exporter to export the subject items for a certain time period to a designated buyer in a designated country. With the permit, the exporter may decide the amount of the exported items at its discretion.
- Catchall permit (Articles 50 to 52 of the Public Notice): For items that are not listed as "strategic items" but that may be regulated depending on the circumstances; exporters that intend to export such items that may be potentially used to manufacture weapons of mass destruction, etc., to countries/region categorized as group Na. Items listed in Appendix 2-2 are also subject to this permit;
- Brokerage permit (Articles 53 to 55 of the Public Notice): Brokerage permit is required when engaging in transfer of strategic items from a third-party country to another third-party country. For each brokerage engagement, a separate permit is required; and
- Transfer permit (Article 56 of the Public Notice): Transfer permits are required for transportation service providers who intend to transfer or transship strategic items.

(b) Export Control Licensing Procedure

An exporter who wants to obtain export license/permit must register and submit an online application on the Yestrade website. Generally, the licensing procedure is completed within 15 days from the date the application was submitted (excluding the time that may be required for examination of the technologies, cooperating/communicating with the relevant government agencies or institutions).

The procedure may vary slightly depending on the final destination country of the exportation. It should be noted, however, if the exported items are transferred in countries/regions categorized Ga-2 or Na (defined next), then such countries/regions are respectively deemed as "final destination" with respect to export controls, and thus require permits/licensing. According to Article 10, Table 6, of the Public Notice, counties/regions are categorized into three groups:

- Region Ga-1: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States
- Region Ga-2: Japan
- Region Na: other countries and regions that are not listed as Region Ga-1 and/or Ga-2

(c) Import and Export Licenses for Military Items

With regard to importation of military items, the Certificate of Purpose of Importation pursuant to Articles 57 to 65 of the Public Notice is required. This certificate is valid up to one year.

With regard to exportation licenses, refer to the procedure stated in Section 27.7(b).

(d) Export Permits and Independent Expert Examination

Application for expert examination of the strategic items may be conducted online on the Yestrade website. The pertinent government agency for issuing the export permit has authority to conduct the examination.

27.8 License Exceptions

Article 26 of the Public Notice lists the exceptions to individual export licenses in the case of exporting nontechnology items with the strategic items that fall under one of the following (not including when in any of the subsections; the final destination state is Sudan, Syria, or North Korea; or the items transits or transships through one of those countries):

1. When exporting nontechnology of the strategic items,
    - The importer shall submit to the head of the licensing agency the export transaction report within seven days after exporting the strategic items;
    - An additional document proving the transaction between the two parties shall be submitted if the party who claimed the items within the country is different from the party returning the items; or
    - If the return destination is located in a country other than the original export country, an additional document must be attached to prove that it is the return destination.
2. When exporting technology of the strategic items,
    - To a member country of the WA;
    - To a country other than the member countries of WA, the total goods exported shall be no more than US$10,000;
    - If a foreign employee who has entered into an employment contract with the same corporate entity is transferred to the relevant foreign employee within the scope necessary for performing their duty; or
    - If the exportation of technology is necessary for the projects carried out under the science and technology cooperation agreement and exchange program approved by the Minister of Foreign Affairs, or under the cooperation agreement that the Korean government executed with the international organization, and the head of the licensing agency recognized the strategic item is eligible for exemption from licensing requirement considering the level of technology and details of the cooperation agreement and after consultation with the Minister of Science and Technology Information and Communication.
3. When transferring technology, transferred from a foreigner, back to the person who originally transferred such technology;
4. When a person who re-exports strategic items, such person shall report the fact that the items are being re-exported to the Minister of Trade, Industry and Energy or the head of the relevant administrative agency within 30 days from the date import declaration has been made; or

5. When the exporter disposes of strategic items after being exempted from obtaining an export license, the exporter shall submit a certificate of disposal to the Minister of Trade, Industry and Energy or the head of the relevant administrative agency.

27.9 Penalties, Enforcement, and Voluntary Disclosures

(a) Administrative Penalties

According to Article 59 of the Foreign Trade Act, persons who violate the restrictions on exports of strategic items will be subject to an administrative fine not exceeding KRW 20 million (approx. US$1,700). In addition, the Minister of Trade, Industry and Energy or the head of the relevant administrative agency may place a restriction on exportation or importation of strategic items, in part or in whole, for a period up to three years.

(b) Criminal Penalties

According to Article 53 of the Foreign Trade Act, any person who falls under any of the following will be punished by imprisonment with labor for not more than five years or by a fine not exceeding three times the value of goods, which are exported, imported, transit, transshipped, or brokered:

- A person who violates a restriction or ban on exportation or importation;
- A person who exports strategic items without export permission;
- A person who obtains export permission by fraud or other improper means;
- A person who exports any goods, etc., subject to situational permission without the situational permission;
- A person who transits or transships strategic items, without transit or transshipment permission; or
- A person who engages in brokering strategic items, without a brokerage permission.

Also according to Article 53 of the Foreign Trade Act, if the person who engaged in the aforementioned activities with the intention of international diffusion of strategic items, will be punished by imprisonment with labor

for not more than seven years or by a fine not exceeding five times the value of goods, and so on, which are exported, transit, transshipped, or brokered. Any attempted crimes will also be treated as the completion of the relevant principal crime for the purpose of criminal penalties.

Additionally, under Article 57 of the Foreign Trade Act, if a representative of a corporation, or an agent, employee of a corporation, or an individual commits the aforementioned crime, the corporation or individual will be also subject to the criminal penalties.

(c) Enforcement

In accordance with Article 59 of the Foreign Trade Act, administrative fines will be imposed and collected by the Minister of Trade, Industry and Energy, the Mayor or the Do Governor, or the head of the relevant administrative agency.

Following general criminal legal procedures in accordance with the Criminal Procedure Act, investigations are conducted by the police. If there is substantial grounds of the accused crimes, prosecutors will file for prosecution to initiate the criminal trial procedure.

(d) Voluntary Disclosures

Korean entities or individuals are not legally required to report any unveiled violation of Foreign Trade Act and relevant regulations, for no applicable regulation imposes such obligation.

27.10 Recent Export Enforcement Matters

According to Article 31 of the Foreign Trade Act, the MOTIE may place a restriction on exportation or importation of strategic items in part or in whole for a maximum of three years to those who export the strategic items without export permission, export any goods subject to situational permission without obtaining such permission, or violate any of the multilateral export control regimes.

Further, under Article 49 of the Foreign Trade Act, the MOTIE may issue an order to take a training course for eight hours or fewer to any person who exported goods without receiving export permission or

situational permission; received export permission or situational permission by fraud or other improper means; transit, transshipped or brokered without transit or transshipment or brokerage permission; or obtained transit or transshipment permission. According to the MOTIE, in the third quarter of 2019, the MOTIE placed a restriction on exportation or importation of strategic items to a total of two corporate entities and issued 27 orders to take the training course.

According to the National Intelligence Service, the number of cases of illegal exportation of strategic items from 2015 to 2019 is as follows: 2015 (4), 2016 (4), 2017 (4), 2018 (8), and 2019 (9). The number of cases of illegal exportation has increased significantly in 2018 and 2019 when North Korea suspended its nuclear and long-range missile tests. However, there has not been a reported case where the destination of strategic items was North Korea.

27.11 Special Topics

(a) Re-exports/Extraterritorial Application of Laws

According to the Korean Security Agency of Trade and Industry, re-exportation of strategic items also requires re-export permits. The procedure is similar to the export permit/licensing procedure and can be conducted online on the Yestrade website.

(b) Intangible Transfer of Technical Information

Korean export control regulations do not provide clear guidance on intangible transfer of controlled items. The current legislation does not provide special documents for formalization of such transfers.

(c) Recordkeeping

Article 88 of the Public Notice stipulates the traders to keep documents and records related to export/import control operations for at least five years and submit the documents and records upon the Head of the pertinent government agency that issued permits/licenses.

(d) How to Be Compliant When Exporting to the Republic of Korea

The Korean importer should classify the item to determine whether the items to be delivered in Korea are "strategic items," such as the items listed in the dual-use or military lists in Appendix 2 and 3 of the Public Notice. If the times are classified as strategic items, under Article 45 of the Public Notice, the importer must obtain the Certificate of Purpose of Importation from the pertinent government agencies, confirming the purpose/use of the imported items and that the importer will not transfer, transship, or export the subject items.

(e) How to Be Compliant When Exporting from the Republic of Korea

1. The Korean exporter should classify the item:
   - Determine if the delivery could be restricted or prohibited (i.e., by comparing description/key words with the dual-use/military lists in Appendix 2 and 3 of the Public Notice) under Korean law;
   - In cases of doubt:
     – The exporter may use the online self-examine tool provided by Yestrade[1] to see whether the subject goods/technologies are subject to Korean export control or not. It should be noted that the result of this self-examination tool is merely a guide; the exporter will still be held responsible for the accuracy of the result of self-examination.
     – The exporter may apply online Yestrade for classification of the subject goods/technologies by the pertinent government agency.
2. On the basis of results of classification, the Korean exporter should:
   - Under Article 66 of the Public Notice, provide a timely report to the KOSTI on the controlled export operations, and properly record export control transactions (documents must be kept for five years);
   - If items are subject to export control, apply for an export license;
   - If items are not subject to export control, export license is not required (report of the trade may be required depending on the

circumstance).

27.12 Encryption Controls

(a) General Comments

Generally, in accordance to Appendix 2 of the Public Notice, an individual export license is required to export encryption items that are categorized as encryption items. However, according to Article 26 of the Public Notice, the licensing requirement is waived in the following circumstances:

- If the encryption items (Control Nos. 5A002.a.1–5A002.a.4, 5B002, and 5D002) are exported for the purpose of (1) establishing and operating an internal system of a private enterprise, or (2) for the development and production of products for the private use of a private enterprise, and the final destination state is a member of WA or is a private sector end user is headquartered in one of the countries listed in Appendix 23 of the Public Notice; or
- If the encryption items categorized as encryption items due to system management-only encryption functions (SNMP, SSH) (Control Nos. 5A002.a.1–5A002.a.4, 5B002, and 5D002) are being exported (provided, that the items that fall under a different control number will not be included).

(b) Import Encryption Clearance Requirements

The import clearance requirement is the same as any other goods. However, if the encryption items are classified as strategic goods, which require an import license, then the trader of such encryption items shall obtain a Certificate of Purpose of Importation as stated in Section 27.11(d).

(c) Encryption Licensing Requirements

As stated in Section 27.12(a), generally, an individual export license is required to export encryption items that are categorized as encryption items, but such licensing requirements may be waived under the circumstances described in the same section.

(d) Penalties for Violation of Encryption Regulations

The licensing requirement is not waived for the encryption items that are considered strategic items. If the licensing requirement is violated, such act of violation will be deemed as exporting the strategic items without export permission under Article 53 of the Foreign Trade Act, which is punishable by imprisonment with labor for not more than seven years or by a fine not exceeding five times the value of the strategic items that were exported.

27.13 Blocking Laws/Penalties for Compliance with Sanction Imposed by Other Countries

Currently, there is no law that blocks compliance with the sanction imposed by other countries against South Korea, nor is there any penalty for compliance with such sanctions.

1. https://www.yestrade.go.kr

28

Export Controls and Economic Sanctions in Switzerland

Raphael Brunner and Maura Décosterd[1]

28.1 Overview

(a) What Is Being Regulated?

In general, Switzerland does not impose any unilateral export controls or sanctions as a result of its commitment to remain neutral with regard to international relations. However, as a member of the United Nations since 2002, and a member of the relevant international export control regimes, Switzerland's export control regime reflects these international treaties and aims to support the fight against terrorism and to promote the nonproliferation of weapons of mass destruction.

Switzerland's export control laws and regulations apply to goods and services, payment and capital transfers, the movement of persons, as well as scientific and technological exchanges, thereby establishing rules applicable to the Swiss customs territory, Swiss public customs warehouses, warehouses for bulk goods, bonded warehouses and Swiss customs-free zones, as well as the transfer of intangible technology. These export control laws apply to individuals and legal entities involved in the sale and export of products and technologies classified as dual-use and military items. These dual-use and military items include a wide range of goods and technologies that may be used for or in connection with the creation of weapons of mass destruction and other sensitive items.

In terms of economic sanctions, Switzerland may apply arms embargoes, restrictions on admissions of listed persons, freezing of assets of listed persons, or economic sanctions, including import and export restrictions on specific economic activities, sectors, and/or goods. As a member of the UN since 2002, Switzerland enacts UN sanctions regimes and may enact the sanctions regimes of Switzerland's main trading partners (predominantly the EU). With respect to EU sanctions, Switzerland has the option to either implement measures against the circumvention of EU sanctions via the Swiss territory or it may implement such sanctions directly. Only by applying emergency law and to protect Switzerland's own interests, the Swiss Federal Council may implement unilateral measures, which need however to be limited in time.

(b) Where to Find the Regulations

All Swiss laws and regulations are available on the official website of Swiss administration in all four official languages (German, French, Italian, Rumansch) and partially, but not officially, in English: www.fedlex.admin.ch/en/home.

An overview of the basic principles of Swiss export controls can be found on the website of the regulator, Switzerland's State Secretariat for Economic Affairs (SECO): www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/ruestungskontrolle-und-ruestungskontrollpolitik--bwrp-/bewilligungswesen/grundlagen-der-exportkontrollpolitik.html.

The Swiss sanctions regulations can be found on SECO's website at: www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/ruestungskontrolle-und-ruestungskontrollpolitik--bwrp-/rechtliche-grundlagen.html.

(c) Who Is the Regulator?

Export controls of war material, dual-use goods, and chemicals are regulated by various federal acts. The acts provide the Federal Council with wide-ranging freedom to implement the details and scope of the laws in various so-called Ordinances. The State Secretariat for Economic Affairs

(SECO) is the implementing, licensing, supervisory, and enforcement authority.

Based on the Federal Act on the Implementation of International Sanctions (Embargo Act, SR 946.231), the Swiss Federal Council was granted the ability to enact compulsory measures in order to implement sanctions that have been ordered by the United Nations, the Organization for Security and Cooperation in Europe (OSCE), and Switzerland's most significant trading partners (EU and USA), and which serve to secure compliance with international law, and in particular the respect of human rights.

SECO has extensive monitoring and enforcement powers relating to export controls and sanctions. A breach of applicable sanctions or export control regulations can result in criminal prosecution. SECO has limited power to impose administrative penalties and initiate criminal proceedings, and severe offenses are subject to criminal prosecution by the Attorney General of Switzerland and the competent courts.

SECO is part of the Federal Department of Economic Affairs and represents the Swiss government entity tasked with the implementation and enforcement of Swiss economic sanctions policy. In cooperation with the Federal Department of Economic Affairs' Directorate of International Law and the Federal Customs Administration, SECO publishes and drafts amendments to legislation relating to sanctions. Policy and legal decisions concerning sanctions issues are within the competence of the Federal Council.

SECO has the responsibility to monitor compliance with sanctions and export controls. It cooperates with the Federal Department of Justice and Police, the Federal Department of Finance, the Federal Customs Administration, and the State Secretariat for Migration.

SECO is also the regulatory authority tasked with issuing export control licenses. Occasionally, it publishes guidance documentation on its website: www.seco.admin.ch/seco/en/home.html.

SECO may be reached at:

Staatssekretariat für Wirtschaft SECO, Holzikofenweg 36, CH – 3003 Bern

Email: sanctions@seco.admin.ch

www.seco.admin.ch/

(d) How to Obtain a License

SECO is responsible for licenses under export control regulations as well as sanctions regimes. The specific licensing requirements are to be found in the respective export control or sanctions ordinances. Where a license is required, an application must be submitted to SECO via its electronic licensing system, called ELIC, found at www.seco.admin.ch/seco/en/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/elic.html.

SECO can only issue a license when the preconditions for granting a license are entirely met. These requirements may be found in the relevant ordinances.

If it is uncertain whether a particular transaction is prohibited or requires a license, the exporter may request a "ruling" from SECO by submitting a description of the proposed transaction and the underlying documents to SECO via ELIC, and SECO will issue a position on the respective matter (so-called "Nullbescheid" or "clearing").

(e) Key Resources

Key resources on export controls are found in the respective acts and regulations on war materials, dual-use goods, their annexes, as well as some additional ordinances. Guidance may be found on the SECO homepage at www.seco.admin.ch.

Because the Swiss Federal Council, like the UN or EU, uses "smart sanctions," which are individually designed for each specific country, situation, or entities linked to sanctionable activities, it is essential to check SECO's home page to find the applicable and current regulations.

28.2 Structure of the Laws and Regulations

(a) International Treaties

Switzerland is a signatory to many international treaties on export controls, and its national regulations draws from those treaties. In particular, Switzerland is part of the following treaties:

- The Convention on Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (1972)
- The Australia Group (AG; 1987)
- The Nuclear Suppliers Group (NSG; 1991)
- The Missile Technology Control Regime (MTCR; 1992)
- The Biological Weapons Convention (1995)
- The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA; 1996)
- The Chemical Weapons Convention (1997)
- The Organization for the Prohibition of Chemical Weapons (OPCW; 1997)
- Charter of the United Nations (2002)
- The Arms Trade Treaty (ATT; 2013)

(b) Swiss National Laws and Regulations on Sanctions and Export Controls

- Federal Act on the Implementation of International Sanctions (Embargo Act, EmbA; CC 946.231)
- Federal Act on War Material (War Material Act, WMA; CC 514.51)
- Ordinance on War Material (War Material Ordinance, WMO; CC 514.511)
- Federal Act on Weapons, Weapon Accessories and Ammunition (Weapons Act, WA; CC 514.54)
- Ordinance on Weapons, Weapon Accessories and Ammunition (Weapons Ordinance, WV; CC 514.541)
- Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods (Goods Control Act, GCA; CC 946.202)
- Ordinance on the Export, Import and Transit of Dual Use Goods, Specific Military Goods and Strategic Goods (Goods Control Ordinance, GCO; CC 946.202.1)
- Ordinance on the Export and Brokerage of Goods for Internet and Mobile Communications Surveillance (IMO; CC 946.202.3)
- Federal Act on Explosives (EA; CC 941.41)
- Explosives Ordinance (EO; CC 941.411)

- Federal Act on Private Security Services Provided Abroad (PSSA; CC 935.41)
- Nuclear Energy Act (NEA; CC 732.1)
- Nuclear Energy Ordinance (NEO; CC 732.11)
- Safeguards Ordinance (CC 732.12)
- Chemicals Control Ordinance (CWC; CC 946.202.21)

(c) Lists of Controlled Goods

- GCO
- Annexes 1 and 2: Dual-use Goods
- Annex 3: Military Goods
- Annex 4: Strategic Goods (currently empty)
- Annex 5: Goods subject to national export controls (weapons and explosives)
- WMO, Annex 1: War material
- Ordinance on measures in connection with the situation in Ukraine, Annex 1: Strategic goods
- Ordinance of measures against Syria
- Annex 1: Goods for Internal Repression
- Annex 1a: Chemicals and Other Materials

(d) Switzerland and UN Security Council Sanctions

As a member of the UN, Switzerland implements UN Security Council resolutions through its Embargo Act. Switzerland implements sanctions imposed by UN Security Council resolutions via ordinances issued by the Federal Council on the basis of the Embargo Act. The Federal Council may also enact independent measures to safeguard Swiss interests.

