CISA Proposes Federal Cyber Incident Reporting Requirements for Businesses Across 16 Sectors

On April 4, 2024, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") published a proposed rule (the "Proposed Rule") in the *Federal Register*: The Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA") Reporting Requirements. The Proposed Rule outlines what will become the first broadly applicable federal cyber incident reporting requirements, and is the first significant regulatory step of CISA's implementation of CIRCIA since the law was enacted in March 2022.

Importantly, the reporting requirements will apply to entities across 16 "critical infrastructure" sectors, and will require "substantial" cyber incidents to be reported to CISA within 72 hours. Covered entities will also be required to report ransom payments to CISA within 24 hours. While CISA expects the final rule to be published in late 2025, companies—especially privately-held companies in sectors that lack current reporting requirements—should assess whether the Proposed Rule applies to them and start to prepare accordingly.

WHAT ENTITIES WILL BE COVERED?

The Proposed Rule requires a "covered entity" to comply with its reporting requirements. Generally speaking, a covered entity is an entity that (i) is within a critical infrastructure sector and (ii) meets either (a) size-based criteria or (b) sector-based criteria.

Starting with the first element, a "covered entity" is an entity within one or more of 16 critical infrastructure sectors enumerated in Presidential Policy Directive 21:

1. Chemical
2. Commercial Facilities
3. Communications
4. Critical Manufacturing
5. Dams
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Financial Services
10. Food and Agriculture
11. Government Facilities
12. Healthcare and Public Health
13. Information Technology
14. Nuclear Reactors, Materials and Waste
15. Transportation Systems
16. Water and Wastewater Systems

The Proposed Rule's release notes the breadth of these sectors: "The overwhelming majority of entities, though not all, are considered part of one or more critical infrastructure sectors."[1]

The second element requires an entity to meet either size- or sector-based criteria. First, an entity within the

critical infrastructure sectors qualifies as a "covered entity" if it exceeds the applicable U.S. Small Business Administration's (the "SBA") small business size standards, based on either number of employees or annual revenue.[2] As of 2022, 99.9% of businesses are "small businesses" under the SBA's standards. Second, and regardless of its size, an entity within the critical infrastructure sectors qualifies as a "covered entity" if it falls within certain sector-specific criteria for 13 of the 16 critical infrastructure sectors.[3] For instance, for the Financial Services Sector, CISA is proposing that covered entities would include entities: (i) that are required to report cybersecurity incidents to their respective primary federal regulator (*e.g.*, national banks, savings and loans holding companies and federally insured credit unions); (ii) as to which the primary federal regulator has indicated an intent to require cybersecurity incident reporting (*e.g.*, futures commission merchants and security-based swap data repositories); or (iii) that are encouraged or expected to report cybersecurity incidents to their primary federal regulator pursuant to an advisory bulletin (*e.g.*, Fannie Mae, Freddie Mac and money services businesses).

Notably, and as the release notes make clear, CISA's view is that "an entity may qualify as a covered entity under a sector-based criterion for a sector with which it does not typically identify." For example, "if a pharmaceutical manufacturer owns a covered chemical facility subject to [the Chemical Sector's sector-based criteria], it would qualify as a covered entity regardless of whether or not the pharmaceutical manufacturer considers itself part of the Chemical Sector."

WHAT WILL NEED TO BE REPORTED?

Substantial Cyber Incidents

The Proposed Rule requires a covered entity to report a "covered cyber incident", which CISA defines as a "substantial cyber incident" experienced by a covered entity.[4] A "substantial" cyber incident is one leading to any of four impacts: (i) "A substantial loss of confidentiality, integrity or availability of a covered entity's information system or network"; (ii) "A serious impact on the safety and resiliency of a covered entity's operational systems and processes"; (iii) "A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services"; or (iv) "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." The "substantial cyber incident" definition explicitly carves out lawfully authorized government activities, good faith events requested by an owner or operator of an information system[5] and the threat of disruption in order to extort a ransom (an imminent but not "actual" event). An incident must actually result in one or more of the four impacts to be a substantial cyber incident requiring reporting; unlike several other reporting schemes, it is not enough for the incident to place the entity at imminent risk of one of the impacts.

Ransom Payments

In addition to covered cyber incidents, the Proposed Rule requires covered entities to report ransom payments made in connection with a ransomware attack. As noted by CISA in the release notes, if a covered entity makes a ransom payment in response to an imminent (but not yet actual) disruption, "even if the disruption never materializes into a substantial cyber incident subject to covered cyber incident reporting. . . , the payment itself would still be subject to ransom payment reporting."

WHEN WILL REPORTS NEED TO BE FILED?

A covered entity is required to file a covered cyber incident report within 72 hours after the covered entity reasonably believes a covered cyber incident has occurred. CISA does not expect a "reasonable belief" will be reached "immediately" upon occurrence of an incident and acknowledges that a covered entity "may need to perform some preliminary analysis". However, CISA emphasizes "that in most cases, this preliminary analysis should be relatively short in duration (*i.e.*, hours, not days). . . and generally would occur at the subject matter expert level, and not the executive officer level".

A covered entity is also required to file a ransom payment report within 24 hours after a ransom payment has been made.[6]

All reports are currently contemplated to be web-based submissions.

WHAT ABOUT REPORTING TO OTHER FEDERAL AGENCIES?

The Proposed Rule does not provide for a general exception for entities that have other cyber incident reporting requirements.

