Westlaw Today
powered by Reuters

DHS agency proposes wide-sweeping cyber incident reporting requirements

By Phillip Seckman, Esq., and Stephen Robison, Esq., Dentons*

MAY 23, 2024

On April 4, 2024, the US Cybersecurity and Infrastructure Security Agency ("CISA") published a Notice of Proposed Rulemaking ("Proposed Rule")[1] associated with the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA").[2]

The proposed draft rule, coming in at 133 pages in the Federal Register, would establish two separate incident reporting requirements for companies that are a part of the US critical infrastructure.

While the proposed rule, if adopted, would impact entities in many different contexts, we focus here on the potential impacts to government contractors and subcontractors.

Key takeaways

- The proposed rule would expand reporting obligations broadly to entities that are part of the US critical infrastructure. Using a size and sector based evaluation the proposed rule would subject an estimated 316K entities to its reporting requirements.
- Under the proposed rule a "covered cyber incident" is reportable to CISA. What constitutes a "covered cyber incident" is likely to be hotly debated and difficult to discern, being determined by a case-by-case and fact specific impact analysis of the event, ancillary effects, disruption of business, and root cause.
- Generally, reporting to CISA would be required within 72-hours for a covered cyber incident (defined below) and 24-hours for any ransom payment to a threat actor.
- Four exceptions to this reporting requirement are proposed, the most relevant being when CISA maintains an information sharing agreement with an agency that also requires substantially the same timeline and similar reporting of a cyber incident.

The definition in the proposed rule that establish what "covered entities" would be impacted, the reporting obligations imposed on covered entities, what constitutes a "covered cyber incident," the reporting exceptions, and foundational compliance measures are discussed below.

In approaching these subjects, we focus on the implications for government contractors and subcontractors.

Proposed 'covered entity' criteria

While not all government contractors and subcontractors would fall within the proposed rule, it is likely that many may fit within the proposed rule's broad "covered entity" definition.

Specifically, the proposed rule defines a "covered entity" as an entity that is within a critical infrastructure sector and is either a large business concern or is a small business and fits within one of the sector-based criteria, for instance an entity that "[p]rovides operational critical support to the Department of Defense or processes, stores, or transmits covered defense information."

The proposed draft rule would establish two separate incident reporting requirements for companies that are a part of the US critical infrastructure.

An entity may be determined to be a "covered entity" under the rule "regardless of the specific critical infrastructure sector of which the entity considers itself to be a part."

Section 226.2(b) of the proposed rule lists the criteria specific to the associated sectors from Presidential Policy Directive 21.[3] A non-exhaustive list of the sectors from the policy and their associated sector-specific agency includes:

- Chemical: Department of Homeland Security
- Communications: Department of Homeland Security
- Defense Industrial Base: Department of Defense
- Energy: Department of Energy
- Finance: Department of Treasury
- Food and Agriculture: US Department of Agriculture and Department of Health and Human Services
- Healthcare and Public Health: Department of Health and Human Services
- Nuclear Reactors, Materials, and Waste: Department of Homeland Security

THOMSON REUTERS®

- Transportation: Department of Homeland Security and Department of Transportation
- Water and Wastewater and Waste: Environmental Protection Agency

Entities in these sectors need not be prime government contractors or subcontractors because the proposed rule broadly defines "covered entity," pulling a large number of entities within the scope of the rule and its requirements. Entities within these sectors should determine if they have any additional reporting requirements associated with their specific agency.

As most government contractors and subcontractors supporting DOD are already aware, DOD currently has an established notification requirement applicable to prime and subcontracts that incorporate DFARS 252.204-7012 ("DFARS Cyber Clause").[4]

This clause requires government DOD prime contractors and subcontractors with a covered contractor information system to submit notification within 72-hours to the Department of Defense Cyber Crime Center ("DC3") when they experience a cyber incident involving Controlled Unclassified Information ("CUI"), Covered Defense Information ("CDI"), Controlled Technical Information ("CTI"), and other sensitive information and data.

While the DFARS Cyber Clause requires notification concerning any controlled and/or sensitive data, this new proposed rule widens the landscape of reportable incidents. Under the DFARS Cyber Clause, a reportable incident is directly linked to the security and confidentiality of the covered information.

Under the new proposed rule, the existence of a covered cyber incident does not turn on facts showing specific types of data were compromised or impacts or actions against information systems that store such data. Instead, the proposed rule's reporting requirements are triggered merely by a covered entity experiencing a covered cyber incident to report within 72-hours.

Consequently, depending on the type, impact, and business disruption of an incident, an entity may have a reporting requirement to CISA but not DOD, vice-versa, or to both at the same time.

Covered cyber incidents and ransomware attacks

CISA noted that this proposed rule is in an attempt to "prevent, deter, defend against, respond to, and mitigate significant cyber incidents." Covered entities must report within: 72-hours of a covered cyber incident and 24-hours for any ransom payment.

The proposed rule defines a "covered cyber incident" as "any substantial cyber incident experienced by a covered entity." Further, an incident would qualify as a "substantial cyber incident" if it meets certain impact-based conditions.