While not a member of the EU (or EEA—European Economic Area), Switzerland may adopt parts of the EU's sanctions regimes in order to preempt any circumvention of EU measures through Switzerland.

(e) Swiss National Laws on Economic Sanctions

Switzerland may enact measures to implement sanctions that have been adopted by the United Nations, the Organization for Security and Cooperation in Europe (OSCE), or by Switzerland's most significant

trading partners and which serve to secure compliance with international law, and the respect of human rights, in particular (Art. 1 para. 1 EmbA). Additionally, the Federal Council has the authority to implement measures to safeguard the interests of the country in accordance with Art. 184 para. 3 of the Federal Constitution (Art. 1 para. 2 EmbA).

(f) Swiss Sanctioned Parties Lists

The Swiss Sanctioned Parties lists are, depending on the enacted sanctions, based on the UN and EU lists (Art. 1 para. 1 EmbA) and can be found at: www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos/sanktionsmassnahmen.html.

A comprehensive sanctions list search tool is found on SECO's website at https://tinyurl.com/yzwqvga5.

Switzerland currently applies sanctions against the following parties/countries:

- People and organizations linked to Usama bin Laden, Al-Qaida, or the Taliban
- Iraq
- Myanmar (Burma)
- Zimbabwe
- Sudan
- The Democratic Republic of Congo
- People linked to the assault on Rafik Hariri
- Belarus
- Democratic People's Republic of North Korea
- Lebanon
- Iran
- Somalia
- Guinea
- Libya
- Syria
- Guinea-Bissau
- The Central African Republic
- Russia
- Yemen

- Burundi
- Republic of South Sudan
- Republic of Mali
- Venezuela
- Nicaragua

28.3 What Is Regulated: Scope of the Regulations

The GCA/GCO regulate the export, import, transit, and brokerage of (1) nuclear goods, goods usable for civilian and military purposes (dual-use goods), and specific military goods that are subject of nonbinding international control measures; (2) strategic goods that are subject to international agreements; and (3) goods subject to national export controls (Art. 1 GCO).

The WMA/WMO regulate the trade, brokerage, import, export, and transit of war material as well as the transfer of intellectual property, including know-how and the granting of rights thereto (Art.1 para. 1 WMO).

The WA/WV regulate the acquisition, import into Switzerland, export, storage, possession, carrying, transport, brokerage, manufacture of, and trade in (1) weapons, essential or specially designed weapon components, and weapon accessories; (2) ammunition and ammunition components (Art. 1 para. 2 WA).

The EA/EO regulate the manufacture and transfer of explosives, pyrotechnical objects, and gunpowder (Art. 1 para. 1 EA).

The NEA/NEO regulate (1) nuclear goods, (2) nuclear installations, and (3) radioactive waste that is generated in nuclear installations, or that has been delivered in accordance with Art. 27 para. 1 of the Radiation Protection Act of 22 March 1991 (RPA).

The MCO regulates the export and brokering abroad of the internet and mobile telephony interception equipment listed in the Annex as well as the transfer of intellectual property, including know-how, and the granting of rights thereto, provided that they relate to the goods listed in the Annex and are made to a natural or legal person resident or domiciled abroad or to a foreign government agency (Art. 1 MCO).

EmbA: Switzerland may enact legislation based on the Embargo Act in order to implement sanctions that have been adopted by the United Nations,

OECD, or by Switzerland's most significant trading partners and which serve to secure compliance with international law, in particular the respect of human rights (Art. 1 para. 1 EmbA). Switzerland may implement compulsory measures that directly or indirectly restrict transactions involving goods and services, payment and capital transfers, and the movement of persons, as well as scientific and technological exchanges, and includes prohibitions, licensing, and reporting obligations as well as other restrictions of rights (Art. 1 para. 3 EmbA).

The PSSA applies to legal entities and business associations (companies) that (1) provide, from Switzerland, private security services abroad; (2) provide services in Switzerland in connection with private security services provided abroad; (3) establish, base, operate, or manage a company in Switzerland that provides private security services abroad or provides services in connection therewith in Switzerland or abroad; (4) exercise control from Switzerland over a company that provides private security services abroad or provides services in connection therewith in Switzerland or abroad (Art. 2 para. 2 PSSA).

The Safeguard Ordinance applies to nuclear materials within the meaning of Art. 1 NEO (possession, import, and export); certain plants with and without nuclear material; as well as the manufacture, assembly, and construction of certain nuclear equipment (Art. 2 of the Safeguard Ordinance).

The CWC applies to the chemicals listed in the Annex (Art. 1 para. 2 CWC).

28.4 Who Is Regulated?

The Swiss export control and sanction regulations apply based on the principle of territoriality to individuals, legal entities, and business associations (companies) that are registered or domiciled in Switzerland (Art. 5 para. 1 and Art. 10 GCO) and any individuals or entities acting within the territory of Switzerland that engage mainly in the import, export, transit, or brokerage of the regulated goods and services on Swiss customs territory, Swiss public customs warehouses, warehouses for bulk goods, bonded warehouses, and Swiss customs-free zones (Art. 1 para. 2 WMO/GCO) or any other relevant activities (banking and finance, contract negotiations, asset management, etc.).

28.5 Classification

(a) Classification of Dual-Use Items

The GCA/GCO regulate the export, import, transit, and brokerage of goods usable for civilian and military purposes (dual-use goods), specific military goods, and strategic goods (Art. 1 GCA). Dual-use goods are those goods that may be used both for civilian and military purposes (Art. 3 lit. b GCA).

Dual-use goods are listed in Annex 2 to the GCO and can be categorized as follows:

0. Nuclear materials, installations, and equipment
1. Special materials and equipment
2. Material processing
3. General electronics
4. Computers
5. Telecommunications and “Information Security”
6. Sensors and lasers
7. Avionics and navigation
8. Marine and ship technology
9. Aeronautics, space, and propulsion

(b) Classification of Military Items

Specific military goods are taken to mean those that have been designed or modified for military purposes, but which are neither weapons, ammunition, explosives, nor any other means of combat, together with military training aircraft equipped with suspension points (Art. 3 lit. c GCA). Military goods are listed in Annex 3 to the GCO and include weapons, weapon systems, ammunition and military explosives, equipment specifically designed or modified for combat operations, or for use in combat and not normally also suitable for civil use.

A component is not considered to be “specially designed” within the meaning of Annex 3 to the GCO if, although manufactured for a specific customer and end use, it:

1. Has the same functions and performance and is equivalent in “form and fit” to a component not covered by the annexes to the SHI,

meaning the component itself, respectively its design has not been amended for customer or use;
2. Consists of components that are made up of components not covered by the annexes to the SHI components, are new, or otherwise combined;
3. “Unfinished,” that is, for the use of which at least one major production step is still required; or
4. Is a passive part of the lowest two integration levels.

For the export of goods listed in Annex 2 Part 2, Annex 3 or 5 to the GCO to countries that participate in all of the international control regimes that are non-binding under international law and are supported by Switzerland, SECO may grant an ordinary general export license (OGL). Annex 7 to GCO lists these countries (Art. 12 para. 1 GCO).

Any person who wishes to export goods from Switzerland that they know or have reason to believe are intended for the development, manufacture, use, passing on, or the deployment of weapons of mass destruction (WMD) must request a license from SECO if (1) the goods are not listed in Annexes 2–5; or (2) exceptions to the licensing requirement apply (catch-all clause; Art. 3 para. 4 GCO).

28.6 General Prohibitions/Restrictions/Requirements

Every export or transfer of export-controlled items requires that export control formalities are met. In case of omission, the respective individual or legal entity may face criminal prosecution for violating the applicable export control regulations.

General prohibitions apply for nuclear, biological, and chemical weapons (Art. 7 WMA), anti-personnel mines (Art. 8 WMA), cluster munition (Art. 8a WMA), and the direct and indirect financing (Art. 8b and 8c WMA) of these war materials. Also, explosives and pyrotechnic articles that are unstable or particularly sensitive to external influences may neither be manufactured in nor imported into Switzerland (Art. 15 EA).

28.7 Licensing/Reasons for Control

(a) Types of Export Control Licenses and Permits for Dual-Use Items

The Swiss export control regime includes three different types of licenses: individual licenses (Art. 8 GCO), an ordinary general export license (art. 12 GCO–OGL), and an extraordinary general export license (Art. 13 GCO–EGL).

Individual licenses apply to certain specific activities and persons or entities.

Ordinary general export licenses (OGL) may be granted by SECO for the export of goods listed in Annex 2 Part 2, Annex 3 or 5 to the GCO to countries that participate in all the international control measures that are non-binding under international law and are supported by Switzerland. Annex 7 GCO contains a list of these countries. SECO may also grant an OGL for the export of goods listed in Annex 4 GCO to EU countries or to countries that the EU has concluded a cooperation agreement on the European Satellite Navigation Programs.

Exceptional general export licenses (EGL) may be granted for the export of goods listed in Annex 2 Part 2, Annex 3 or 5 to the GCO to countries other than those in accordance with Annex 7 GCO considering the specific circumstances.

(b) Export Control Licensing Procedure

Licenses are issued by SECO only to natural persons or legal entities that are domiciled or have their registered office or permanent establishment on the Swiss customs territory or in a Swiss customs-free zone. SECO may authorize exceptions in justified cases. Where the license is for a legal entity, the applicant must provide SECO with proof of reliable internal controls on compliance with the export control regulations (i.e., an internal compliance program or ICP).

For the export of firearms, their parts and components and accessories, as well as ammunition and ammunition parts and components, an import certificate from the destination country must also be submitted unless the recipient is a foreign government or a company acting for a foreign government. Instead of the import certificate, proof may be provided that such a certificate is not required (Art. 5 GCO).

SECO is authorized to refuse to issue a license (in accordance with Art. 6 para. 1 lit. a and b GCA) if there is reason to believe that the goods that are to be exported:

1. Are intended for the development, manufacture, use, passing on, or deployment of NBC weapons;
2. Contribute to the conventional armament in a country to an extent that leads to increased regional tension or instability or an escalation in an armed conflict; or
3. Will not remain in the possession of the declared end recipient.

There may also be grounds for refusal (Art. 6 para. 1 lit. b GCA) where:

1. A partner country has refused the export of a similar good to the same end recipient;
2. The country of origin notifies Switzerland that it must consent to the re-export and such consent is not forthcoming; or
3. The destination country prohibits the import (Art. 6 GCO).

SECO may request the following documents from applicants for individual licenses: company profiles; order confirmations, contracts of sale, or invoices; an import certificate from the recipient state; and end-use certificates from the end recipient (Art. 8 GCO).

General export licenses are granted only to legal entities that are entered in the Swiss or Liechtenstein commercial register. Universities and public institutions are exempt from this requirement. The natural person or the officers of the legal entity making the application must not have received a legally binding conviction in the two years prior to filing of the application for offences against the applying export control regulations (Art. 10 GCO).

SECO may request the following documents in particular from applicants for general export licenses: company profiles, internal control programs (ICP), and reports on the goods exported in terms of the general export license (Art. 11 GCO).

Individual and general licenses are valid for two years. Individual licenses may be extended by two years on one occasion (Art. 9 and 14 GCO).

(c) Licenses for War Materials

The Swiss export control regulations for war materials are based on a dual licensing requirement. First, the regulated activity requires an initial license to ensure the compliance with national interests. Second, a specific license is required for the import, export, transit, or brokerage of the regulated good to recipients abroad.[2]

Anyone who, on Swiss territory, wishes to manufacture war material and wishes to trade in war material for his own account or for the account of another, or to broker war material on a professional basis for recipients abroad, irrespective of the location of the war material, requires an initial license (Art. 9 WMA).

Specific licenses can be granted through a brokerage license, import license, export license, transit license, license to enter into agreements relating to the transfer of intellectual property, including know-how, or the granting of rights thereto; and trading license (Art. 12 WMA).

(d) Post-shipment Verification Checks

As a general rule, an export license may be granted only if it relates to a delivery to a foreign government or to an undertaking acting on behalf of a foreign government, and if a declaration is provided by that government stating that the material will not be re-exported (a non-re-export declaration; Art. 18 WMA).

Art. 5a para. 3 of the WMO enables SECO to verify compliance with the non-re-export declaration on site as part of a post-shipment verification (PSV). This provision was added to the WMO by the Federal Council following an incident in 2012 where hand grenades exported from Switzerland to the United Arab Emirates in 2003 and 2004 appeared in the possession of insurgents in Syria. Since then, SECO started to perform PSVs since it is considered one of the best methods for preventing exported war material from being passed on to undesirable recipients. Switzerland was the first country in Europe to introduce this PSV measure.[3]

28.8 General Licenses/License Exceptions

(a) General Licenses

- WMA/WMO: Anyone who on Swiss territory (1) wishes to manufacture war material; (2) wishes to trade in war material for his own account or for the account of another, or (3) to broker war material on a professional basis for recipients abroad, irrespective of the location of the war material, requires an initial license (Art. 9 WMA).

  With respect to the activities that require a license in terms of the WMA, a distinction is made between the following specific licenses: brokerage license; import license; export license; transit license; license to enter into agreements relating to the transfer of intellectual property, including knowhow, or the granting of rights thereto; and trading license (Art. 12 WMA).
- GCA/GCO: Any person who wishes to export nuclear goods from Switzerland in accordance with Annex 2 Part 1, dual-use goods, in accordance with Annex 2 Part 2, special military goods, in accordance with Annex 3, strategic goods, in accordance with Annex 4, or goods subject to national export controls in accordance with Annex 5 requires an export license from SECO.

  Any person who wishes to export nuclear goods from Switzerland in accordance with Annex 2 Part 1 with the export control numbers (ECN) 0C001 or 0C002 requires a license from the Swiss Federal Office of Energy (SFOE). This requirement also applies to goods with ECN 0D001 or 0E001 where these are software or technology for goods with ECN 0C001 or 0C002. In these cases, the SFOE takes the place of SECO in relation to the application of the other provisions of this ordinance.

  Any person who wishes to export goods from Switzerland that comprise parts and components of a good in accordance with Annex 2 or 3 requires a license from SECO if the parts and components are among the main elements of this good or make up more than 25 percent of its value in accordance with Article 9 of the Ordinance of 12 October 2011 on International Trade Statistics.

  Any person who wishes to export goods from Switzerland that they know or have reason to believe are intended for the development, manufacture, use, passing on, or the deployment of NBC weapons must request a license from SECO if (1) the goods are

not listed in Annexes 2–5 or (2) exceptions from the license requirement are given (Art. 3 GCO).

(b) License Exceptions

- WMA: No initial license is required by those who (1) supply as sub-contractors companies in Switzerland that hold an initial license; (2) execute orders from the Swiss government in respect of war material for the Swiss armed forces; (3) manufacture, trade in, or acts as a professional broker outside Switzerland for firearms under the legislation on weapons, their components or accessories, or their munitions or munitions components and who therefore holds a license to trade arms under the legislation on weapons; (4) manufactures or trades in Switzerland in explosives, pyrotechnic devices, or propellant powder covered by the legislation on explosives and who therefore holds a license under the legislation on explosives (Art. 9 para. 2 WMA).

  Any person who manufactures war material in Switzerland in his own production plant may broker or trade abroad without a specific license only if an initial license for the brokerage or the trade of products analogous to those manufactured in the production plant has been granted (Art. 6 para. 1 WMO). No specific license is required for the brokerage of or the trade in war material involving states listed in Annex 2 WMO; however, dealers and professional brokers always require an initial license (Art. 6 para. 2 WMO).
- GCO: No export license is required for (1) goods in accordance with Annexes 2–5 that are being returned to the original supplier, provided they have not achieved a technical increase in value; (2) chemicals in accordance with Annex 2 Part 2 with ECN 1C111 or ECN 1C350, provided they are used as samples and the total quantity per supply amounts to less than 1 kg; Article 14 paragraph 1 letter a of the Chemicals Control Ordinance of 21 August 20131 remains reserved; (3) firearms with their parts and components and accessories as well as the ammunition and ammunition parts and components pertaining thereto, which are covered by Annex 3 or 5 and exported to a country in accordance with Annex 6; (4) firearms with the ammunition pertaining thereto that security agents employed by foreign states re-

export following prearranged official visits; (5) firearms with the ammunition pertaining thereto that security agents employed by Switzerland export for prearranged official visits abroad, provided they re-import these weapons into Switzerland thereafter; (6) goods that are exported by Swiss troop units and their members for international operations or for training purposes; (7) goods that are re-exported by foreign troop units and their members following training in Switzerland; (8) hunting and sports weapons with the ammunition pertaining thereto that are credibly shown to be needed by persons for hunting, sports shooting, or martial arts abroad, provided these weapons are re-imported into Switzerland thereafter; (9) hunting and sports weapons with the ammunition pertaining thereto that are credibly shown to be needed by persons for hunting, sports shooting, or martial arts in Switzerland, provided these weapons are re-exported thereafter (Art. 4 GCO).

28.9 Penalties, Enforcement, and Voluntary Disclosures

(a) Export Control Laws and Regulation

Negligently or intentionally violating the War Material Act or its ordinances or the Goods Control Act or its ordinances may lead to criminal prosecution and penalties such us fines and/or imprisonment of up to ten years depending on the violation and the level of fault.

(b) Sanctions Laws and Regulations

Swiss courts take several circumstances into account when determining criminal penalties for a breach of sanctions regulations, such as the seriousness of the criminal conduct, the number of exports, and whether the breach was committed with negligence or intent (level of fault).

