Articles + Publications | May 21, 2024

Locke Lord QuickStudy: CISA's Proposed Cyber Incident Reporting Rules Under CIRCIA

Locke Lord LLP

WRITTEN BY

Laura L. Ferguson | John K. Arnold | Kenneth K. Suh | Emma Bennett

RELATED OFFICES

Houston

On April 4, 2024, the United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") released for public comment its long-awaited proposed rules to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA").

The proposed rules impose reporting requirements for hundreds of thousands of covered entities that experience a substantial cyber incident (generally within 72 hours, but 24 hours for a ransom payment). Similar to current industry specific regulations, the proposed rules have specific deadline and substantive requirements. CIRCIA's broad reach creates the prospect of complicating an already segmented landscape of state, federal, and industry-specific reporting requirements. This Quick Study tries to uncomplicate that landscape by providing summaries of key elements of the proposed rules.

CIRCIA Encompasses 16 Industry Sectors—Amounting to Over 316,000 Covered Entities

CIRCIA does not internally define which entities are subject to the rules (a "Covered Entity"), instead requiring entities to cross-reference other federal standards and definitions, and, for those that qualify as small businesses under the Small Business Administration regulation, then review sixteen lengthy sector-based criteria to determine if they are still subject to the reporting rules.

A critical initial question is whether an entity is a small business under the Small Business Administration's existing regulations. Entities that exceed the small business threshold for their type of business are subject to different criteria than those that qualify as a small business.

The first way to be covered is to be an "entity in a critical infrastructure sector" that exceeds the applicable small business size standard.[1] A "critical infrastructure sector" pursuant to Presidential Policy Directive 21 includes 16 sectors including: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems. To determine if an entity is in one of these sectors, an entity must review the current version of the Sector-Specific Plans, which are on the CISA website.

The second way to be covered is to be a "small business"[2] in a critical infrastructure sector that meets one of the following sector-based criterion (see the regulation for detail on these):

1. Owns or operated a covered chemical facility;
2. Provides wire or radio communications service;
3. Owns or operate critical manufacturing sector infrastructure;
4. Provides operationally critical support to the Department of Defense or processes, stores, or transmits covered defense information;
5. Performs an emergency service or function;
6. Bulk electric and distribution system entities:
7. Owner or operates financial services sector infrastructure;
8. Qualifies as a State, local, Tribal, or territorial government entity;
9. Qualifies as an education facility;
10. Involved with information and communications technology to support elections processes;
11. Provides essential public health-related services;
12. Information technology entities;
13. Owns or operates a commercial nuclear power reactor or fuel cycle Facility;
14. Transportation system entities;
15. Subject to regulation of the Maritime Transportation Security Act; and
16. Owners or operates a qualifying community water system or publicly owned treatment works.

Importantly, CISA emphasized that CIRCIA is not limited to "entities that own or operate systems or assets that meet the statutory definition of 'critical infrastructure'" and the "overwhelming majority of entities will be within one of more sectors." CISA estimates that there will be approximately 316,244 covered entities. This expansive view appears to apply the reporting obligations not just to an entity that would be "critical" but also to vendors, contractors, and service providers or other entities in critical infrastructure sectors. As a welcome relief for some entities, CISA notes examples of entities that generally are not considered part of one or more critical infrastructure sector, such as advertising firms, law firms, political parties, graphic design firms, think tanks, and public interest groups.

Covered Cyber Incidents Fall into Four Categories—With Various Qualifiers

Covered cyber incidents, or "substantial cyber incidents," are defined as those incidents that lead to any of the following four impacts:

1. A substantial loss of confidentiality, integrity or availability of a Covered Entity's information system or network.

To determine whether a loss of the confidentiality, integrity or availability is "substantial", a Covered Entity needs to consider a variety of factors such as the type, volume, impact, and duration of the loss. Examples of this type of covered cyber incident include a denial-of-service attack, encryption of core business or information systems, any access to high-value information systems, and data theft when coupled with an actual or credible threat of data leak. By contrast, the preamble suggests if a public facing website was merely unavailable for a few minutes, it is unlikely to meet the standard of a "substantial cyber incident" under this type of incident.

2. A serious impact on the safety and resiliency of a Covered Entity's operational systems and processes.

To determine whether an impact on the safety and resiliency of an operation system or process is “serious”, a Covered Entity needs to consider a variety of factors, such as the safety or security hazards associated with the system or process, and the scale and duration of the impact. Examples of this type of covered cyber incident include cyber incidents that noticeably increase the potential for release of a hazardous material, compromising a bulk electric system, and disrupting emergency alert communications.

3. A disruption of a Covered Entity’s ability to engage in business or industrial operations, or deliver goods or services.