There are four criteria, noted below, that CISA uses to define what qualifies as a "substantial cyber incident" resulting in a "covered cyber incident":

1. Substantial Loss of Confidentiality, Integrity, or Availability:
    - Determined by a multitude of factors including restriction to information, personal privacy, destruction or modification of data, and/or reliable access to use information.
2. Serious Impact on Safety and Resiliency of Operational Systems and Processes:
    - This criteria includes the safety or security hazards associated with the systems or process, and the scale and duration of the impact.
3. Disruption of Ability to Engage in Business or Industrial Operations:
    - Defined as a disruption of an entity's ability to operate and deliver goods or services.
4. Unauthorized Access Facilitated or Caused by — (a) Third-party or (b) Supply Chain Compromise:
    - The last criteria focuses on the cause of the incident. While it may not be distinguishable at the beginning of an incident, an entity will be required to submit a report where it has a "reasonable belief" that a covered incident occurred. Thus, even if it cannot be determined that a third-party caused the incident, the entity is likely required to submit a report as it likely falls within one of the other three prongs.

Importantly, the proposed rule does not require that each of the foregoing criteria be met. One criterion, on its own, could be sufficient. In order to identify the impact and breadth of an incident an analysis must be conducted. Additionally, once an entity "reasonably believes" a covered cyber incident has occurred they must conduct an analysis "as soon as reasonably practicable after becoming aware of the covered cyber incident."

This analysis should occur within hours, not days, of identifying a potential incident. Overall, this analysis should be conducted at the "subject matter expert level and not the executive officer level" to create an informative understanding of the event for efficient and effective reporting.

Reporting requirements

As discussed, covered entities would be obligated to report within: 72-hours of a covered cyber incident and 24-hours for any ransom payment. Moreover, in most cases, the expectations regarding this timing requires notification when there is a "reasonable belief" that a "covered cyber incident" has occurred and the appropriate analysis of the environment has been conducted by a subject matter expert.

In contrast, all ransom payments must be reported within 24-hours. Consequently, even if the cyber incident does not qualify as a substantial cyber incident using the above test, any ransom payment is considered a reportable incident, even if a third party makes the payment on behalf of the entity that has suffered the ransom incident.

Accordingly, a cyber incident, that is not a covered cyber incident, is one that "actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an

information system; or actually jeopardizes, without lawful authority, an information system."

As such, a cyber incident that also includes a ransom payment, which means the "transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack," is reportable as noted within 24-hours.

Generally, the information required in both reports (i.e., a covered cyber incident report or ransom payment report) requires information such as technical data of the incident, types of information potentially compromised, security and policies in place prior to the incident, scope of the incident, identification of law enforcement and other agencies that have been notified.

Additionally, any evidence of the root cause of the incident and other exploits utilized during the incident. Separately, a ransom payment report requires details associated with the payment, such as bitcoin wallets, identification of supposed recipient, and amount of payment.

Reporting exceptions

To avoid duplicative and burdensome reporting, the proposed rule allows for four exceptions. The first exception allows a single report to be provided when there is a "covered cyber incident" and ransom payment made related to the same event.

Additionally, this exception is only applicable if the ransom payment is made within the 72-hour reporting window for a covered cyber incident. As such, if an entity experiences a "covered cyber incident" and makes a ransom payment on the first day of the incident, the only report necessary would be the one detailing the ransom payment with the incident information included.

The second exception is conditioned upon CISA partnering and maintaining an information sharing agreement with the federal agency that the covered entity is already required to report when a cyber incident occurs. Additionally, the report to the other federal agency must be substantially similar regarding the information provided and the timeline of reporting.

Finally, the report must be able to be shared with CISA within the required timeframe according to the information sharing agreement. For instance, a covered entity may not have to report to CISA if they have a DOD cyber reporting requirement, the DOD agency has an information sharing agreement with CISA satisfying the 72-hour sharing of the report, and the reporting criteria/information are substantially the same.

The third and fourth exceptions are narrowly written applying to a limited number of covered entities. Specifically, the reporting requirement would not apply to Federal Agencies that are technically considered "covered entities" and entities that "develop, implement, and enforce policies concerning the Domain Name System."

Accordingly, understanding the contracts and reporting requirements an entity already has will be critically important to ensure compliance while also saving time, effort, and money.

Foundational compliance

Make sure your entity is ready to implement the appropriate policies, technical, and physical safeguards required for your industry, contractual obligations, and data stored. The below foundational compliance measures can facilitate a smooth transition to ensuring your company complies with applicable reporting requirements by implementing:

- Workforce training — Top down implementation.
- Contract analysis — Identify and prioritize all reporting requirements.
- Incident response — Plan, policies, and practice.

Notes:

[1] https://bit.ly/4aur15S

[2] https://bit.ly/3yE9ydV

[3] https://bit.ly/4bs1knY

[4] https://bit.ly/4dMVyyJ

About the authors

Dentons partner **Phillip Seckman** (L) aids clients with commercial item acquisitions, U.S. General Services Administration schedule contracting, cybersecurity, compliance, internal investigations and bid protests. He can be reached at phil.seckman@dentons.com. Firm associate **Stephan Robison** (R) focuses on cybersecurity, federal investigations, cost accounting standards and False Claims Act matters. He can be reached at stephen.robison@dentons.com. The authors are based in Denver. This article was originally published May 9, 2024, on the firm's website. Republished with permission.

This article was published on Westlaw Today on May 23, 2024.