The following options are available for sanctions breaches:

- In case of an intentional violation of an ordinance based on the Embargo Act, a fine of a maximum of 500,000 Swiss francs can be imposed by the Swiss courts (Art. 9 para. 1 EmbA).

- In a serious case, the penalty is imprisonment of up to five years, which can be combined with a fine of a maximum of one million Swiss francs (Art. 9 para. 2 EmbA).
- In a case of negligence, a fine of a maximum of 100,000 Swiss francs can be imposed (Art. 9 para. 3 EmbA).

A maximum fine of 100,000 Swiss francs can be imposed on anyone who willfully (1) refuses to provide information, to hand over documents, or to allow access to business premises in terms of Article 3 and Article 4 paragraph 1, or who provides false or misleading information in this connection or (2) in the absence of culpable conduct that would constitute any other criminal offence, violates in any other manner the terms of this act or any provision of an ordinance in terms of Article 2 paragraph 3, provided such violation is declared to be subject to prosecution, or any order issued and that carries a reference to the liability to penalties under this article (Art. 10 para. 1 EmbA). Attempts and aiding and abetting can also lead to prosecution (Art. 10 para. 2 EmbA). In the event that the offence is committed through negligence, the penalty is a fine of a maximum of 40,000 Swiss francs (Art. 10 para. 3 EmbA). The prosecution of respective infringements is subject to a statute of limitations of five years. This statute of limitation may be extended under specific preconditions for an additional two and a half years (Art. 10 para. 4 EmbA).

When sanctions regulations are breached within an organization, the responsible managers can be subject to criminal prosecution if they negligently or intentionally violate a legal obligation, or do not avoid a breach of sanctions regulations by their subordinates, for example, by not implementing organizational measures ensuring the organizations compliance with sanction laws.

(c) Enforcement

Other than imposing criminal penalties against the violation of sanctions regulations, SECO has various powers to enforce the respective regulations: the power to confiscate assets, the power to require the provision of certain information, or to enter business premises, and the power to process and share personal data.

As property and assets are subject to coercive measure under the Embargo Act, they can be confiscated in the event that their lawful use is

not guaranteed, regardless of whether the particular person is criminally liable or not.

As a second option, Swiss authorities can enter and inspect the business premises of individuals who are subject to a duty of disclosure, without any prior notice. The visit can be carried out during normal working hours and includes the examination of relevant documents. The authorities can, in this case, also seize any incriminating material and require information and documentation necessary for appropriate controls.

The third option for the enforcement of sanctions regulations in Switzerland is the power to process data which can be shared with other Swiss authorities. The data can eventually even be disclosed to foreign authorities, organizations or bodies and includes data relating to the nature, quantity, place of destination, purpose, use and recipients of good, relating to persons involved in the manufacture, supply or brokerage and also relating to certain financial aspects of the underlying transfer.

In practice, the Swiss government heavily emphasizes the upholding of the principles of international law and the enforcement of international sanctions, even if it is not able to actively pursue all breaches of sanctions due to its limited resources. Therefore, the system mostly relies on voluntary disclosures from companies. The amount of such submitted disclosures is not made public, but if enforcement measures are applied, typically these are fines, rather than imprisonment. When this happens, companies usually do not appeal, and cases remain undisclosed. The amount of the fine depends on the individual facts of each case; with certain reductions in cases where a voluntary disclosure is submitted. An example of a fine based on voluntary disclosure is the Iran sanctions prior to the “Iran nuclear deal” due to violations of the standalone funds transfer controls, which were not disputed.

(d) Voluntary Disclosures

There is no legal basis for voluntary self-disclosure in the Swiss sanctions regulations, but it is accepted in practice and typically results in a mitigation of penalties. Still, there is no industry-specific duty in Switzerland to disclose violations of sanctions regulations.

28.10 Recent Export Enforcement Matters

In 2017, an American company was charged for unauthorized export of goods with cryptographic functions as dual-use goods according to Art. 14 para. 1 lit. a GCA, since the goods were classified in ECN 5A002.a1 of Annex 2 to the GCO. The company had to pay a criminal penalty of 9,000 Swiss francs and a fine of 1,000 Swiss francs.[4]

In 2019, the Federal Department of Foreign Affairs reported a criminal offence to the Federal Prosecutor, as the Swiss aircraft company Pilatus Flugzeugwerke AG did not comply with PSSA by performing maintenance work on military aircrafts for Saudi Arabia, even though SECO had permitted the activity from an export control perspective. The Federal Prosecutor suspended the trial, while the Federal Department of Foreign Affairs banned Pilatus from supplying their services in Saudi Arabia and the United Arab Emirates.[5]

28.11 Special Topics

(a) Re-exports/Extraterritorial Application of Laws

Only the Federal Act on Private Security Services provided Abroad (PSSA) has extraterritorial reach. The PSSA applies to legal entities and business associations (companies) that:

- Provide, from Switzerland, private security services abroad;
- Provide services in Switzerland in connection with private security services provided abroad;
- Establish, base, operate, or manage a company in Switzerland that provides private security services abroad or provides services in connection therewith in Switzerland or abroad; or
- Exercise control from Switzerland over a company that provides private security services abroad or provides services in connection therewith in Switzerland or abroad (Art. 2 para. 1 PSSA).

Any company intending to carry out one of those listed activities shall declare it to the competent authority (Art. 10 para. 1 PSSA).

In case of a direct participation in hostilities (Art. 8 PSSA) or serious violation of human rights (Art. 9 PSSA), a company may face imprisonment of up to three years or a monetary penalty.

(b) Intangible Transfer of Technical Information

The transfer of technical information—such as data stored on hardware, knowhow on data carriers, or by means of cloud computing or knowledge transfer by people—falls under Art. 2 GCA. Technology includes information for the development, manufacture, or use of goods that is neither generally accessible nor serves the purposes of pure scientific research.

Thus, not all data transmission across borders requires a license. Therefore, it is important to check whether the transmitted data crossing the Swiss border can be assigned to an export control number (ECN) in Annexes 2–5 to the GCO. If the data is to be outsourced to a server, the location of the server is decisive for the authorization of the transmission. Access on regulated data from abroad already constitutes an export within the meaning of the GCO (Art. 3 para. 1). The authorization procedure is carried out via SECO's electronic licensing approval platform, ELIC.

If the data cannot be assigned an ECN, the transmission does not require a license. In this case Art. 3 para. 4 GCO applies, by which a person who wishes to export goods that they know or have reason to believe are intended for the development, manufacture, use, passing on, or the deployment of NBC weapons must request SECO for a license if the goods are not listed in Annexes 2–5 or exceptions from the license requirement are made.

The last step involves checking whether the specific country, to which data is transmitted, requires a license according to a Swiss sanctions regulation.

Business trips abroad, frontier workers, and home offices in foreign customs territory do not count as export, provided that technologies covered by the GCO are not made available to third parties. The data carriers must be secured (VPN access, encryption) and not accessible by third parties abroad. Printouts fall under this exception provided that they are (at all times) under the control of the "exporter" and are not made available to third parties.

(c) Practical Issues Related to Export Control Clearance

Export control clearances are granted via SECO's electronic licensing system, ELIC. The license number has to be declared as part of the customs

export declaration. To obtain a license, companies need to provide SECO with information about the transaction and are requested to provide additional information.

The following documents are mandatory:

- Statement of end user or recipient
- Invoice, proforma-invoice, offer, consignment note
- Product description (e.g., prospectus, data sheet, drawing, picture)
- Internal Control Program for export controls (ICP)
- Technical assessment on the classification of goods
- The following documents are requested but not mandatory:
- Order confirmation/order
- Contract
- Company profile
- Import license
- Re-export license
- Official documents
- Others

(d) Recordkeeping

Records must be maintained on the manufacture, purchase, sale, or brokerage of or any other form of trade in war material, as well as contracts entered into in terms of Art. 20 WMA. The records must, at all times, disclos: the entries, exits, and stocks of war material; the names and addresses of suppliers, purchasers, and contractual parties; and the data and subject matter of commercial transactions.

The following documents must be available for inspection for a period of ten years in order to substantiate records: invoices from suppliers; copies of invoices addressed to purchasers and contractual parties; where payment is made in cash, receipts for the goods signed by the purchasers; contracts relating to transactions relating to intellectual property, including know-how pertaining to war material; and transport documents with details of the transit states (Art. 17 WMO).

In general, all essential documents relating to the export of regulated goods must be retained for ten years after customs clearance and must be submitted to the responsible authorities on request (Art. 18 para. 4 GCO).

(e) How to Be Compliant When Exporting to Switzerland

For goods covered by the WMO and certain goods covered by the GCO, an import license is required. Import licenses as well as export licenses can only be requested by Swiss domiciled entities/persons.

To identify a potential license requirement, companies should:

- Classify the goods according to the annexes to the WMO and GCO and identify any import license requirement under goods control regulations
- The order of review is:
  1. Annex 1 WMO
  2. Annex 3 GCO
  3. Annex 2 GCO
- Identify any other license requirement with the HS Code of the good via Swiss customs system TARES
- Apply for relevant licenses from the relevant authorities

(f) How to Be Compliant When Exporting from Switzerland

- Classify the goods according to the annexes to the WMO and GCO and identify any export license requirement under goods control regulations
- The order of review is:
  1. Annex 1 WMO
  2. Annex 3 GCO
  3. Annex 2 GCO
  4. Annex 4 GCO
  5. Annex 5 GCO
- Identify any other license requirement with the goods' HS Code via Swiss customs system TARES
- Apply for relevant licenses from the relevant authorities

28.12 Encryption Controls

(a) General Comments

The GCO covers goods with encryption technology within the Category 5 Part 2 of Annex 2 GCO.

(b) Import Encryption Clearance Requirements

There are no specific clearance requirements for the import of encryption technology.

(c) Encryption Licensing Requirements

There are no specific licensing requirements for encryption.

General Software Note Annex 1 to the GCO may release software from a license requirement if, among other things, the software is publicly available or where the object code represents the minimum necessary for the installation, operation, maintenance, or repair of goods for which an export license has been granted. This release is not applicable to software specified in Category 5 Part 2 ("Information Security"), which would always require a license for export from Switzerland.

(d) Penalties for Violation of Encryption Regulations

There are no specific fines for violations of license requirement for the export of encryption technology. Fines are defined as described in Section 28.9.

28.13 Blocking Laws/Penalties for Compliance with Sanction Imposed by Other Countries

Blocking laws or penalties for compliance with sanctions imposed by other countries are not applied in Switzerland.

---

1. Raphael Brunner is Legal Partner and Maura Décosterd is Senior Legal Advisor, MME, Zurich, Switzerland.
2. SECO, Factsheet—Overview of the Basic Principles of Export Controls, at 2.
3. *Id*. at 6.
4. Decision of the Federal Court from 1st of June 2018, 6B_1032/2017.
5. www.seco.admin.ch/seco/en/home/seco/nsb-news.msg-id-75587.html.

29

Export Controls in Taiwan

Benson Yan[1]

29.1 Overview

(a) What Is Regulated?

Taiwan's regulations on export controls are based on the Regulations Governing Export and Import of Strategic High-tech Commodities (the "SHTC Regulations"), which was first introduced in 1994 pursuant to Article 13 of the Foreign Trade Act (Article 13, Foreign Trade Act). Although not a member of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Good and Technologies (WA), Taiwan voluntarily and substantially adheres to WA's control lists. Any individual, legal entity, or group engaged in the export business must observe the export controls regulations in Taiwan. However, there is a wide variety of reasons for implementing restrictions and/or controls on the import and the export trade, and many such reasons (e.g., hygiene, culture, ecology, environment, etc.) are not relevant to the type of export controls to be discussed here and will not be covered by this outline.

(b) Where to Find the Regulations

The regulations and other relevant information may be found at the website of the Bureau of Foreign Trade (BOFT), www.trade.gov.tw. However, information may be available only in the local language and not necessarily in English.

(c) Who Is the Regulator?

The Ministry of Economic Affairs (MOEA) is the regulatory authority under the Foreign Trade Act; however, the agency under the MOEA responsible for the official business is the BOFT, which deals with the formulation and implementation of trade policies, among other things.

(d) How to Get a License

The exporter shall apply for a Strategic High-tech Commodities (SHTC) export license with the BOFT. Such an export license may be applied for electronically and may take from three to seven days for the BOFT to process in the case of going to a nonrestricted region; however, it may take up to 25 to 45 days in the case of going to a restricted region (which is defined in Section 29.2(f) Taiwan Sanctioned Parties Lists).

(e) Key Websites

The website of the BOFT is www.trade.gov.tw, and that of the MOEA is www.moea.gov.tw

29.2 Structure of the Laws and Regulations

(a) International Treaties

Taiwan is not a member of WA, Nuclear Suppliers Group (NSG), Australia Group (AG), Missile Technology Control Regime (MTCR), Chemical Weapons Convention (CWC), or the Treaty on Non-proliferation of Nuclear Weapons, but it voluntarily conforms to these established controls.

(b) Taiwan National Laws and Regulations on Export Controls

The Foreign Trade Act is the national law and Article 13 thereof creates the framework for the SHTC Regulations. The purpose of the law is to enhance national security and strengthen the development of high-tech industries in Taiwan through international cooperation and agreements, and export and import regulations.

(c) Control Lists

- The Export Control List for Dual-use Items and Technology
- Common Military List(Copies of the preceding control lists can be found at the website of the BOFT.[2])
- Sensitive Commodities List for North Korea
- Sensitive Commodities List for Iran[3]

- High-Tech Commodities List for Exportation to Russia and Belarus[4]

The control lists will further include commodities that are not contained in the aforementioned lists but their end uses or end users are suspected of developing or manufacturing nuclear, chemical, or biochemical weapons, missiles, or any other weapons of mass destruction. Additionally, for any commodity for which an International Import Certificate (IC), a Written Assurance Certificate (WA), a delivery verification (DV), or similar documents issued by Taiwan is required by the exporting country for the export of an item to Taiwan, such an item shall be automatically considered an SHTC upon arrival and will be regulated as such. All trade with North Korea has been banned since September 25, 2017, and as a result, the Sensitive Commodities List for North Korea is no longer used.

(d) Taiwan and UN Security Council Sanctions

Taiwan is not a member of the UN. Yet, the rationale underlying Taiwan's decision to ban trade with North Korea on September 25, 2017, is believed to have been based on the Security Council's Resolutions Nos. 2270, 2321, 2371, and 2375.

(e) Taiwan National Laws on Economic Sanctions

For national security reasons, the Foreign Trade Act authorizes the MOEA, by itself or in conjunction with another government agency, to submit a proposal to the Executive Yuan for its approval to ban or restrict trade with a particular country or territory, provided that such ban or restriction shall be submitted to the Legislative Yuan for its ratification within one month from the date of the publication of the order thereof. In addition, the MOEA may suspend import from or export to specific countries or territories, or import or export of specific goods, or take other necessary measures under one of the following circumstances: (1) when any natural disaster, incident, or war occurs; (2) when national security is endangered or protection of public safety is hindered; (3) when the domestic or international market suffers a serious shortage of a specific material or the price thereof drastically fluctuates; (4) when serious imbalance is caused or threatened in international payments; (5) when any international treaty, agreement, United Nations resolution, or international cooperation calls for it; or (6)

when a foreign country impedes import and/or export with measures violating international agreements or principles of fairness and reciprocity.

(f) Taiwan Sanctioned Parties Lists

The country lists currently include Iran, Iraq, North Korea, and China (the People's Republic of), Sudan, and Syria, each of which is called a "restricted region." A complete ban on trade with North Korea was imposed on September 25, 2017. China is considered a restricted region in connection with 12 categories of semiconductor wafer fabricating equipment for the purposes of exportation of SHTCs: that is, chemical-mechanical polishers, photo-resist strippers, photo-resist developers, rapid thermal processors, deposition apparatuses, cleaning equipment, dryers, electron microscopes, etchers, ion implanters, photo-resist coaters, and lithography equipment. For other SHTCs, China is subject to regulations applicable to a non-restricted region.

29.3 What Is Regulated: Scope of the Regulations

Full regulation enforcement of the export controls began in July of 1995, with all goods subject to the control lists of Coordinating Committee for Multilateral Export Controls (COCOM), the predecessor to the WA, requiring a license to export. In November of 1998, the control lists of Australia Group (AG), the Nuclear Supplier Group (NSG), and the Missile Technology Control Regime (MTCR) were incorporated. In July of 1999, the chemical substances listed by the Chemical Weapons Convention (CWC) was incorporated.

In January of 2004, a catchall control was implemented to enhance the check and audit of final use and/or final user of the goods to be exported. In June of 2006, as an effort to meet UN Security Council's trade sanctions against North Korea and Iran, the Sensitive Commodity List for North Korea and the Sensitive Commodity List for Iran were added to the control lists, aiming to control any export and re-export of sensitive commodities to those countries. In January of 2009, the Community Regime for the Control of Exports of Dual Use Items and Technology and Common Military List of the European Union were adopted, integrating all the control lists of WA, AG, NSG, and MTCR as well as the CWC. As of the time of this outline,

the most recently updated version in Taiwan tracking the Community Regime was published by the BOFT on December 13, 2019.

29.4 Who Is Regulated?

Any person that imports or exports goods is subject to the export controls regulations regardless of whether it is incorporated or not, whether it is of a profit-seeking nature or not, or whether it has been registered with the Bureau of Foreign Trade as an import and/or export business or not.

29.5 Classification

(a) Classification of Dual-Use Items

Taiwan's classification follows that of the European Union, which consists of ten categories listed here. The volume of the latest control lists of dual-use items in Taiwan was published on December 13, 2019, which may not have reflected the changes made by EU on October 17, 2019.

Category 0—Nuclear materials, facilities, and equipment
Category 1—Special materials and related equipment
Category 2—Materials processing
Category 3—Electronics
Category 4—Computers
Category 5—Telecommunications and "information security"
Category 6—Sensors and lasers
Category 7—Navigation and avionics
Category 8 Marine
Category 9—Aerospace and propulsion

(b) Classification of Military Items

Taiwan's classification follows that of the European Union, which consists of the 22 categories listed here.