To determine whether a Covered Entity’s ability to engage in business or industrial operations, or deliver goods or services is “disrupted”, a Covered Entity needs to consider a variety of factors and circumstances, such as the scope of the disruption and what was disrupted. An example of this type of covered cyber incident is provided in the preamble to the proposed rules: “critical access hospital is unable to operate due to a ransomware attack on a third-party medical records software company on whom the critical access hospital relies; the critical access hospital, and perhaps the medical records software company as well if it also is a Covered Entity, would need to report the incident.”

4. Unauthorized access to a Covered Entity’s information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a:

a. Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or

b. Supply chain compromise.

Notably, this type of substantial cyber incident does not contain a qualifier, like “substantial” or “serious,” which reflects CISA’s position that any unauthorized access to a Covered Entity’s information system or network, or any nonpublic information contained therein, through a third party (such as a managed service provider) or a supply chain compromise is serious. Examples of this type of covered cyber incident provided in the preamble to the proposed rules include unauthorized intrusion into, or exfiltration of information out of, an information system due to a supply chain compromise and exploited cloud services vulnerabilities through a managed service provider.

Reporting Requirements—Lengthy Report Content Requirements and Short Turnaround Times

A Covered Entity is required to electronically submit a report to CISA, using the CIRCIA Incident Reporting Form, upon the occurrence of a covered cyber incident or ransom payment:

1. Covered Cyber Incident Report – within 72 hours of the reasonable belief that a covered cyber incident has occurred. The report will require a description of the incident, unauthorized access, vulnerabilities exploited, security measures in place, tactics and procedures used to perpetrate the incident, indicators of compromise, description of or samples of malicious software, identifying information about responsible actor for the incident, and description of mitigation actions.
2. Ransom Payment Report – within 24 hours of making a ransom payment. The report will require the date of the ransom payment, ransom payment amount and type of assets used, ransom demand (including the type and amount), ransom payment instructions; and outcomes of disbursing the ransom payment.

Unlike many similar existing regulations, CISA expressly acknowledges that a Covered Entity may not be able to provide all the aforementioned information by the required 24- and 72-hour deadlines and in such cases an entity could respond to some of the required requests as “unknown at this time” or “pending the results of additional investigation.”

The proposed rules also have a handful of exceptions to the reporting requirement, one of which is an important exception for entities subject to substantially similar reporting to another federal agency.[3] This exception applies for those entities who are legally required to report substantially similar information within a substantially similar timeframe to another federal agency, as long as there is a CIRCIA Agreement in place allowing information sharing between that federal agency and CISA. In such a case, if the Covered Entity timely reports to the other agency, such report will satisfy its obligations under these rules. CISA advises that it will work in good faith with other federal agencies to have CIRCIA Agreements finalized before the effective date of the final rules.

Enforcement Procedures—From Requests to Civil Actions

In addition to imposing reporting requirements, CIRCIA grants CISA the authority to issue a Request for Information (“RFI”) if there is a reason to believe a Covered Entity experienced a covered cyber incident, or made a ransom payment, but did not submit its required report. A Covered Entity has 72 hours to respond to an RFI before CISA may issue a subpoena. If a Covered Entity does not respond to CISA’s subpoena, CISA may refer the matter to the Attorney General to enforce the subpoena in District Court. Other penalties include acquisition penalties and suspension and debarment of the entity. Any person who knowingly submits false statements in a report, response to RFI, or subpoena may be subject to penalties under 18 U.S.C. § 1001. While it is historically the case that regulating agencies like CISA will be judicious in imposing enforcement consequences on Covered Entities that might not be familiar with these new requirements, it’s also the case that a significant breach of security requirements could result in CISA imposing serious enforcement consequences to serve as an example to Covered Entities.

Conclusion

The principal impact of this new regime appears to be potentially overlapping reporting requirements. While CISA states it is committed to harmonizing reporting requirements with other federal agencies, the proposed rules do not categorically address or reconcile such duplicative and overlapping reporting requirements. Covered Entities can thus expect to have overlapping reporting requirements at least until CISA releases its proposed CIRCIA Agreements. Still, CISA’s effort to harmonize reporting is not likely to come until after the final rules become effective in 2025.

CISA is accepting public comments until June 3, 2024. For more information on CISA’s proposed reporting rules, please contact the authors of this article.

—

[1] See 13 CFR part 121, which describes the small business size standard specified by the applicable North American Industry Classification System Code in the U.S. Small Business Administration’s Small Business Size Regulations.

[2] The Small Business Administration's regulations (under 13 CFR 121) has varying standards to determine if your business is a "small business" which vary by industry, number of employees, and revenue.

[3] Other exceptions include those entities that manage Domain Name Systems and federal agencies that are already required to report to CISA under the Federal Information Security Modernization Act of 2014.

RELATED INDUSTRIES + PRACTICES

- Energy
- Health Care + Life Sciences
- Privacy + Cyber