The Proposed Rule provides for a process, however, whereby CISA can enter into information sharing agreements and report sharing mechanisms with other federal agencies if such agencies require "substantially similar" cyber incident reports under "substantially similar" time frames. Once CISA and a federal agency have entered into such an agreement and set up a sharing mechanism, covered entities that submit reports to the other agency may thereby satisfy the covered entity's CIRCIA incident reporting requirements. Until such information sharing agreements and mechanisms are in place, however, separate reports to CISA will be required.

WHAT OTHER KEY OBLIGATIONS ARE IN THE PROPOSED RULE?

Covered entities will be required to preserve data and records related to a covered cyber incident for at least two years from the date of the latest report in connection with an incident, with the preservation obligation beginning from the earlier of the initial ransom payment or the moment the entity arrives at a reasonable belief that a covered cyber incident occurred. The Proposed Rule sets out 10 categories of data and records requiring preservation.[7]

WHAT'S NEXT?

The Proposed Rule is open for public comment for 60 days (through June 3, 2024). In the Proposed Rule release, CISA estimates that the final rule will be published in late 2025 and will likely become effective in early 2026.

As CISA acknowledges, few companies will fall outside the 16 critical infrastructure sectors: "Illustrative examples of entities that generally are not considered part of one or more critical infrastructure sector[s] include advertising firms, law firms, political parties, graphic design firms, think tanks, and public interest groups."

Companies should therefore evaluate whether they fall within the size or industry-specific criteria and are thus within the proposed definition of a "covered entity" and, if so, monitor the rulemaking process for key developments as the rule nears finalization. Companies in scope should assess and update their policies, procedures and controls to ensure they are prepared to come into compliance when the rule goes into effect.

Companies in regulated industries, and public companies, will already have policies, procedures and controls in place to provide for incident reporting under existing regulatory regimes, such as procedures to assess the materiality of cybersecurity incidents that may trigger reporting on Item 1.05 of Form 8-K under recently adopted Securities and Exchange Commission rules.[8] However, those policies, procedures and controls will need to be assessed and modified to comply with CIRCIA's new requirements.

For those companies not subject to an existing cyber incident reporting regime, there will necessarily be more work required to comply with the reporting requirements, and planning for compliance should begin well in advance of finalization.

---

1 Covered entities are those that own and/or operate critical infrastructure, as well as entities understood to be part of one or more of the critical infrastructure sectors, as described in the Directive's Sector-Specific Plan ("SSP") for each such sector developed pursuant to the National Infrastructure Protection Plan. CISA recommends that entities review the SSPs for those sector(s) most closely aligning with their activities to determine whether they are part of such sector(s).

2 The SBA size standards are codified at 12 C.F.R. part 121. For industries in which small business status is determined by number of employees, the employee threshold ranges from 100 to 1,500 employees. For industries in which small business status is determined by revenue, the revenue threshold ranges from $2.25 to $47 million.

3 The Commercial Facilities, Dams and Food and Agriculture Sectors do not have proposed sector-based criteria.

4 CIRCIA defined a "covered cyber incident" as a "substantial cyber incident experienced by a covered entity that satisfies" the definition and criteria in CISA's final rule. *See* 6 U.S.C. § 681(3). CISA explains that it sought to define a "covered cyber incident" as including all "substantial cyber incidents", consistent with the definition in CIRCIA, and also "the least complicated approach". Under this approach, "a covered entity simply needs to determine if a cyber incident is a substantial cyber incident for it to be reported."

5 Good faith events would include, for example, "a properly authorized penetration test that inadvertently results in a cyber incident with actual impacts", or a cyber incident "result[ing] from security research testing conducted by security researchers who have been authorized . . . to attempt to compromise the system, such as in accordance with a vulnerability disclosure policy or bug bounty programs published by the owner or operator".

6 If a ransom payment is made within the 72-hour window for reporting a covered cyber incident, then the covered cyber incident report and the ransom report can be submitted jointly within the 72-hour window.

7 Communications with the threat actor; indicators of compromise; relevant log entries; relevant forensic artifacts; network data; data and information that may help identify how the information system was compromised; system information that may help identify exploited vulnerabilities; information about any exfiltrated data; data and records related to any ransom payment made; and any forensic or other reports about the cyber incident produced or procured by the covered entity.

8 *See* Cravath's August 1, 2023 client alert, "SEC Adopts Cybersecurity Disclosure Rules for Public Companies".

NEW YORK

David J. Kappos
+1-212-474-1168
dkappos@cravath.com

John D. Buretta
+1-212-474-1260
jburetta@cravath.com

Sasha Rosenthal-Larrea
+1-212-474-1957
srosenthal-larrea@cravath.com

Evan Norris
+1-212-474-1524
enorris@cravath.com

Michael L. Arnold
+1-212-474-1664
marnold@cravath.com

Dean M. Nickles
+1-212-474-1135
dnickles@cravath.com

WASHINGTON, D.C.

Jeffrey A. Rosen
+1-202-869-7724
jrosen@cravath.com

Cravath, Swaine & Moore LLP

NEW YORK

Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
+1-212-474-1000

LONDON

CityPoint
One Ropemaker Street
London EC2Y 9HR
+44-20-7453-1000

WASHINGTON, D.C.

1601 K Street NW
Washington, D.C. 20006-1682
+1-202-869-7700

cravath.com