ML1—Smooth-bore weapons with a caliber of less than 20 mm, other arms and automatic weapons with a caliber of 12.7 mm (caliber 0.50 inches) or less and accessories

ML2—Smooth-bore weapons with a caliber of 20 mm or more, other weapons or armament with a caliber greater than 12.7 mm (caliber 0.50 inches), projectors and accessories, as follows, and specially designed components therefor
ML3—Ammunition and fuse setting devices, as follows, and specially designed components therefor
ML4—Bombs, torpedoes, rockets, missiles, other explosive devices and charges and related equipment and accessories, as follows, and specially designed components therefor
ML5—Fire control, surveillance and warning equipment, and related systems, test and alignment and countermeasure equipment, as follows, specially designed for military use, and specially designed components and accessories therefor
ML6—Ground vehicles and components
ML7—Chemical agents, “biological agents,” “riot control agents,” radioactive materials, related equipment, components and materials
ML8—“Energetic materials” and related substances
ML9—Vessels of war (surface or underwater), special naval equipment, accessories, components and other surface vessels
ML10—“Aircraft,” “lighter-than-air vehicles,” “Unmanned Aerial Vehicles”
(UAVs), aero-engines and “aircraft” equipment, related equipment, and components, as follows, specially designed or modified for military use
ML11—Electronic equipment, “spacecraft” and components, not specified elsewhere on the Common Military List
ML12—High-velocity kinetic energy weapon systems and related equipment, as follows, and specially designed components therefor
ML13—Armored or protective equipment, constructions and components
ML14—Specialized equipment for military training or for simulating military scenarios, simulators specially designed for training in the use of any firearm or weapon specified by ML1 or ML2, and specially designed components and accessories therefor
ML15—Imaging or countermeasure equipment, specially designed for military use, and specially designed components and accessories therefor

ML16—Forgings, castings, and other unfinished products, specially designed for items specified by ML1 to ML4, ML6, ML9, ML10, ML12, or
ML19
ML17—Miscellaneous military equipment, materials and “libraries,” and specially designed components therefor
ML18—“Production” equipment and components
ML19—Directed energy weapon (DEW) systems, related or countermeasure equipment and test models, and specially designed components therefor
ML20—Cryogenic and “superconductive” equipment, as follows, and specially designed components and accessories therefor
ML21—“Software”
ML22—“Technology”

29.6 General Prohibitions/Restrictions/Requirements

Under Article 13 of the Foreign Trade Act,

- No export of SHTCs is allowed without authorization;
- Where international import certificate or a written assurance certificate is issued by the government of this country for the import of an item into this country, neither change of the importer nor transfer to any other country/region is allowed without authorization; and
- The intended use and the end user shall be truthfully declared at the time of import and no change shall be allowed without authorization.

Moreover, without prior authorization SHTCs in transit to a restricted region may not transit, transship via a commercial port of this country, nor can they be stored in bonded warehouses, logistics centers, and free trade ports/zones of this country.

29.7 Licensing/Reasons for Control

(a) Types of Export Control Licenses and Permits for Dual-Use Items

To export SHTCs, an exporter shall first apply for an SHTC export license with the BOFT.

(b) Export Control Licensing Procedure

An SHTC export license should be applied for electronically with the BOFT, and such application may take up to seven days for the BOFT to process in case of going to a nonrestricted region and up to 45 days in case of going to a restricted region.[5] This export license will have a validity of six months, under which there can be multiple shipments permitted. Under either of the following conditions, the period of validity may be granted by the BOFT for up to two years:

- Export to a country belonging to all four international export control regimes, that is, WA, MTCR, NSG, and AG.
- Export to a nonrestricted region to which the exporter has regularly exported SHTCs to the same country, or territory, and to the same importer for five or more times during the last six months.

(c) Import and Export Licenses for Military Items

To import or export military items, a separate approval is required from the Ministry of National Defense or the National Police Agency (an agency under the Ministry of Interior), depending on the purpose. To export military items, an SHTC export license or a regular export license is required to be applied for. The import and export of military items are restricted.

(d) Export Permits and Independent Expert Examination

For the purpose of determining whether a commodity constitutes an SHTC, the Identification and Audit Team of the Ministry of Economic Affairs was created. Currently, Industry and Technology Research Institute (ITRI) is retained by the BOFT as an expert for this purpose.[6] It is not legally required to consult the ITRI if an exporter possess the knowledge to determine if an item is an SHTC.

29.8 General Licenses/License Exceptions

(a) General Licenses

There are no general licenses, but if an exporter has implemented the Internal Compliance Program (an "ICP Exporter"), it may submit documents and apply for recognition by the BOFT. Detailed discussion of the Internal Compliance Program is beyond the scope of this outline, but, briefly put, it is an internal audit and control program implemented by an exporter so that there may be sufficient mechanisms or checkpoints in the process of exporting from this country, starting from a customer's inquiry, handling of purchase orders, and accounting procedures to making deliveries.[7] An ICP Exporter who wishes to export SHTCs may apply for an SHTC export license that is valid for multiple countries, buyers, consignees, and end users, and may be granted for a validity up to three years by the BOFT. An ICP Exporter should submit the previous year's internal review to the BOFT by March 31 each year.

In applying for an SHTC export license, an exporter shall submit the following documents:

- An application form for an export license for SHTC;
- An International Import Certificate, a Certificate of End Uses, or a Written Assurance Certificate issued by the government of the importing country, or a Written Assurance of End Uses provided by the foreign importer or end user, including the intended end uses and the identity of end users;
- Relevant transaction documents; and
- Other documents as may be required by the BOFT.

When an ICP Exporter applies for a three-year export license, if the foreign importer or end user is the same company as the ICP Exporter, or is the controlling company, or is the subsidiary company of the ICP Exporter, a Written Assurance of End Uses can be issued by the head office or controlling company, and the ICP exporter may not need to submit the aforesaid transaction documents.

(b) License Exceptions

If SHTCs are to be exported to the United States or Japan under either of the circumstances listed here, and the exporter has checked that the overseas trader is not in the international export control list and is not

named specifically by the competent authority for control purposes, the export licensing may be exempted under any of the following conditions:

- Where the total value (FOB) of the same commodity subject to export control is less than NTD300,000;
- Where an exporter has implemented an ICP, and has been recognized by the BOFT (see Section 29.8(a)).

29.9 Penalties, Enforcement, and Voluntary Disclosures

(a) Administrative Penalties

The following are violations in connection with import or export of SHTCs:

- Where such goods are transported to a nonrestricted region without authorization;
- Where, after an import certificate (or other similar documents) has been granted by this country, such goods are diverted to a nonrestricted region without authorization;
- Where, after being imported, the use or end user that was originally declared of such imported goods is changed without authorization and it is used not for the production or development of military weapons.

For these types of violations, the following penalties may be imposed:

- A fine from NT$60,000 to NT$3,000,000;
- Suspension of import/export trading in specific goods or import/export trading entirely from one month to one year; or
- Abolishing the liable party's exporter/importer registration.

(b) Criminal Penalties

Violation in connection with import or export of SHTCs:

- Where such goods are transported to a restricted region without authorization;
- Where, after an import certificate (or other similar documents) has been granted by this country, such goods are diverted to a restricted region without authorization;

- Where, after being imported, the use or end user that was originally declared of such imported goods is changed without authorization and it is used for the production or development of military weapons.

For these types of violations, the following penalties may be imposed: imprisonment of up to five years, detention, and/or a fine up to NT$3,000,000. It should be noted that if the representative of a juristic person, agent, employee, or any other staff member of a person (which can be a natural person and also an entity) commits the forgoing offense in their course of business, both the individual offender and the entity the offender works for will also be punishable by the prescribed fine.

(c) Enforcement

Administrative penalties are imposed by the BOFT and criminal penalties are imposed by the ordinary court. In addition to the ordinary court, there is the administrative court.

Pursuant to the Administrative Penalty Act, the timeframe for a government agency to impose an administrative penalty is three years, calculated from the date that the act in breach is completed, or, where the result of the act occurs at a later date, from such later date.

The right for the government to prosecute an offense such as the one discussed in Section 29.9(b) will be time barred if more than 20 years have elapsed.

(d) Voluntary Disclosures

Pursuant to the Criminal Code, if a person who turns himself in for an offense that is yet to be discovered, his punishment may be reduced. On the other hand, if the prosecution results in a conviction, in imposing a penalty, the court may consider various factors, including the attitude of the accused after the commission of the offense pending the imposition of the penalty. The “attitude” may be dependent on whether the accused has cooperated with the investigation and/or prosecution.

29.10 Recent Export Enforcement Matters

An administrative penalty is imposed by the BOFT; however, the BOFT does not release statistics in this regard. The administrative penalties imposed by the BOFT are infrequently challenged. According to the online database administered by the MOEA, in the last five years, we noted only one case where the decision of the BOFT imposing an administrative penalty (see Section 29.9(a)) was challenged and appealed to the Petitions and Appeals Committee of the MOEA.

As noted in Section 29.9(b), the criminal penalties are imposed by the court. According to an online database administered by the Judicial Yuan of this country, in the last ten years there have been only sporadic cases of violations that ended up in court: one case decided in 2012 by Tainan District Court, one in 2014 by Shih-lin Summary Court, and one in 2017 to Taichung District Court (subsequently appealed to Taiwan High Court Taichung Branch). In most of these cases, the court having considered the accused being first-time offenders, imposed penalties at the lower spectrum of the penalties. This list does not include potential cases, if any, that might be still pending in the judicial system, the decisions of which have yet to be rendered.

29.11 Special Topics

(a) Re-exports/Extraterritorial Application of Laws

If an item that has been imported into this country with an international import certificate (IC), a written assurance (WA) certificate, or a delivery verification (DV) issued by the government of this country for its import at the time of importation, such an item shall be automatically made an STHC and become subject to the SHTC Regulations. The importer of record cannot be changed, nor will any transfer to another country be allowed unless authorized. Any declared end use and end-user cannot be changed without authorization.

Once an STHC export license has been obtained to export an STHC to a given country, and the particular STHC has been exported to that country, Taiwan laws do not require the exporter to monitor said STHC subsequent to its export. It mainly relies on the documents submitted by the exporter at the time of applying for the export license, which, in addition to the SHTC export application form, must include a proper International Import

Certificate, a Certificate of End Uses, a Written Assurance Certificate issued by the government of the importing country, or a Written Assurance of End Uses provided by the foreign importer or the foreign end user.

(b) Intangible Transfer of Technical Information

If any technical information falls into any of the categories discussed in Section 29.2(c), its export shall be controlled as SHTCs, and no export shall be permitted unless an SHTC export license is applied for and issued. Taiwan does not control deemed exports, that is, the release of SHTC technology to non-Taiwanese persons in Taiwan.

(c) Practical Issues Related to Export Control Clearance

An exporter who is uncertain whether an item falls under controls lists is urged to make an application with the Identification and Audit Team of the BOFT for verification. Such an application should include the relevant product catalog, product brochure, technical documents and specifications. The application is free of charge and is submitted online. Currently, Industry and Technology Research Institute (the ITRI) is retained by the BOFT as an expert for this purpose. The process will normally take no longer than 12 days for the ITRI to issue a verification report. The application to ITRI is now online,[8] and in addition to a standard application form to be filled out, the exporter must provide product catalogs, pamphlets, and technical specifications. Normally, the review is based on submitted documents and no physical examinations are required.

An exporter should check if a foreign buyer is one listed in the international entity export controls list issued by this country (https://icp.trade.gov.tw/ICP/Display.action?pageName=OList) and whether a transaction exhibits any of the red-flagged irregularities. Red flags are any suspicious circumstances in a transaction that may take on any one of the following examples:

- Overseas traders who are named on the international export control list or those named specifically by the competent authority
- Overseas traders or agents who are not willing to provide the end uses or end users of the commodities, or traders that have virtually no business background

- Product functions and specifications that are not consistent with business requirements of overseas traders or technological standards of the importing countries
- Selling prices, trade terms, and conditions or payments that are not consistent with international trade norms
- Overseas traders who are not familiar with product functions but insist on buying them, or overseas traders who refuse routine installation, training, or follow-up maintenance services
- For no specific reasons the dates of transportation and destination are uncertain, the end-consignee for the forwarder or the consignee and place have been suddenly changed
- For no specific reasons, the packing methods, shipping routes or labels of commodities are suspicious

(d) Recordkeeping

All relevant records shall be kept for at least five years from the date of export. Relevant records include transactions records, accounting books and records, computer files, and databases.

(e) How to Be Compliant When Exporting to Taiwan and from Taiwan

Whether a company or individual is exporting to or from Taiwan, the issues of compliance are largely the same, although the SHTCs Regulations are export-oriented and less concerned with import. The following discussion is centered on exporting from Taiwan.

The import and export of goods are free to a large extent; however, a small percentage may still face restrictions and controls. Such restrictions and controls are imposed for a variety of considerations in respect of international treaties, trade agreements, national defense, public security and order, culture, hygiene, environmental and ecological protection, and/or other public policies. In Taiwan, nomenclatures of goods subject to restrictions and controls are compiled by the BOFT after consulting with relevant government agencies. As briefly noted in Section 29.1(a), the underlying reasons for the restrictions and controls go beyond the scope of this outline. For example, exportation of endangered species of wild fauna and flora, and products thereof, is not allowed without authorization, nor is

importation of the same allowed unless it is exported with an export permit issued by the government of the exporting country. Obviously, this restriction has nothing to do with the SHTC Regulations. Therefore, even if an item does not require a license based on the SHTC Regulations, it does not necessarily mean that there are not any other restrictions and controls that may require a license or that the item may be simply prohibited from import or export (i.e., no license will be granted).

The restrictions and controls other than those for the purposes of the SHTCs are more straightforward in their compliance, and whether an item is restricted or subject to controls can be queried by accessing the online portal of the CPT (Customs-Port-Trade) database. The CPT databases are administered by the National Customs Administration and consist not only of tariff codes and rates but also includes whether an item is subject to any restrictions and/or controls in both the import and the export trade. The online system is transparent and promptly kept up to date.[9] However, these resources currently are not available in English, and they do not purport to cover the SHTCs. To be compliant, an exporter would normally depend on the importer to properly utilize these resources appropriately, or use a third party that has the relevant knowledge. If there is difficulty to determine the tariff code of an item, under the Customs Act it is permissble to seek an advance ruling from Customs on the applicable tariff code.

Since the SHTC Regulations are export oriented, exporting from Taiwan would have the additional requirements of complying with the SHTC Regulations. In this connection, the discussions regarding the practical issues relating to export control clearance in Section 29.11(c) are highly relevant and should be referred to for the purpses of this section.

29.12 Encryption Controls

Encryption is controlled in the same way as other SHTCs for export purposes since certain encryption hardware, software, and technology are controlled as SHTCs. In general, there is no import or use control.

29.13 Blocking Laws/Penalties for Compliance with Sanction Imposed by Other Countries

Taiwan has no implementation of relevant legislation in this regard.

---

1. CHLY & Partners, Taipei, Taiwan.
2. In Taiwan, the first and the second lists are combined into one volume, “軍商兩用貨品及技術出口管制清單及一般軍用品清單” (https://ekm101.trade.gov.tw/ckfinder/connector?command=Proxy&lang=en&type=Files&currentFolder=%2F&hash=c245c263ce0eced480effe66bbede6b4d46c15ae&fileName=(%E4%BA%8C-1-1)%E8%BB%8D%E5%95%86%E5%85%A9%E7%94%A8%E8%B2%A8%E5%93%81%E5%8F%8A%E6%8A%80%E8%A1%93%E5%87%BA%E5%8F%A3%E7%AE%A1%E5%88%B6%E6%B8%85%E5%96%AE%E5%8F%8A%E4%B8%80%E8%88%AC%E8%BB%8D%E7%94%A8%E8%B2%A8%E5%93%81%E6%B8%85%E5%96%AE1081213(%E5%90%AB%E6%97%A5%E6%9C%9F).pdf).
3. In local language, “ ”(https://ekm101.trade.gov.tw/ckfinder/connector?command=Proxy&lang=en&type=Files&currentFolder=%2F&hash=c245c263ce0eced480effe66bbede6b4d46c15ae&fileName=(%E4%BA%8C)%E8%BC%B8%E5%BE%80%E4%BC%8A%E6%9C%97%E6%95%8F%E6%84%9F%E8%B2%A8%E5%93%81%E6%B8%85%E5%96%AE.pdf)
4. This control list was initially issued on April 6, 2022, and subsequently Belarus was added to the list on May 6 of the same year.
5. For the website to file SHTC export licenses, see https://cfgate.trade.gov.tw/boft_pw/PW/login.jsp.
6. For the website to determine whether a commodity constitutes an SHTC, see https://shtc.org.tw/WebPage/login.aspx
7. One may find additional information at the BOFT’s website regarding the ICP (https://www.trade.gov.tw/Pages/List.aspx?nodeID=1305).
8. https://shtc.itri.org.tw/WebPage/index.aspx.
9. The online data bases can be accessed at https://portal.sw.nat.gov.tw/PPL/index.

30

Export Controls in Thailand

Melisa Uremovic[1]

30.1 Overview

(a) What Is Regulated?

The main legislation relating to export controls and economic sanctions in Thailand is as follows:

- Customs Act B.E. 2560 (2017) (Customs Act)
- Export and Import of Goods Act B.E. 2522 (1979), as amended (Exim Act)

Other export requirements may be set out in specific legislation (e.g., the Hazardous Substances Act B.E. 2535 (1992), as amended (Hazardous Substances Act)).

(b) Where to Find the Regulations

All laws and regulations can be found on the Council of State's website at: http://www.krisdika.go.th/. However, the laws and regulations are provided in Thai, with only certain laws including an English translation.

In addition, all laws and regulations (which are required to be published in order to be enforceable) are published on the Royal Gazette's website at: https://ratchakitcha.soc.go.th/. Again, the laws and regulations are only available in Thai.

Subordinate legislation (which is not required to be published in the Royal Gazette and is not available on the Council of State's website or the Royal Gazette's website) may be found on the websites of relevant authorities. Most are only provided in Thai, with limited availability of English translations. For example:

- The Department of Foreign Trade (DFT) of the Ministry of Commerce (MOC) provides relevant laws and regulations in relation to foreign trade, including export controls, on its website at

http://www.dft.go.th/th-th/%E0%B8%81%E0%B8%8E%E0%B8%AB%E0%B8%A1%E0%B8%B2%E0%B8%A2, and certain English translations can be found at http://www.dft.go.th/en-us/Legal-Translation.

