INSIDE CYBERSECURITY
News. Analysis. Community.

DAILY NEWS

Former DHS attorney: Automated incident reporting may be infeasible under CISA regime for critical infrastructure

By **Sara Friedman** / April 6, 2022

Producing details for cyber incident reports to CISA will require input from business, technical and legal stakeholders on what should be included, according to Allison Bender, a former DHS attorney involved in establishing initial automated reporting requirements in 2015, who says CISA would be better served by asking for narrative information than just using structured data fields.

"The type of reporting that we're likely to see under the critical infrastructure reporting requirement will be very different from the automated indicator process. Things that are sensitive are typically not shared in an automated process. The trust building process with the federal government hasn't gotten there yet," Bender told *Inside Cybersecurity*.

She added, "The legal community is still improving their understanding of when cyber threat information sharing can be useful and is not harmful from a security perspective."

Bender chaired the Automated Indicator Sharing Privacy and Compliance Working Group during her time at DHS. Bender said the group's work turned into the "basis for a lot of policy positioning and language" that was included in the Cybersecurity and Information Sharing Act of 2015, which provides liability protections to companies that share information with DHS.

The **new cyber incident reporting law** for critical infrastructure builds on the 2015 info-sharing law by setting up a mandatory regime and establishing a requirement to report cyber incidents to the Cybersecurity and Infrastructure Security Agency within 72 hours, as well as a 24-hour requirement for reporting ransomware payments.

CISA has 24 months to craft a proposed rule that includes a definition of "covered entity," and definition and criteria for a "covered cyber incident."

Bender, a partner at law firm Dentons, said she is looking for the rule to provide "clarity" on the definitions as well as describing the "process." She said, "Business appreciates certainty, something you can plan around, update your incident response plan, and brief your board or senior leadership on how you do X, Y, and Z."

"The clearer CISA can make the reporting process, the threshold definitions and the methods of reporting, the more likely CISA will be successful," Bender said.

"With the critical infrastructure reporting requirement," Bender said, "I don't see that being automated for a long time, possibly ever. It will be similar to what we see with the [European Union's General Data Protection Rule] where there's a quick turnaround between discovery of a personal data breach and reporting to a supervisory data protection authority."

Bender said the information CISA is asking for is different from automated indicator sharing, which she described as "routine steady state noise from the internet. This will be much more focused, targeted, it will require more stakeholders to approve it before it goes out."

With the 72-hour deadline, Bender said it would be helpful for CISA to provide detail on what information they are going to accept, arguing that there could be "less information, less detail in the beginning in exchange for speed."

"It will also be the best-known information at the time and there's only so many hours you can investigate before hitting that trigger, so things may change afterwards. Allowing for more information to be filed later [and] corrective information to be filed later" should be considered when crafting the new regime, Bender said.

"Companies providing that information shouldn't be penalized for not knowing the answers right away for a potentially very complex incident which requires a lot of effort to respond to in addition to just reporting out," Bender said.

CISA is establishing ways to "structure reports or primarily put the data in structured fields that will allow them to automate their internal triage and review process," Bender said, while adding "I do think allowing a place for notes and narrative is helpful because you can provide more context that is likely to be useful. I think it also remains to be seen how many critical infrastructure incidents that meet the definition are likely to come in on a daily basis."

Bender said, "We don't know yet how many incidents are likely to come in. I don't think it is going to be a massive deluge but each one will need to be reviewed and prioritized for action. Part of that will be automation, part of it will be hiring additional personnel and also having very thoughtful and clear triggers internally such as what are the

intelligence requirements or tiering of critical infrastructure priority."

The law creates the intergovernmental **Cyber Incident Reporting Council** led by DHS which will be responsible for harmonizing incident reporting requirements across agencies. Bender pointed to the Securities and Exchange Commission's **proposed rule** for publicly traded companies and **Nuclear Regulatory Commission requirements** for nuclear power licensees as examples of federal regimes.

"The council will have to decide whether all critical infrastructure reporting can be harmonized to a single standard, does it make sense to except out certain critical infrastructure sectors, and what is uniquely different about this critical infrastructure sector versus that critical infrastructure that bears an additional reporting box under the CISA regime," Bender said.

For example, Bender said there could be a box specific to the energy sector "regarding impacts to SCADA and other industrial control systems."

She also pointed to a **new cyber incident reporting regime** for the U.S. banking sector, which went into effect on April 1, as a place where harmonization would be helpful.

According to the Office of the Comptroller of the Currency, "The final rule requires a banking organization to notify its primary federal regulator of any significant computer-security incident as soon as possible and no later than 36 hours after the banking organization determines that a cyber incident has occurred." -- *Sara Friedman (sfriedman@iwpnews.com)*