- The Royal Thai Customs ("Customs") provides relevant laws and regulations on its website at http://www.customs.go.th/list_strc_download_with_docno_date.php?ini_content=announce_160426_01&ini_menu=menu_Interest_and_law_160421_07&left_menu=menu_Interest_and_law_160421_07_160421_01&order_by=date&sort_type=0&lang=th&left_menu=menu_Interest_and_law_160421_07_160421_01.

(c) Who Is the Regulator?

Customs is the authority that generally regulates imports and exports in Thailand. The DFT of the MOC is the main authority that determines the goods subject to export restrictions and supervises the approval process, unless the goods otherwise fall under the supervision of other authorities in accordance with specific laws. Specific laws govern the export of specific products that require a license or a written permission from the relevant authorities.

(d) How to Get a License

In summary, any party exporting goods from Thailand is required to contact Customs in order to export the goods, subject to certain of the following conditions.

Currently, an exporter wishing to export restricted goods under the DFT's supervision must apply for approval online at http://edi2.dft.go.th/ or https://smart-1.dft.go.th/.

After the DFT receives a complete set of documents, the DFT will issue the export license within 30 minutes or within several hours, depending on the number of applications. In any case, the license will be issued within one day. The applicant must also obtain an exporter card from the DFT before exporting goods. The export card application can also be submitted online.

As mentioned earlier, certain goods are restricted or prohibited for export under other specific laws. There is no centralized export control

authority in Thailand, where the exporter can get a license for all exports of controlled goods. Further details of the licensing process are set out later in the chapter.

(e) Key Websites

Relevant information on export controls and economic sanctions is found at the Customs website (unfortunately, only a Thai version is available and may not be up-to-date): http://www.customs.go.th/cont_strc_simple.php?ini_content=business_160426_03_160930_01_160930_01&ini_menu=menu_goods_control_permit&lang=th&left_menu=menu_goods_control_permit.

Relevant information on export controls under the regulations of the DFT is available at http://www.dft.go.th/th-th/dft-service-data-import-export (again, only a Thai version is available and may not be up-to-date). An English summary of certain goods requiring an export license is available at http://www.dft.go.th/en-us/Information-Service/Measures-Related-to-Imports-and-Exports (and is not up-to-date).

30.2 Structure of the Laws and Regulations

As set out earlier, there are a number of laws in Thailand that deal with different aspects of export controls and economic sanctions. These laws broadly cover the requirements of export control, such as the licenses and permits required for export of goods from Thailand, and also the offenses and penalties for failing to comply with these requirements.

The laws are then further supported by the related subordinate laws, in the form of notifications and regulations. This subordinate law provides more detail and further explanation on the nature of the export controls and economic sanctions in Thailand.

30.3 What Is Regulated: Scope of the Regulations

Different aspects of export control and economic sanctions are covered by different laws and authorities, as follows:

- The Customs Act broadly establishes Customs as the regulator and sets out its powers as well as general procedures and restrictions regarding export;
- The Exim Act provides general powers to the MOC, through the DFT, to specify any goods as goods controlled for export, and also sets out the power to regulate the export licensing for such controlled goods; and
- Specific laws govern the export of specific products that require a license or a written permission from the relevant authorities.

30.4 Who Is Regulated

Any party who wishes to export goods from Thailand will be regulated under the applicable laws. It is the exporter (i.e., the party issuing the commercial invoice to the overseas customer) who will have to comply with the requirements of, among other things, obtaining the appropriate export permit for the export of goods from Thailand.

30.5 Classification

Before exporting goods from Thailand, exporters should be aware of the classification system, and should be able to classify their goods under the appropriate product codes. This ensures that the exporter is able to obtain any necessary export license, permit, or approval from any competent authorities.

Goods are classified in Thailand according to an eight-digit tariff nomenclature, as set out under the Customs Tariff Decree B.E. 2530 (1987), as amended. This classification system is adopted from the ASEAN Harmonized Tariff Nomenclature, which is also an eight-digit classification system used by all ten ASEAN member countries. This is, in turn, based on the Harmonized System (HS) developed by the World Customs Organization. The current HS system implemented by Thailand is HS2022.

In order to determine the appropriate HS codes for their products, exporters can refer to Customs' online database at http://itd.customs.go.th/igtf/viewerExport-Tariff.do?param=langEn, or simply consult with the Customs official on their hot-line: 1164.

Once the HS codes of the goods have been determined, the exporter may then use this to determine whether the goods are classified as controlled goods and therefore require the approval of the relevant competent authority before export.

30.6 General Prohibtions/Restrictions/Requirements

(a) General

As mentioned earlier, the main requirements for export are set out in the Customs Act and the Exim Act, under the authority of Customs and the DFT, respectively.

There are three main categories of export restrictions under the Exim Act:

- Goods that cannot be exported (for example, sand, counterfeit products, weapons (to certain countries));
- Goods for which the exporter must obtain prior approval (such as rice, coffee, gold, sugar, re-export products); and
- Goods that must be registered before export (such as canned pineapple, orchids, canned tuna, and unpolished diamonds).

Specific laws govern the export of specific products that require a license or a written permission from the relevant authorities, including but not limited to:

- Defence Industrial Department (Ministry of Defence), which controls weapons, military equipment, and chemical materials under the Act Controlling the Exportation of Arms, Armaments and War Implements B.E. 2495 (1952) (Weapon Export Control Act) and the Royal Decree Controlling the Exportation of Arms, Armaments, and War Implements B.E. 2535 (1992), as amended (Weapon Export Control Decree);
- Department of Industrial Works under the Ministry of Industry (MOI), which controls toxic chemicals under the Hazardous Substances Act;
- Department of Medical Sciences (Ministry of Public Health), which controls micro-organisms, pathogens, and animal toxins under the

Pathogens and Animal Toxins Act B.E. 2558 (2015); and

- Office of Atoms for Peace (Ministry of Higher Education, Science, Research and Innovation), which controls nuclear materials and other by-product materials (radioactive materials) under the Nuclear Energy for Peace Act B.E. 2559 (2016), as amended.

(b) Dual-Use Goods

In 2015, in order to implement the resolution of the UN Security Council No. 1540 (2004), Thailand issued a measure to control the export of dual-use goods, which includes transit, transshipment, and re-export. In October 2015, Thailand issued the Notification of the Ministry of Commerce specifying dual-use goods as goods requiring approval and specifying the goods that must comply with the export control measure B.E. 2558 (2015) (Notification on Dual-Use Goods). Under the Notification on Dual-Use Goods, dual-use goods means those goods that can be used for both commercial and military purposes. Two lists of goods are attached to the Notification on Dual-Use Goods: one requires an export permit (the list of which has adopted the EU List) and the other requires the exporter to comply with the export control measures, that is, self-registration with the DFT and confirmation with the DFT that the goods are not dual-use goods. However, the enforcement of the Notification on Dual-Use Goods has been postponed several times and was finally repealed in January 2020.

In April 2019, Thailand enacted the Trade Controls of Weapons of Mass Destruction Act B.E. 2562 (2019) (TCWMD Act) controlling goods involving the spread of weapons of mass destruction. The responsible authority under the TCWMD Act is the DFT. The TCWMD Act came into force on January 1, 2020.

Under the TCWMD Act, goods involving the spread of weapons of mass destruction (WMD) mean (1) weapons of mass destruction; (2) arms and armaments; and (3) dual-use goods. Dual-use goods mean goods that can be used for both commercial and military purposes, and can be used to design, develop, produce, utilize, modify, store, or transport weapons of mass destruction, or can be used in any manner in order to obtain weapons of mass destruction.

After several public hearings, the Notification of the Ministry of Commerce regarding measures for the purpose of control of goods related

to the proliferation of WMD and measures related to the goods with a reasonable doubt of the end use or the end user related to the proliferation of WMD, also known as the Catch-all Control notification (CAC Notification), was issued to set out the general rules regarding the measure imposed for the control of dual-use goods. The CAC Notification came into force on December 26, 2021.

Under the CAC Notification, the DFT aims to impose the control measure over dual-use goods only where information reported by government agencies reveals that such dual-use goods carry the relevant risks, which would in turn raise the risk of proliferation of WMD. This essentially aims to block any shipment of dual-use goods (or any goods which may be dual-use goods, and also include the transfer of technology and software) that will be delivered to a high-risk end-user.

The control measure under the CAC Notification prohibits the export, re-export, transshipment, transit, and transfer of technology and software of goods related to the proliferation of WMD and goods where there is reasonable doubt of the end use or the end user being related to the proliferation of WMD. This prohibition is a complete prohibition if there exists a risk of proliferation of WMD as specified in the CAC Notification.

(c) Trade Sanctions and Embargos

Thailand implements certain trade sanctions approved by the UN Security Council. Currently, Thailand has trade sanctions and embargos on exports of goods (such as weapons, military equipment, and so on) against the following countries:

- Central African Republic
- Democratic Republic of Congo
- Iran
- Libya
- North Korea
- Somalia
- Sudan
- The Republic of South Sudan
- Yemen

Exemptions may apply for certain countries. For example, military equipment for use in the United Nations Organization Stabilization Mission

in the Democratic Republic of the Congo was excluded from the arms embargo imposed on Congo by approval of the Committee of the Security Council established under the resolutions of the UN Security Council No. 1279 (1999) and 1291 (2000). Therefore, the relevant sanctions must be reviewed on a country-by-country basis.

Thailand also has trade sanctions and embargos on exports of goods (such as weapons, military equipment, and economic resources) against the following militant groups or organizations or individuals involved:

- Al-Qaeda and the Islamic State of Iraq and the Levant (the resolution of the UN Security Council No. 2253 [2015]); and
- The Taliban (the resolution of the UN Security Council No. 2255 [2015]).

30.7 Licensing/Reasons for Control

(a) Export Declaration

The normal procedure for export requires the submission of an Export Declaration, with most Export Declarations submitted electronically via the E-export system. Customs' website at http://www.customs.go.th provides some useful information in this regard.

Where the export products are "red line" (high risk shipments), such as those requiring an Export License, the cargo may be removed for physical inspection. In the case of green line, the procedure is quite simple, and once the content of the Export Declaration is verified and validated, export will be approved.

(b) Restricted Goods/Export Licenses

The DFT of the MOC is the main authority that determines the goods subject to export restrictions and supervises the approval process.

Regulations may be issued under the Exim Act to impose restrictions, for example, the recent notifications on embargos in accordance with resolutions of the UN Security Council or the Thai government's particular policies.

Currently, an exporter wishing to export restricted goods must apply for approval online at http://edi2.dft.go.th/ or https://smart-1.dft.go.th/. After the DFT receives a complete set of documents, the DFT will issue the export license within 30 minutes or a few hours, depending on the number of applications. In any case, the license will be issued within one day. The applicant must also obtain an exporter card from the DFT before exporting goods. The export card application can also be submitted online.

A list of restricted goods is available online (in Thai only) (http://www.dft.go.th/th-th/dft-service-data-import-export).

Certain types of controlled goods may be subject to additional regulatory requirements. Certain goods may require special export procedures and be considered "red line" (high risk shipments), such as "Type 3" hazardous substances under the Hazardous Substances Act, which must meet the following requirements:

- An exporter applies for an Export Permit from the Ministry of Industry (MOI);
- A Pre-Export Notification (PEN), attaching the Export Permit, may need to be submitted to the MOI;
- After receiving the PEN form, but prior to export, the exporter must complete a form called "WorAor./AorGor.6" to inform the MOI of various prescribed details; and
- The preceding documentation must be submitted with the Export Declaration, invoice, and any other relevant documents to Customs at the time of export.

30.8 General Licenses/License Exceptions

(a) Export Permit Exemptions

There are no general exemptions for export permits in respect of controlled goods provided under the Exim Act. As stated earlier, certain products may be subject to an export control measure under relevant specific laws, which provide an exemption thereunder. For example, under the Weapon Export Control Act and Weapon Export Control Decree, an export control measure does not apply in case of (1) personal belongings brought out by a person

for personal use as necessary or for repair; or (2) exporting as sample, and so on.

Under the Hazardous Substances Act, the relevant authority may issue an exemption from the export control measure for (1) a hazardous substance that, by its nature or quantity, may cause minor injury or against which the enforcement of various measures under this act will incur unreasonable burden; (2) a hazardous substance the purpose of which is to be used for the benefit of education, tests, analysis, research, and development; or (3) a hazardous substance of the ministries, bureaus, departments, local administrations, state enterprises, government agencies, Thai Red Cross Society, or other agencies, as appropriately designated.

30.9 Penalties, Enforcement, and Voluntary Disclosures

(a) Penalties for Failure to Comply with Export Requirements

Under the Exim Act, an exporter that does not comply with the prohibitions or prior approval requirements set out in the Exim Act could be subject to punishment of up to ten years' imprisonment and/or to a fine equivalent to five times the value of the exported goods. In addition, the goods (including containers and vehicles used in connection with the transport of the goods as well as vehicles used in the haulage of such goods) must be confiscated.

The Exim Act also allows for payment of a reward to the informer(s) and the officer(s) who assist in identifying offenders.

In the case of noncompliance with the requirement for prior registration, the offender is liable to imprisonment of not exceeding one year and/or to a fine not exceeding THB20,000.

Under the Customs Act, a duty evasion offense with regard to export could subject the exporter to punishment of up to ten years' imprisonment and/or to a fine equivalent to from one-half but not exceeding four times the duty additionally payable. We note that, if the matter proceeds to court and results in a conviction, the court does not have the ability to reduce the applicable fine.

As mentioned earlier, there are also various specific laws regulating export of specific goods, the penalties of which are provided under such respective laws.

(b) Voluntary Disclosure Program

From time to time, Customs opens a Voluntary Disclosure Program (VDP), in which operators can review their declaration and, if any incorrect declarations have been made, Customs would agree that such operator who joins the VDP pays only deficit duty (as well as value added tax (VAT) and VAT surcharge as applicable under the Revenue Code). In the case of VDP, all fines and import duty surcharges are waived.

However, the VDP is not supported by legal provisions, but is instead a practice that the Customs implements from time to time in order to build good cooperation between Customs and business operators, and to reduce the costs and time involved in Customs' officials in investigating alleged customs violations under the Customs Act.

Certain exclusions are imposed on participation in the VDP, and Customs has the power to consider whether an exporter or an importer is entitled to join the VDP. In practice, the VDP is offered based on the condition that no intention of duty evasion is involved. The VDP is not intended to serve as a blanket amnesty provision.

The VDP is provided by Customs, therefore, it does not provide a waiver of penalties arising from offenses under laws other than the Customs Act.

In addition, most of the offenses under the Customs Act relate to import, very few relate to export. Therefore, it is not usual to see the exporter joining the VDP.

30.10 Recent Export Enforcement Matters

In response to the outbreak of the coronavirus disease (Covid-19) in Thailand, the Central Committee on the Price of Goods and Services (MOC) issued several regulations regarding export control measures on surgical face masks. Under the regulations, surgical face masks include (1) medical masks and/or with a component of carbon and/or with a valve and N95 masks; (2) disposal masks for industry; and (3) disposal dust masks and/or with a component of carbon and/or with a valve, N95 masks to prevent dust, pollen, fog, smoke. These masks do not include reusable fabric masks.

As such, the export of surgical face masks is not permitted unless an approval is granted. This particular export control measure was enforced until late January 2024, unless any further relevant regulation was issued.

30.11 Special Topics

There are no special topics to be covered in relation to export controls and economic sanctions in Thailand.

1. R&T Asia (Thailand) Limited, part of Rajah & Tann Asia.

31

Export Controls and Economic Sanctions in the United Kingdom

Daniel Martin and Anthony Eskander[1]

31.1 Overview

(a) What Is Regulated?

The United Kingdom (UK) sanctions and export controls stem from both domestic and foreign policy, including international treaty commitments to the UN and, as at the time of writing, from its obligations as a former member of the European Union.

As a former EU member state, EU sanctions and export controls, as promulgated by EU Regulations, continued to have effect in the UK until the end of the Transition Period on December 31, 2020, as so-called acquired law.

The effects of Brexit are considered in more detail later in the chapter in Section 31.1(g), but the key point is that from January 1, 2021, UK national law (and not EU law) mandates export controls and economic sanctions in the UK, with the Sanctions and Anti-Money Laundering Act 2018 being the key piece of domestic legislation for UK sanctions.

The Sanctions and Anti-Money Laundering Act 2018 sets the framework for all individual sanctions programs, and on July 6, 2020, the UK introduced its first autonomous sanctions, targeting global human rights abuses.

The ambit of sanctions and embargoes depends on the ultimate objectives of the institution imposing the sanctions. For the UN, its fundamental objective is to maintain or restore international peace and security.[2] It achieves this by implementing decisions by its Security Council. The EU adopts measures in order to achieve the objectives of its Common Foreign and Security Policy, such as preventing violations of human rights.[3] The UK adopts financial sanctions to achieve a specific foreign policy or national security objective.[4] The targets of sanctions and embargoes are ordinarily countries, entities, and individuals who are acting contrary to such objectives.

The range of sanctions imposed by the UK includes financial sanctions (such as asset freezes), trade sanctions, arms embargoes, restrictions on the provision of certain services, travel bans, and diplomatic restrictions.

The UK's financial sanctions include targeted sanctions that not only freeze the assets of specified individuals and entities but also prohibit anyone who is subject to UK jurisdiction from making funds or economic resources available, directly or indirectly, to or for the benefit of a listed person. They also include prohibitions and restrictions on the provision of financial or insurance services in specified circumstances. Other economic sanctions include restrictions on trade in certain goods, targeted to have maximum impact on the particular sanctioned regime.

Export controls focus on the nature of the goods due to be exported, the ultimate end use of the goods, the location of the end user and any intermediate countries involved, in addition to whether there is any technical assistance, trafficking, and/or brokering of the controlled goods due to be transported between two countries. Neither the UK nor the EU have "deemed" export controls (where the release of goods to a non-UK or EU person, regardless of where the export takes place, is deemed to be an export).

There are controls on the brokering of military and dual-use goods. Brokering means buying or selling, or arranging or negotiating transactions for the purchase, sale, or supply, of dual-use items located in one country for transfer to another. In practice, brokering could include the following activities: (1) arranging supply from overseas factories/warehouses; (2) arranging intra-company transfers; (3) drop shipping; or (4) acting as a "project manager" for a project in one third country who sources supplies for that project in other third countries but it does not include ancillary

services (defined as transportation, financial services, insurance or re-insurance, or general advertising or promotion).

The UK regulates the following activities through export controls:

- Exports of goods listed on the UK Strategic Export Control Lists. This includes military goods, dual-use goods (listed in the EU Dual-Use Regulation), radioactive sources, goods used for torture and internal repression, and goods used for weapons of mass destruction (WMD);
- Goods covered by the Military End-Use Control and WMD End-Use Control;
- Technical assistance in connection with a WMD program; and
- Trafficking and brokering ("trade") in military and dual-use goods.

(b) Where to Find the Regulations?

UK legislation generally can be accessed at http://www.legislation.gov.uk/.

Regulations specific to the UK's financial sanctions regime can be accessed via this page on the Office of Financial Sanctions Implementation's (OFSI) website: https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation. The page lists all financial sanctions imposed in the UK by country, administration, or terrorist group.

(c) Who Is the Regulator?

The Department for International Trade (DIT)[5] implements and enforces trade sanctions and other trade restrictions (such as the import, export, and movement of goods and technology; the provision and supply of services; and the involvement of UK people in these activities).

HM Treasury (HMT)[6] implements and enforces financial sanctions. OFSI,[7] established in March 2016 as part of HMT, has a mandate to ensure that financial sanctions are properly understood, implemented, and enforced in the UK.

HMT is the UK's national competent authority for applications for licenses for exemption from financial sanctions, as well as notifications and requests for authorization under the EU rules on transfer of funds.

The Export Control Organization (ECO) is the UK's national competent authority in charge of regulating exports from the UK, including goods that are regulated under international sanctions. It assesses and issues export licenses, helps to shape worldwide arms control policies, and develops UK export licensing legislation.[8] It is part of the Department for Business, Energy and Industrial Strategy (BEIS) under its International Affairs, Trade Policy, and Export Controls directorate. BEIS is a ministerial department, meaning that it is ordinarily led by a government minister who is a Secretary of State and a member of the Cabinet.

(d) How to Get a License

The Export Control Joint Unit (ECJU), which is part of the DIT, manages the export licensing process.

The online SPIRE system can be used to obtain a specific export license or to find and register to use an Open General Export License (OGEL). It is accessible here: https://www.spire.trade.gov.uk/spire/fox/espire/LOGIN/login

(e) Key Websites

The ECJU website can be accessed at https://www.gov.uk/government/organisations/export-control-organisation. From this site you can access relevant pages on export licensing and details of controls on military and dual-use goods. It also contains information on how to apply for a specific export license and how to register to use an OGEL.

OFSI's website can be accessed at https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation. From this site you can access relevant pages on country-specific sanctions regimes maintained by the UK, the UK's consolidated list of financial sanctions targets (the "Consolidated List"), and details on enforcement of financial sanctions.

31.2 Structure of the Laws and Regulations

(a) International Treaties

The UK participates in a number of international treaties on export controls and its national regulations are based on such treaties. In particular, the UK participates in the following:

- The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1995)
- The Treaty on Non-Proliferation of Nuclear Weapons (NPT; 1968)
- The Convention on Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (1993)
- The Convention on Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (1972)
- The Nuclear Suppliers Group (NSG)
- The Zangger Committee (ZC)
- The Missile Technology Control Regime (MTCR)
- The United Kingdom–United States of America Agreement (UKUSA)
- The Australia Group

(b) The UK's National Laws and Regulations on Export Controls

For export controls, the key primary legislation in the UK is the Export Control Act 2002 ("the Act"). The Export Control Order 2008 ("the Order") is the main UK secondary legislation enacted under the Act.

The Order controls:

- The export of strategic goods (as listed in the UK Strategic Export Control Lists, discussed in more detail in Section 31.2(c));
- Transfer of technology;
- The provision of technical assistance;
- Trade of military equipment between overseas countries where any part of the activity takes place in the UK; and
- Trade controls with destinations where an arms embargo has been imposed by the UK.

Additionally, it provides licensing and enforcement powers to the ECO/BEIS in respect of sanctions and embargoes.

Up until June 21, 2021, the central piece of EU legislation was Council Regulation (EC) No. 428/2009 ("the Dual-Use Regulation"),[9] as amended. This has now been superseded by Council Regulation (EU) 821/2021 ("the Recast Dual-Use Regulation").

The Recast Dual-Use Regulation does not automatically apply in Great Britain; however, provisions within the EU Dual-Use Regulation were retained in Great Britain by the European Union (Withdrawal) Act 2018. It remains to be seen whether Great Britain will adopt provisions within the Recast Dual-Use Regulation and how the government will administer the revised rules for exports from Northern Ireland to other parts of the UK. As such, this chapter will focus on the EU Dual-Use Regulation.

The EU Dual-Use Regulation is a "Community," that is, EU-wide regime for the control of exports of dual-use items. Dual-use items are defined in Article 3 as items, including software and technology, that can be used for both civil and military purposes. The Order criminalizes noncompliance with the EU Dual-Use Regulation. The EU Dual-Use Regulation applied in UK until the end of the Transition Period on December 31, 2020, at which point it was incorporated into UK domestic law as EU retained law (for a full discussion, see the "Brexit" section, Section 31.11(g)).

The EU Dual-Use Regulation requires that all dual-use items listed in Annex I are subject to effective control when being exported outside of the Community or delivered to a third country, that is, any country outside of the EU, as a result of brokering services provided by a broker within the Community. It additionally imposes a requirement that all dual-use items listed in Annex IV are subject to control when being transferred between countries within the Community.[10] It states that the responsibility for deciding on export authorizations and authorization for brokering services lies with national authorities.

From January 1, 2021, UK exporters have to rely on the OGEL (export of dual-use items to EU member states) in order to export dual-use goods from the UK to EU member states or the Channel Islands.[11] Details on registering for an OGEL can be found later in the chapter in Section 31.7.

(c) Controlled Lists

The UK Strategic Export Control Lists[12] are lists of goods found within the following laws and regulations:

- UK Military List (Schedule 2 of the Order)[13]—military, security, and paramilitary goods, arms, ammunition, and related material;
- UK Dual-Use List (Schedule 3 of the Order)[14]—dual-use goods including explosives;
- European Union (EU) Human Rights List (Annexes II and III of 2005 EC Regulation 1236/2005)[15]—goods that could be used for torture, capital punishment, or cruel, inhuman, or degrading treatment or punishment to be sent to non-Community states;
- UK National Security and Paramilitary List (Article 9 of the Order)[16]—security and paramilitary goods;
- UK National Radioactive Sources List (Schedule referred to in Article 2 of Export of Radioactive Sources (Control) Order 2006)[17]—radioactive sources; and
- Annex I and Annex IV of the EU Dual-Use Regulation—dual-use goods.

If an entity intends to export goods listed within the UK Strategic Export Control Lists it requires a license from the ECO in order to do so.

On December 8, 2021, the Secretary of State for International Trade published a Trade Police Update.[18] Within the Update, the government confirmed a revised version of the licensing criteria for strategic export controls, to be known as the Strategic Export Licensing Criteria. The changes were made applicable from December 8, 2022, and were made applicable to all license decisions for export, transfer, trade, transit, and transshipment of goods, software, and technology subject to strategic controls; and to the provision of technical assistance or other services related to the aforementioned items.

(d) The UK and UN Security Council Sanctions

The UK implements all UN Security Council Sanctions. The Consolidated List,[19] published by HMT, is a list of all asset freeze targets designated by the UN and the UK pursuant to UK autonomous financial sanctions legislation.

Under an autonomous UK sanctions regime, where listings are made under a new UN Security Council resolution or sanctions committee, they will have effect in UK law via regulations made under the Sanctions and Anti-Money Laundering Act 2018.

(e) The UK's National Laws on Economic Sanctions

The UK's national laws on economic sanctions are contained in the following statutory instruments:

- Sanctions and Anti-Money Laundering Act 2018
- Counter Terrorism Act 2008
- Anti-Terrorism, Crime and Security Act 2001
- Terrorist Asset-Freezing etc. Act 2010

(f) The UK's Sanctioned Parties Lists

As indicated earlier, HMT publishes the Consolidated List,[20] and maintains a useful homepage for all of the various UK sanctions, UK legislation, and guidance.[21] The Consolidated List is also likely to include targets relating to retained EU law.[22]

OFSI maintains a separate list of entities subject to capital market restrictions. These entities are not contained on the Consolidated List and are listed pursuant to the Ukraine (Sovereignty and Territorial Integrity) Regime imposed under Council Regulation (EU) No. 833/2014.

The Home Secretary maintains a list of organizations proscribed under the Terrorism Act 2000. This list of proscribed organizations is not included in OFSI's Consolidated List.

31.3 What Is Regulated: Scope of the Regulations

Broadly speaking, UK export controls contained in the Order control the following:

- Export of "strategic goods," as listed on the UK Strategic Export Control Lists (as described earlier in Section 31.2(c));
- Transfer of technology;

- Provision of technical assistance, trade of military equipment between overseas countries where any part of the activity takes place in the UK; and
- Trade controls with destinations where an arms embargo has been imposed by the UK.

There are further export controls contained in country-specific sanctions regimes on the export of certain goods to certain countries or persons located within such countries.

The Act provides that the Secretary of State may by order make provision for or in connection with the imposition of:

- Export controls in relation to goods of any description;
- Transfer controls in relation to technology of any description;
- Technical assistance controls in relation to technical assistance of any description; and
- Trade controls in relation to goods of any description.

Export controls in relation to any goods means "the prohibition or regulation of their exportation from the UK or their shipment as stores."[23] Export controls may also be imposed in relation to the removal from the UK of vehicles, vessels, and aircraft (as an exportation of goods), whether or not they are moving under their own power or carrying goods or passengers.[24]

Transfer controls in relation to any technology, means the prohibition or regulation of its transfer:

- By a person or from a place within the UK or place outside the UK;
- By a person or from a place outside the UK to a person or place that is also outside the UK (but only where the transfer is by, or within the control of, a UK person);
- By a person or from a place within the UK to a person or a place that is also within the UK (but only where there is reason to believe that the technology may be used outside the UK); or
- By a person or from a place outside the UK to a person or place within the UK (but only where the transfer is by, or within the control of, a UK person and there is reason to believe that the technology may be used outside the UK).[25]

Technical assistance controls in relation to any technical assistance, means the prohibition or regulation of participation in the provision outside the UK of that technical assistance.[26] Technical assistance means services provided or used, or which are capable of being used, in connection with the development, production, or use of any goods or technology.[27] Participating in the provision of technical assistance outside the UK means (1) providing technical assistance outside the UK or agreeing to do so; or (2) making an arrangement under which another person provides technical assistance outside the UK or agrees to do so.

Trade controls in relation to any goods means the prohibition or regulation of:

- Their acquisition or disposal,
- Their movement; or
- Activities that facilitate or are otherwise connected with their acquisition, disposal, or movement.

Trade controls may be imposed on acts done outside the UK and the Isle of Man, but only if they are done by a person who is, or is acting under the control of, a "UK person" (see the following section, 31.4).[28]

31.4 Who Is Regulated?

All UK persons are regulated. The term "UK person" means any person within the territory and territorial sea of the UK and all UK nationals, wherever they are in the world. This means that:

- All individuals and legal entities who are within or undertake activities within the UK's territory must comply with UK financial sanctions that are in force.
- All UK nationals and legal entities (including entities or bodies incorporated or constituted under the law of the established UK law, and their branches) must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.[29]

The term "UK national" encompasses:

- British citizens, British Overseas Territories citizens, British National (Overseas) or a British Overseas citizens;

- Persons who under the British Nationality Act 1981 are British subjects; and
- British protected persons within the meaning of the British Nationality Act 1981.[30]

With regard to export controls, it is necessary to analyze the wording of each specific restriction in order to determine its reach. Provisions such as Article 19(2) of the Order (prohibiting the provision of technical assistance to WMD activities) apply to UK nationals even if they are operating outside the "customs territory," which after the end of the Transition Period means the UK. Similarly, Article 20 of the Order, which makes provision as to embargoed destinations, applies to persons carrying out activities in the UK and to UK nationals irrespective of where they are situated.

31.5 Classification

(a) Classification of Dual-Use Items

Dual-use items are classified in the UK Dual-Use List, contained in Schedule 3 to the Order (and formerly the EU Dual-Use list, contained in Annex I and Annex IV to Council Regulation (EC) No. 428/2000).

The UK Dual-Use List classifies dual-use goods as follows:

- Explosive-related goods and technology (PL8001);
- Materials, chemicals, micro-organisms and toxins (PL9002, PL9003, PL9004);
- Telecommunications and related technology (PL9005);
- Detection equipment (PL9006);
- Vessels and related software and technology (PL9008);
- Aircraft and related technology (PL9009);
- Firearms (PL9010, PL9011); and
- Submersible vessels and related goods, software and technology (PL9012).

The EU Dual-Use List, contained in Annex I to Council Regulation (EC) No. 428/2009, classifies dual-use goods as follows:

- Category 0—Nuclear materials, facilities and equipment;
- Category 1—Special materials and related equipment;

- Category 2—Materials processing;
- Category 3—Electronics;
- Category 4—Computers;
- Category 5—Telecommunications and “information security”;
- Category 6—Sensors and lasers;
- Category 7—Navigation and avionics;
- Category 8—Marine; and
- Category 9—Aerospace and propulsion.

(b) Classification of Military Items

Military items are classified in the UK Military List, contained in Schedule 2 to the Order. The categories of the UK Military List are as follows:

- ML 1—Smooth-bore weapons with a caliber of less than 20 mm, other firearms and automatic weapons with a caliber of 12.7 mm (caliber 0.50 inches) or less and accessories, as follows, and specially designed components therefor;
- ML2—Smooth-bore weapons with a caliber of 20 mm or more, other armament or weapons with a caliber greater than 12.7 mm (caliber 0.50 inches), projectors and accessories, as follows, and specially designed components therefor;
- ML3—Ammunition and fuse setting devices, as follows, and specially designed components therefor;
- ML4—Bombs, torpedoes, rockets, missiles, other explosive devices and charges, and related equipment and accessories, as follows, and specially designed components therefor;
- ML 5—Fire control equipment and related alerting and warning equipment, related systems, test and alignment and countermeasure equipment, as follows, specially designed for military use, and specially designed components and accessories therefor;
- ML6—Ground “vehicles” and components;
- ML 7—Chemical agents, “biological agents,” toxic chemicals and mixtures containing such agents or chemicals, “riot control agents,” radioactive materials, related equipment, components and materials;
- ML 8—“Energetic materials,” and related substances, as follows;
- ML 9—“Vessels” of war, special naval equipment, accessories, components, and other surface “vessels”;

- ML 10—“Aircraft,” “lighter-than-air vehicles,” “Unmanned Aerial Vehicles” (UAVs), aero-engines and “aircraft” equipment, related goods, and components as follows, specially designed or modified for military use;
- ML 11—Electronic equipment, “spacecraft” and components, not specified elsewhere in this Schedule;
- ML 12—High velocity kinetic energy weapon systems and related equipment, as follows, and specially designed components therefor;
- ML 13—Armored or protective goods and constructions;
- ML14—Specialized equipment for military training or for simulating military scenarios, simulators specially designed for training in the “use” of any firearm or weapon specified in ML1 or ML2,and specially designed components and accessories therefor;
- ML15—Imaging or countermeasure equipment, as follows, specially designed for military use, and specially designed components and accessories therefor;
- ML16—Forgings, castings, and other unfinished goods, specially designed for any of the “goods” specified in ML1 to ML4, ML6, ML9, ML10, ML12 or ML19;
- ML17—Miscellaneous goods, material and “libraries,” as follows, and specially designed components therefor;
- ML18—Production equipment and components;
- ML19—Directed energy weapon (DEW) systems, related or countermeasure equipment and test models, as follows, and specially designed components therefor;
- ML20—Cryogenic and “superconductive” equipment, as follows, and specially designed components and accessories therefor;
- ML21—“Software”;
- PL5001—Other security and paramilitary police goods; and
- ML22—“Technology.”

31.6 General Prohibitions/Restrictions/Requirements

Whether or not UK persons will require an export license to export goods will be determined by four factors:

- The nature of the goods to be exported;

- The destination;
- The ultimate end use of the goods; and
- The licensability of the trade activities.

An export license will be required to export controlled military goods, software and technology, and UK dual-use items from the UK to another country. These items are contained in the UK Strategic Export Control Lists.

A trade control license will be required for UK persons and persons located in the UK to engage in certain activities that involve the supply or delivery, the agreement to supply or deliver, or any activity that will promote the supply or delivery of, certain goods from one third country (non-EU country) to another.

The online checker tool,[31] maintained by the DIT, can be used to determine whether goods are controlled and if so which export license is required.

The general position in respect of imports to the UK is governed by the Import of Goods (Control) Order 1954. Article 1 of this Order prohibits the importation of all goods into the United Kingdom. Articles 2 and 5 of this Order permit the Secretary of State to grant import licenses subject to a wide discretion.

The Secretary of State, exercising the powers conferred by Articles 2 and 5, has granted an Open General Import License (OGIL), which permits imports of all goods into the UK unless such imports are expressly prohibited by exceptions to the OGIL set out in Annexes I and II, EU restrictions, or other domestic measures.

The OGIL prohibits the import of goods listed in Annex I of the OGIL that originate in certain restricted countries.

31.7 Licensing/Reasons for Control

(a) Types of Export Control Licenses and Permits for Dual-Use Items

There are a number of OGELs available in respect of dual-use goods. Details of the specific OGELs available in respect of dual-use goods can be found on the OGELs web page maintained by the ECJU.[32] From January 1,

2021, in order to export dual-use items to EU member states and the Channel Islands, UK exporters will need to rely on the OGEL (export of dual-use items to EU member states).[33]

OGELs are pre-published licenses that one needs to register for via the ECJU's export licensing database SPIRE;[34] more details on this process are set out in Section 31.7(b).

Holders of OGELs must meet all specified terms and conditions and are subject to compliance audits conducted by the ECJU. If an applicant cannot meet all the listed conditions they will need to apply for another license type, such as a Standard Individual Export License (SIEL) or an Open Individual Joint License (OIEL).

A SIEL can be applied for to send a single shipment of dual-use items to a specific named consignee and/or end user. An OIEL can be applied for to cover longterm contracts, projects, and repeat business. It should be used to replace at least 20 SIEL applications a year. A company applying for an OIEL will usually need to establish a track record of exporting before applying for an OIEL.

(b) Export Control Licensing Procedure

The ECJU has an online export licensing database called SPIRE,[35] all license applications and OGEL registrations should be made electronically via SPIRE.

When making an application, the following documentation should be attached:[36]

- Technical specifications of the product to be exported;
- Quantity or amount of each type of item being exported;
- Value of each item to be exported in GBP (even if only nominal);
- End user undertakings (if applicable e.g. for an SIEL); and
- Consignee undertakings (if applicable e.g. for an OIEL).

Minimal supporting documentation will be required for an OIEL, as a company in possession of an OIEL will receive regular compliance checks from the ECJU. Compliance checks and initial contact with exporters fall into the following categories:

- First time contact: to raise awareness of those new to export controls on their legal obligations and licensing requirements.

- First compliance check: the ECJU aims to conduct the first compliance visit within six months of first use of the license(s).
- Routine compliance checks: these occur for businesses that have had a first compliance check and continue to hold open licenses. The time between these routine checks depends on a risk assessment and whether the ECJU has been made aware of changes in circumstances that have arisen, such as a business takeover or change in key staff.
- Revisits: revisits arise when a company has been found noncompliant at a compliance check and, as a result, the ECJU aims to revisit within six to eight months.[37]

(c) Import and Export Licenses for Military Items

There are a number of OGELs available in respect of less-restricted controlled military goods. Details of these OGELs can be found online at page maintained by the ECJU.[38]

As with dual-use goods, to the extent an OGEL is not available, a SIEL can be applied for to send a single export shipment of military items to a specific named consignee and/or end user. An OIEL can be applied for to cover long-term contracts, projects, and repeat business.

There is an OGIL that permits imports of all goods into the UK unless such imports are expressly prohibited by exceptions to the OGIL set out in Annexes I and II, EU restrictions, or other domestic measures. The OGIL prohibits the import of goods listed in Annex I of the OGIL that originate in certain restricted countries. The import of certain military items originating from certain countries is prohibited by Annex I.

(d) Export Permits and Independent Expert Examination

The DIT provides online OGEL and Goods Checker Tools, which enable exporters to search for their goods and determine whether their goods are subject to export controls, and whether an OGEL applies based on the nature of the goods and their destination.[39]

Exporters may apply for an assessment of their goods against the UK Strategic Export Control Lists by the ECJU through the Control List Classification service. This process is provided through the SPIRE system. This assessment does not cover restrictions under sanctions regimes.

Similarly, the ECJU also provides an End-User Advice Service, also available through SPIRE. Use of the control list classification service does not absolve exporters from their legal obligations under the UK's export control legislation.

31.8 General Licenses/License Exceptions

(a) General Licenses

As discussed in Section 31.7(a) in respect of dual-use goods, OGEL are not specific to a company or individual. A person wishing to rely upon an OGEL must register on the SPIRE system to do so. Holders of OGELs must meet all specified terms and conditions and are subject to compliance audits conducted by the ECJU.

(b) License Exceptions

The Order contains a number of exceptions in respect of the export and transfer controls (as provided for in Articles 3, 4, and 5). Where an exception applies, no license is required for the subject activity. In broad terms, the exceptions apply (subject to further specific conditions) in respect of:

- The export immediately preceding import of aircraft on scheduled journeys;
- The export of vessels neither registered nor constructed within the UK, having been temporarily imported into the UK;
- The export of various specified types of firearms, where these comprise the personal effects of the holder of a European firearms pass or which were purchased or acquired pursuant to various certifications or permits;
- The transit or transshipment of goods, subject to various conditions. This exception does not apply in respect of certain specified goods and end destinations; and
- The transfer of software or technology in the public domain; for scientific research; or for installation, operation, maintenance, or repair of noncontrolled goods or software.

(c) Licenses Relating to Financial Sanctions

UK sanctions contain a number of licensing grounds to authorize activities that would otherwise breach UK financial sanctions. Depending on the specific program, licenses could be granted for the following purposes:

- To enable the basic needs of a designated person, or (in the case of an individual) any dependent family member of such a person, to be met;
- To enable the payment of reasonable professional fees for the provision of legal services;
- To enable, by the use of a designated person's frozen funds or economic resources, the satisfaction of an obligation of that person (whether arising under a contract, other agreement or otherwise), provided that (1) the obligation arose before the date on which the person became a designated person, and (2) no payments are made to another designated person, whether directly or indirectly; and/or
- To enable anything to be done to deal with an extraordinary situation.

Generally, exceptions apply in respect of asset freeze measures under UK sanctions that permit without license the crediting of frozen accounts with:

- Interest;
- Payments due under past contracts concluded prior to the date of the subject's designation;
- Payments due under judicial, administrative arbitral judgments rendered prior to the subject's designation; and
- Funds transferred by third parties.

Such credits must, however, also be frozen.

In the context of the financial sanctions against Russia, OFSI has issued a number of general licenses.[40] These include licenses for winding down business operations in Russia, and wind down of positions involving certain sanctioned Russian entities (including banks), humanitarian activity, and news media services.

31.9 Penalties, Enforcement, and Voluntary Disclosures

(a) Administrative Penalties

Since April 2017, OFSI and HMT have had the power to impose both civil and criminal penalties for breaches of financial sanctions.[41] These powers to impose civil financial penalties in respect of sanctions breaches are contained in the Policing and Crime Act 2017 from Section 146 onwards.[42] The penalties can be up to £1 million or, where the relevant offense involves a breach of the asset freeze, up to 50 percent of the value of the relevant funds or economic resources, whichever is the higher.[43]

The power to impose civil financial penalties is notable. The previous requirement was for OFSI to prove on the civil standard of proof, the "balance of probabilities" (as opposed to the stricter criminal standard of proof, "beyond reasonable doubt"), that there had been a breach of EU/UK sanctions and that the suspect knew or had "reasonable cause to suspect" that it was in breach. A change to section 146(1A) of the Policing and Crime Act 2017, as amended by the Economic Crime (Transparency and Enforcement) Act 2022, came into force on June 15, 2022. This change enables OFSI to impose civil financial penalties on a strict liability basis, thus removing the requirement to prove that a person had knowledge or reasonable cause to suspect that they were in breach of financial sanctions.

In its guidance, "OFSI Enforcement and Monetary Penalties for Breaches of Financial Sanctions," OFSI states that it will act proportionately when reviewing the actions of suspects and will assess factors such as the severity of the breach, the suspect's level of actual and expected knowledge of financial sanctions, considering the kind of work they do and their exposure to financial sanctions risk, as well as due diligence efforts to prevent such breaches, and whether a self-disclosure was made.[44]

(b) Criminal Penalties

Breaches of financial sanctions (any UK or EU sanctions regime that imposes asset freezes or other forms of financial and economic sanction) constitute criminal offenses. On conviction, such offenses are punishable by up to seven years in prison.[45]

In investigating a potential breach of financial sanctions, OFSI can refer a case to law enforcement agencies for criminal investigation and potential

prosecution.[46] OFSI will not usually impose a monetary (civil) penalty on a person who has already been prosecuted in respect of a criminal offense.[47]

Breaches of part 2 or 4 (relating to export/transfer controls and trade controls) of the Order constitute criminal offenses. On conviction, these offenses are punishable on summary conviction by a fine of up to £1,000. There are more stringent penalties in the event that the breach of part 2 or 3 (relating to export and transfer controls or technical assistance controls) of the Order is committed knowingly or with information, awareness, or grounds for suspecting that the goods, software, or technology are or may be intended in their entirety or in part for WMD purposes.[48]

In these circumstances, the offender may be arrested and shall be liable on summary conviction to a fine not exceeding the statutory maximum,[49] imprisonment for a term not exceeding 12 months (in the case of England and Wales and Scotland) or six months (in the case of Northern Ireland) or both. The same penalties apply to knowing breaches of restrictions[50] in the EU Dual-Use Regulation[51] and any breach of the WMD restrictions in the EU Dual-Use Regulation.

(c) Enforcement

OFSI reports that its approach can be summarized by the "compliance and enforcement model: promote, enable, respond and change" and it "promotes and enables compliance through engagement and guidance."[52]

Where there is suspected noncompliance, OFSI responds by "intervening to disrupt the attempted breaches and by addressing breaches effectively. It does this to change behaviour and to promote further compliance with financial sanctions."[53] Please see Section 31.10 for detail on recent instances of OFSI enforcement.

(d) Voluntary Disclosures

OFSI values voluntary disclosure, and its guidance on monetary penalties for breaches of financial sanctions, updated in April 2021,[54] includes a lengthy section on voluntary disclosure (paragraph 3.29 onwards). Cooperation is a sign of good faith and makes enforcing the law simpler, easier, quicker, and more effective. OFSI will make up to a 50 percent reduction in the final penalty amount for a prompt and complete voluntary

disclosure of a breach of financial sanctions in “serious” cases, or reductions of up to 30 percent for voluntary disclosure in the “most serious” cases.

There are several factors for an exporter to consider before voluntarily disclosing a compliance breach. The exporter should first conduct its own internal investigation, with the assistance of a lawyer, in order to determine what has happened and how to rectify it as quickly and effectively as possible. One benefit of involving a lawyer is that the details of the investigation may become legally privileged.

Should the exporter decide to voluntarily disclose the breach, it should be ready to address any questions raised by the ECO or HMRC quickly—it should have information available on the nature of the breach, the goods and destination in question, how the breach was discovered, and what steps have been taken to address it. The objective of this process is to minimize the possibility that further enforcement action is taken by the ECO or HMRC.

As set out earlier, once a voluntary disclosure has been made and the relevant authorities become involved, there are several possible outcomes, depending on the specific circumstances and nature of the breach. While the ECO may not take the matter further, it is, at a minimum, likely to record the matter and potentially increase the frequency of audits and the extent of those audits to which the exporter is subject in the future. The ECO, or even HMRC, may launch investigations into the breach, issue a warning letter, issue an HMRC fine (compound settlement), or even refer the matter to the Crown Prosecution Service for criminal prosecution (or to the Public Prosecution Service for Northern Ireland or the Crown Office and Procurator Fiscal Service in Scotland).

31.10 Recent Export Enforcement Matters

Since it obtained the power to issue fines in April 2017, OFSI has issued four penalties, with the amounts in question increasing significantly each time. While the last penalty which OFSI imposed on Standard Chartered amounted to £20.47 million, it remains the case that enforcement by OFSI has been limited, both in terms of the number of cases and the amounts of the penalties that have been imposed.

OFSI's first monetary penalty was issued in January 2019 in respect of Raphaels Bank. The penalty amounted to £5,000 (reduced from £10,000) and was imposed on Raphaels Bank for breaching the EU sanctions against Egypt. The bank had dealt in funds totalling £200 that belonged to a target of the asset freeze.[55] The initial penalty had amounted to £10,000 but it was reduced in line with OFSI's guidance on case assessment to reflect the Bank's disclosure and cooperation with OFSI's investigation.

In March 2019, OFSI announced its second monetary penalty, amounting to £10,000, had been imposed on Travelex UK. Travelex UK had, in breach of EU sanctions against Egypt, dealt with funds of the same asset freeze target that Raphaels Bank had also dealt with.[56] The value of the funds in question was £204, and OFSI determined that Travelex dealt with the funds despite having direct, in-person contact with the designated person and reference to the individual's passport.

In September 2019, OFSI announced that Telia Carrier UK Ltd. had been issued with a monetary penalty of £146,000 (reduced from £300,000) for facilitating phone calls to SyriaTel, a designated person under the EU Syria regime.[57] Notably, OFSI determined that this resulted in the company repeatedly making funds and economic resources indirectly available to the designated entity over an extended time-frame. Telia Carrier requested a ministerial review of the decision and used this as an opportunity to provide further information on the transactions in question. This led to OFSI significantly halving the assessed value of the breaches and reducing the penalty accordingly.

Most recently, in March 2020, OFSI's £20.47 million penalty on Standard Chartered was upheld. The penalty was reduced from £31.5 million and was imposed in respect of Standard Chartered's breach of EU financial sanctions on Sberbank and its former subsidiary Denizbank A.S.[58] Even the reduced fines still represent by far the highest penalty imposed by OFSI to date.

Standard Chartered reportedly made a series of 102 loans to Denizbank A.S. between 2015 and 2018. At the time the loans were made, Denizbank A.S. was majority owned by Sberbank. EU persons are, and were at the time of the loans, prohibited from making certain loans or credit available to Sberbank. The restrictions on Sberbank also applied to Denizbank, due to its majority ownership by Sberbank.

According to the OFSI report, Standard Chartered was aware of these restrictions, but believed that its loans fell within an exemption in the EU regime that permits loans or credit that finance the import/export of nonprohibited goods between the EU and any third country. In fact, 70 of the loans (with an estimated transaction value of over £266 million) lacked the necessary EU nexus, as the underlying trade did not involve the import or export of nonprohibited goods from the EU.

OFSI indicate that, on discovery of the mistake, Standard Chartered conducted an internal investigation and made a voluntary disclosure to OFSI. OFSI imposed penalties in respect of 21 loans, made between April 7, 2017, and January 26, 2018, with a combined value of £97.4 million.

As a result of Standard Chartered's voluntary disclosure, the penalty amount was initially reduced by 30 percent, from £45 million to £31.5 million, in line with OFSI's guidance on case assessment. Following ministerial review, the fines were further reduced to £20.5 million (around 45 percent of the maximum penalty).

This trend toward greater enforcement and higher penalty sums imposed by OFSI begins to mirror the U.S. approach, where settlements routinely reach multiple millions. We have also seen EU countries moving toward heavier fines for sanctions infringements, such as those imposed by the Dutch court in respect of Euroturbine (€600,000) and its Bahrain subsidiary (€ 4 million) for breaching EU and Dutch export controls on Iran.

In May 2022, OFSI imposed a penalty of £15,000 on Tracerco Limited[59] as a result of two payments (totalling less than £3,000) which Tracerco made to Syrian Arab Airlines for an employee to take flights home between May 2017 and August 2018.

The enforcement report link sets out a number of aggravating and mitigating factors, as follows: the fact that the payments were part of a pattern of breaches by Tracerco was an aggravating factor, but the breaches were of an indirect nature, were not deliberate, and were of a low value, which were mitigating factors, and the payments were voluntarily disclosed, so Tracerco received a 50 percent discount on the monetary penalty amount.

31.11 Special Topics

(a) Re-exports/Extraterritorial Application of Laws

UK export controls prohibit UK persons, wherever located, from moving goods subject to export controls from one country to another country without a license.[60] UK sanctions laws apply within the UK, and to UK persons wherever located.

(b) Intangible Transfer of Technical Information

Technical information (such as blueprints, diagrams, technical and training manuals) related to controlled goods requires an export license in order to be exported from the UK.

(c) Practical Issues Related to Export Control Clearance

Applications for export control licenses must be made through the SPIRE system.

The most recent data from the DIT (which relates to mid-2018) records[61] that 84 percent of license applications are processed within 20 working days, and 96 percent within 60 working days. The median time to process a license application was ten days.

(d) Recordkeeping

Any person acting under an export license must keep detailed records of:[62]

- The act;
- The goods, software or technology to which the act relates;
- Dates of the act;
- Quantity of goods;
- Name and address of the person acting;
- Name and address of the consignee/recipient;
- Name and address of the end user (so far as possible);
- Name and address of the supplier; and
- Any further information required by the license.

Such records must be kept for a minimum of four years where a general license is relied upon to authorize activity that would otherwise be prohibited under the Trade Controls part (Part 4) of the Order, and for three years in all other cases. The UK does not maintain a statute of limitation in

respect of criminal offenses and it may be advisable to retain records for a longer period in order to be able to demonstrate compliance.

(e) How to Be Compliant When Importing into the UK

In order to import non-EU goods into the UK, and EU goods from January 1, 2021, importers will generally need to:

- Complete customs declarations;
- Account for customs duty;
- Account for import Value Added Tax (VAT); and
- Submit safety and security declarations.

Additional requirements apply in respect other goods, such as those subject to international conventions, sanitary and phytosanitary controls, or other specific requirements.

Importers will also need to consider whether they need to appoint a fiscal representative, and whether direct or indirect representation is more appropriate.

(f) How to Be Compliant When Exporting from the UK

In order to export goods outside of the UK, exporters will generally need to:

- Determine the customs classification of their goods, and whether any restrictions apply. The UK government provides a useful "Goods Checker" online service;[63]
- Determine the tariffs that apply by reference to the commodity code of the export; and
- Register for a GB Economic Operators Registration and Identification number.

Additional restrictions apply in respect of certain classes of goods, including those subject to export controls. The process for obtaining clearance for goods subject to export controls is described in Section 31.7.

Many exporters rely on intermediaries, such as freight forwarders, to manage export compliance issues. However, export obligations are nondelegable.

(g) Brexit

The UK left the EU on January 31, 2020, commencing the Transition Period. During the Transition Period, EU law continued to apply in the UK, and the UK continued to be treated as if it were an EU member state. The Transition Period expired on December 31, 2020.

The UK made provision through the European Union (Withdrawal) Act 2018 for the majority of directly effective EU law, as it applies in the UK on expiry of the Transition Period to be retained in UK law ("retained EU law"). However, from the end of the Transition Period the UK will no longer be treated as part of (amongst other things) the Customs Union, and border controls for goods moving from the EU to the UK will be introduced on a phased basis. Equivalent controls will be applied by the EU, but as of the time of writing the details have not yet been published.

Brexit will have no impact on the overall framework of UK export controls in respect of military and dual-use goods. The EU Dual-Use Regulation will be retained in UK law, although there is scope for divergence between the EU and the UK as to the list's contents over time.

However, a license is needed to export dual-use items from the UK to the EU. The ECJU has already published an OGEL for exports of dual-use goods to the EU (exporters will need to register to use this OGEL as usual). UK issued licenses may no longer be relied upon to export dual-use items from the EU to a third country. Licenses are needed to export dual-use goods from the EU to the UK.

With the end of Transition Period on January 1, 2021, the UK has implemented its own autonomous sanctions regimes under the authority of the Sanctions and Anti-Money Laundering Act 2018. Individual sanctions regimes are provided for through secondary legislation.

The UK is assuming responsibility for making designation decisions (outside of UN sanctions regimes) and will have control over its own sanctions policy. The UK has already demonstrated its appetite to drive forward sanctions policy, implementing the Global Human Rights Sanctions Regulations 2020, which echoes the U.S.'s Global Magnitsky sanctions. The EU subsequently adopted its own Global Human Rights Sanctions Regime. UK persons are now subject to UK sanctions and not directly subject to EU sanctions. It is likely that there will be increasing divergence in sanctions policy, sanctions targets, and forms of sanctions between the UK and the EU over time.

It will also be interesting to see the extent to which the courts in the UK will take guidance published by the EU, as well as decisions of the European Court of Justice, into account when construing language in UK sanctions that is identical to language in EU sanctions that have been transposed unchanged into domestic law.

31.12 Encryption Controls

(a) General Comments

Cryptographic goods subject to EU export controls are listed in Category 5 Part 2 of Annex 1 of the EU Dual-Use Regulation. All goods listed in the Council Regulation (EC) 428/2009 are retained under the European Union (Withdrawal) Act 2018.[64] Authorization is required for the export of such goods from the UK and the EU Customs territory.

The list of controlled cryptographic goods is subject to the "Cryptography Note," which can be found at Note 3 to Category 5 Part 3 of Annex 1 of the EU Dual-Use Regulation. The Cryptography Note exempts from export control cryptographic products that meet various criteria. The Cryptography Note broadly exempts mass-market consumer-grade cryptographic products from export controls, reflecting the increasing ubiquity and sophistication of cryptographic software and equipment available to consumers.

The DIT has issued guidance on the Cryptography Note,[65] and confirms that the cryptographic goods (as well as components and software thereof) that meet the following high-level criteria may be exempted from export controls. In broad terms, the goods:

- Must be easily acquirable by the public;
- Must require little or no support to install; and
- Cannot have their cryptographic function modified by the consumer.

In determining the potential application of the Cryptography Note exemption, the DIT will consider the functionality and capability of the product as a standalone item, and a product may be controlled even where its individual components would not be controlled by themselves.[66]

The Cryptography Note will not exempt goods from export controls where those goods are listed elsewhere in the EU Dual-Use or UK Military Lists.[67]

(b) Import Encryption Clearance Requirements

Encryption and information security goods and technologies are not generally subject to import controls. They are not excepted from the scope of the OGIL, and their import is not otherwise prohibited or restricted.

However, the import of goods found on the EU Dual-Use List of Iranian and North Korean origin, including encryption goods, is prohibited.

(c) Encryption Licensing Requirements

Applications for export licenses are made to the ECJU as for other goods subject to export controls.

The UK has issued an OGEL in respect of certain information security items, including cryptographic technologies. This allows for the export of the specified items to countries other than those listed in the OGEL. In order to use the OGEL, exporters must register through the SPIRE system and state where they will keep records.

(d) Penalties for Violation of Encryption Regulations

Penalties for violation of the prohibition on unauthorized export of products subject to the EU Dual-Use Regulation, including in respect of cryptographic equipment, are reserved to EU member states. By virtue of the European Union (Withdrawal) Act 2018, breaches of the relevant provisions of the EU Dual-Use Regulation continue to be criminal offenses under UK law, and may result in a fine or imprisonment up to ten years.

31.13 Blocking Laws/Penalties for Compliance with Sanctions Imposed by Other Countries

EU Council Regulation 2271/96 (as amended) (the "EU Blocking Regulation") prohibits EU persons from complying with extraterritorial U.S. sanctions under the following U.S. legislation:[68]

- National Defense Authorization Act for Fiscal Year 1993, Title XVII Cuban Democracy Act 1992, sections 1704 and 1706
- Cuban Liberty and Democratic Solidarity Act of 1996
- Iran Sanctions Act of 1996
- Iran Freedom and Counter-Proliferation Act of 2012
- National Defense Authorization Act for Fiscal Year 2012
- Iran Threat Reduction and Syria Human Rights Act of 2012

The Commission may authorize otherwise prohibited activity.

The EU Blocking Regulation also:

- Prevents the recognition or enforcement of court judgments or administrative decisions giving effect to the specific extraterritorial legislation within the EU;
- Creates a right of action for those who have suffered loss as a result of the extraterritorial measures against the person or entity who caused the damage; and
- Imposes various reporting requirements on affected parties.

Individual member states are responsible for imposing penalties for breaches of the EU Blocking Regulation within their jurisdiction. The UK creates such penalties through the Extraterritorial US Legislation (Sanctions against Cuba, Iran and Libya) (Protection of Trading Interests) Order 1996 and the Extraterritorial US Legislation (Sanctions against Cuba, Iran and Libya) (Protection of Trading Interests) (Amendment) Order 2018. It is a criminal offense to breach Article 5 of the EU Blocking Regulation, which may be penalized with an unlimited fine.[69]

With the end of the Transition Period, the EU Blocking Regulation is retained EU law. Various consequential amendments have been made to the EU Blocking Regulation, its amending legislation and domestic legislation imposing penalties as described earlier, through the Protecting against the Effects of the Extraterritorial Application of Third Country Legislation (Amendment) (EU Exit) Regulations 2019.[70] These reflect the narrower jurisdictional scope of the EU Blocking Regulation as it operates in the UK (applying to the UK nationals and within UK jurisdiction) and substituting the relevant UK minister for the Commission as the authorizing authority and entity to whom disclosure should be made.

The UK government does not publish guidance in respect of the EU Blocking Regulation, but instead refers to and thereby endorses the EU

Commission Guidance.[71]

There is no binding judicial interpretation of the EU Blocking Regulation in English law. However in *Mamancochet Mining Limited v. Aegis Managing Agency Limited and Others*, Teare J gave obiter (i.e., nonbinding) consideration of the meaning of "comply . . . with any requirement or prohibition . . ." in Article 5 of the EU blocking Regulation. Teare J considered that the EU Blocking Regulation would not be engaged where an insurer's liability to pay was suspended under a sanctions clause. He drew a distinction between, on the one hand, complying with a third country's prohibition and, on the other hand, relying upon contractual wording (i.e., the exclusion clause in the policy). This treatment is only persuasive and will not necessarily be followed by other courts.

31.14 Sanctions on Russia

The Russia (Sanctions) (EU Exit) Regulations 2019 came into force on December 31, 2020 ("Russia Regulations"). They were adopted to ensure that sanctions relating to Russia continued to operate effectively after Brexit.

They have since, however, been expanded substantially to impose financial, trade, aircraft, shipping, and immigration sanctions for the purposes of encouraging Russia to cease actions that destabilize Ukraine or undermine or threaten the territorial integrity, sovereignty, or independence of Ukraine.

In order to achieve the stated purposes, the Russia Regulations impose a number of prohibitions and requirements. In order to enforce these, the Russia Regulations establish penalties and offenses, which are set out in detail in the report, "Report under Section 18 of the Sanctions and Anti-Money Laundering Act 2018, in Relation to Criminal Offenses."[72]

It is prohibited to intentionally participate in any activities if the object or effect of the activity is to directly or indirectly circumvent the prohibitions imposed by the Russia Regulations or to enable or facilitate the contravention of those prohibitions. The prohibitions and requirements imposed apply to all UK persons (see Section 31.4, Who Is Regulated?).

In terms of recent events:

- On March 4, 2022, OFSI published its updated Guidance for the Financial and Investment Restrictions in Russia (Sanctions) (EU Exit) Regulations 2019, which was updated on July 18, 2022.[73]
- On May 4, 2022, the UK Foreign Secretary announced an intended ban on UK services exports, including management consulting, accounting, and public relations, to Russia.[74]
- On June 8, 2022, the OFSI published amended enforcement and monetary penalties guidance for breaches of financial sanctions.[75]
- On June 23, 2022, The Russia (Sanctions) (EU Exit) (Amendment) (No. 10) Regulations 2022 came into force imposing a tranche of new trade sanctions on Russia.[76]

The key export controls and sanctions within the Russia Regulations are as follows:

(i) Asset Freezes

Persons designated by the Russia Regulations are subject to asset freezes. There are additionally restrictions on making funds and/or economic resources available to, or for the benefit of, designated persons, either directly or indirectly. That said, any designated person (or representative thereof) may apply for a license from OFSI, in order to enable the otherwise prohibited use of frozen funds.

(ii) Financial Services and Investments

- The Russia Regulations prohibit dealing, directly or indirectly, in certain categories of transferable securities and/or money market instruments, issued by:
  - The government of Russia (or on its behalf);
  - Designated entities, including Sberbank, Rosneft, and Gazprombank (or by an entity incorporated or constituted in a country other than the UK, which is owned directly or indirectly by one or more of those institutions); or
  - A legal person:
    (i) Incorporated and constituted under UK law; and
    (ii) Owned by a designated person; or
- A legal person acting on behalf, or at the direction, of preceding (i) or (ii).

- It is also prohibited for a person to deal, directly or indirectly, in certain categories of transferable securities and/or money market instruments, if issued by:
  - A person connected with Russia, that:
    - Is not a designated person; or
    - Is a person that, at 0:01 on March 1, 2022, is domiciled in a country other than Russia, or a branch or subsidiary of such a person wherever domiciled;
- An entity owned or acting on behalf, or at the direction, of any of the preceding.

A person is "connected with Russia" if that person is:

- An individual who is, or an association or combination of persons who are, ordinarily resident or located in Russia; or
- A legal person that is incorporated or constituted under the law of Russia, or domiciled in Russia.

"Government of Russia" is defined as any of:

- The presidency of Russia;
- Public bodies and agencies subordinate to the president of Russia, including the Administration of the President of the Russia;
- The chairman of the government of Russia (and deputies thereof);
- Any ministry of the Russian Federation;
- Any other public body or agency of the government of Russia, including the armed forces and law-enforcement organs of Russia; and
- The Central Bank of the Russian Federation.

(iii) Loan and Credit Arrangements

- It is prohibited to, directly or indirectly, enter into certain categories of arrangement issued by:
  - Designated entities, including Sberbank, VTB Bank, and Gazprombank; or
  - Entities incorporated or constituted under UK law and owned by a designated entity.

- It is prohibited for a person to, directly or indirectly, grant certain categories of loans or credit to:
  - A legal person connected with Russia;
  - The government of Russia; or
  - A legal person domiciled in a country other than Russia.

(iv) Correspondent Banking Relationships

- UK credit or financial institutions are prohibited from:
  - Establishing, or continuing with, correspondent banking relationships with:
    (i) Designated persons; or
    (ii) Credit or financial institutions owned or controlled, directly or indirectly, by a designated person.
- Processing (including clearing and settling) sterling payments to, from, or via either (i) or (ii), if it has reasonable cause to suspect that payment is to, from, or via a designated person.

(v) Foreign Exchange Reserve and Asset Management

- UK legal or natural persons are prohibited from providing financial services for the purpose of foreign exchange reserve and asset management to:
  - The Central Bank of the Russian Federation;
  - The National Wealth Fund of the Russian Federation;
  - The Ministry of Finance of the Russian Federation;
  - A legal person owned or controlled, directly or indirectly, by any of the preceding; or
  - A person acting on behalf, or at the direction of, directly or indirectly, any of the preceding.
- There are various exceptions, including where the loan is to make emergency funds available to meet applicable solvency or liquidity criteria for a certain subsidiaries.

(vi) Instruments in Relation to Crimea and Russia

- There are various prohibitions on making acquisitions of ownership interests in land or entities in or connected with Crimea or Russia.
- Subject to certain exceptions, there are prohibitions on:

- Granting any loan or credit to a relevant entity in Crimea, in addition to establishing a joint venture in Crimea or with a relevant entity; and
- Providing certain commercial arrangements in Russia, such as establishing new branches, offices, and subsidiaries, as well as joint ventures with persons connected with Russia; and
- Providing certain categories of investment services, directly or indirectly, to relevant entities.

(vii)Supply of Goods and Services

- There are restrictions on the export and import of a wide range of goods and services, including
  - The export of restricted goods and restricted technology to or for use in Russia (these are widely defined and include critical-industry goods, dual-use goods, military goods, aviation and space goods, oil refining goods, and maritime goods);
  - The export of goods for use in nongovernment controlled Ukrainian territory;
  - The export of energy-related goods to or for use in Russia;
  - The export of luxury goods to or for use in Russia;
  - The import of iron and steel products from Russia;
  - The export of jet fuel and fuel additives to or for use in Russia;
  - The import of a wide range of so-called revenue-generating goods from Russia;
  - The import of coal and coal products from Russia (from August 10, 2022);
  - The import of oil and oil products from Russia (from January 1, 2023); and
  - The direct or indirect provision of business and management consulting services to a person connected with Russia.

---

1. Daniel Martin, Partner & Global Head of Regulatory, HFW; Anthony Eskander, Independent Barrister, London.

2. Article 1 of the Charter of the United Nations (http://www.un.org/en/documents/charter/chapter1.shtml).

3. http://eeas.europa.eu/cfsp/index_en.htm.

4. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1100991/General_Guidance_-_UK_Financial_Sanctions__Aug_2022_.pdf.

5. https://www.gov.uk/government/organisations/department-for-international-trade.
6. https://www.gov.uk/government/organisations/hm-treasury.
7. https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation.
8. https://www.gov.uk/government/organisations/export-control-organisation/about#who-we-are.
9. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF.
10. Article 22(1) of the EU Dual-Use Regulation.
11. https://www.gov.uk/government/publications/open-general-export-licence-export-of-dual-use-items-to-eu-member-states.
12. https://www.gov.uk/guidance/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items.
13. http://www.legislation.gov.uk/uksi/2008/3231/schedule/2/made.
14. http://www.legislation.gov.uk/uksi/2008/3231/schedule/3/made.
15. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:200:0001:0019:EN:PDF.
16. http://www.legislation.gov.uk/uksi/2008/3231/article/9/made.
17. http://www.legislation.gov.uk/uksi/2006/1846/article/2/made.
18. https://questions-statements.parliament.uk/written-statements/detail/2021-12-08/hcws449.
19. https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets.
20. *Id.*
21. https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases.
22. As defined in section 6 of the European Union (Withdrawal) Act 2018.
23. Section 1 Export Control Act 2002.
24. *Id.*
25. Section 2 Export Control Act 2002.
26. Section 3 Export Control Act 2002.
27. *Id.*
28. Section 4 Export Control Act 2002.
29. Section 21 Sanctions and Anti-money Laundering Act 2018; *see also* OFSI Guidance: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961516/General_Guidance_-_UK_Financial_Sanctions.pdf.
30. Section 21 Sanctions and Anti-money Laundering Act 2018.
31. https://www.ecochecker.trade.gov.uk/spirefox5live/fox/spire/OGEL_GOODS_CHECKER_LANDING_PAGE/new.
32. https://www.gov.uk/government/collections/open-general-export-licences-ogels#military-goods-open-general-export-licences.
33. https://www.gov.uk/government/publications/open-general-export-licence-export-of-dual-use-items-to-eu-member-states.
34. https://www.spire.trade.gov.uk/spire/fox/espire/LOGIN/login.
35. *Id.*
36. https://www.gov.uk/government/publications/spire-online-export-licensing-guidance/using-spire-to-get-an-export-licence#applying-for-a-licence-trade-restrictions.
37. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1006254/United-Kingdom-Strategic-Export-Controls-Annual-Report-2021.pdf.
38. https://www.gov.uk/government/collections/open-general-export-licences-ogels#dual-use-open-general-export-licences.
39. https://www.ecochecker.trade.gov.uk/spirefox5live/fox/spire/OGEL_GOODS_CHECKER_LANDING_PAGE/new.

40. https://www.gov.uk/government/collections/ofsi-general-licences.
41. Policing and Crime Act 2017.
42. Section 146 onwards, Policing and Crime Act 2017.
43. Section 146(3) Policing and Crime Act 2017.
44. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1083297/15.06.22_OFSI_enforcement_guidance.pdf.
45. Sections 144 Policing and Crime Act 2017.
46. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1083299/15.06.22_OFSI_enforcement_guidance.pdf.
47. *Id.*
48. Section 34 Export Control Order 2008/3231.
49. Practically speaking, this may mean an unlimited fine, as the statutory cap of £5000 on the maximum fine that can be imposed on summary conviction has been removed for most common law and statutory criminal offences.
50. In particular, Articles 3(1), 4(1), 4(2), 5(1) or 22(1) of the EU Dual-Use Regulation.
51. Controls contained in Article 4(1) EU Dual-Use Regulation—as per section 35 Export Control Order 2008/3231.
52. https://www.gov.uk/government/collections/enforcement-of-financial-sanctions.
53. *Id*.
54. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1083299/15.06.22_OFSI_enforcement_guidance.pdf.
55. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781275/21.01.2019_Penalty_for_Breach_of_Financial_Sanctions.pdf.
56. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804021/Travelex_monetary_penalty.pdf.
57. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/842548/Telia_monetary_penalty.pdf.
58. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876971/200331_-_SCB_Penalty_Report.pdf.
59. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1086645/29.06.22_Tracerco_monetary_penaly_notice.pdf.
60. For instance, Article 35 Export Control Order Export Control Order 2008 (SI 2008/3231) and section 68 Customs and Excise Management Act 1979.
61. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/839284/strategic-export-controls-commentary-1-July---30-September-2018.pdf.
62. Article 29 Export Control Order 2008.
63. https://www.ecochecker.trade.gov.uk/spirefox5live/fox/spire/.
64. The caveat to this is that Council Regulation (EC) 428/2009 has direct effect in Northern Ireland.
65. https://www.gov.uk/government/publications/notice-to-exporters-201807-guidance-on-the-cryptography-note/notice-to-exporters-201807-guidance-on-the-cryptography-note.

66. *Id.*
67. *Id.*
68. Article 5 of the EU Blocking Regulation.
69. Section 2 of the Extraterritorial US Legislation (Sanctions against Cuba, Iran and Libya) (Protection of Trading Interests) Order 1996 (as amended).
70. See also DIT Guidance "Protection of Trading Interests (retained blocking regulation)": https://www.gov.uk/guidance/protection-of-trading-interests-retained-blocking-regulation.
71. http://www.legislation.gov.uk/uksi/2018/1357/pdfs/uksiem_20181357_en.pdf and https://www.gov.uk/government/publications/doing-business-with-iran/frequently-asked-questions-on-doing-business-with-iran#challenges-and-risks-of-doing-business-in-iran.
72. https://www.legislation.gov.uk/uksi/2022/241/pdfs/uksiod_20220241_en.pdf.
73. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092033/OFSI_Russia_guidance_July_2022.pdf.
74. https://www.gov.uk/government/news/russia-cut-off-from-uk-services.
75. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1083297/15.06.22_OFSI_enforcement_guidance.pdf.
76. https://www.legislation.gov.uk/uksi/2022/689/contents/made.