8 Questions To Ask Before Final CISA Breach Reporting Rule

By **Arianna Evers and Shannon Mercer** (May 8, 2024)

Arianna Evers

Shannon Mercer

On April 4, the Cybersecurity and Infrastructure Security Agency published a notice of proposed rulemaking setting out mandatory reporting requirements for covered entities that experience cybersecurity incidents or make ransom payments in relation to a cybersecurity incident.[1] While the rule will inevitably change following the notice and comment period, the proposed rule represents the overall approach that CISA will take when it promulgates a final rule.

Complying with the new rule will take considerable preparation, and companies should begin planning for compliance now.

First, companies should understand whether the proposed rule would apply to them, and if it does, what will be required. Given the broad definition of "covered entity" under the proposed rule, companies in a variety of industries, such as those in financial services, healthcare, communications services, transportation, and education, to name a few, may fall under the rule's purview.

The proposed rule will further complicate data breach notice reporting requirements — which have been increasing in number — by mandating shorter reporting timelines and requiring more detailed information about breaches while such breaches may still be in progress or where remediation is continuing. Below we provide some background on the proposed rule, as well as key questions companies should be asking in order to prepare.

Background and Rule Overview

In March 2022, President Joe Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act.[2] CIRCIA established mandatory federal reporting requirements for cyber incidents across various sectors and critical industries and directed CISA to promulgate rules around these reporting requirements. The proposed rule establishes two key incident reporting requirements for covered entities: a 72-hour requirement to report "covered cyber incidents" and a 24-hour requirement to report "ransom payments" to CISA.[3]

Public comments and related material must be submitted by June 3, 2024. CISA expects its final rule to be published in late 2025, with a likely effective date in early 2026.

Key Questions Compliance Personnel Should Be Asking

1. Will my company be covered by the proposed rule?

Covered entities must report substantial cyber incidents and ransom payments under the proposed rule.

CIRCIA broadly defines "covered entities" to include the 16 critical infrastructure sectors[4] that were established under Presidential Policy Directive 21.[5] CISA's proposed rule

establishes two additional criteria for an entity to qualify as covered — size-based and sector-based criteria — either of which must be met for an entity to have mandatory reporting requirements.[6]

Notably, the reporting requirements apply to entire entities, not just subparts or constituents of entities performing critical functions. In some cases, these rules impose reporting requirements on entities in sectors that may not currently have had any incident reporting requirements under federal law. Companies should revisit whether they qualify as critical infrastructure entities under the rule.

2. How will this intersect with other federal cyber reporting obligations my company may already have?

In an effort to harmonize regulations and reduce duplicative reporting, the proposed rule provides an exception to CISA's reporting requirements if a covered entity is already required to report substantially similar information to another federal agency in a substantially similar time frame, and where CISA has an information sharing agreement — called a CIRCIA agreement — in place with that federal agency.[7]

CISA states that it will maintain a catalog of all CIRCIA agreements on a public-facing website so that the public will have notice of such agreements. It will be the covered entity's responsibility to confirm that a CIRCIA agreement exists and applies.

But until any such CIRCIA agreements are in place, there are some anticipated potential duplicative notice requirements.

For example, CISA explicitly acknowledges that financial services sector entities, such as national banks, that may otherwise have an obligation to report cybersecurity incidents to their primary federal regulators are also in scope for this CIRCIA reporting requirement. The NPRM explains that this is purposeful, citing the integral nature of these entities to economic security, their importance to the reliable operation of critical infrastructure, and the frequent targeting of such entities.

Despite the potential duplicative requirements, the proposed rule would cover such entities to help ensure that the government receives what it believes to be necessary cybersecurity-specific information on any given incident instead of relying on other regulators whose primary focus may not be cyberthreat identification and neutralization.

By way of further example, the issue of duplicative obligations may arise in the defense sector as well. Defense contractors are required to adhere to cyber incident reporting requirements under Defense Federal Acquisition Regulation Supplement 252.204-7012[8] and Title 32 of the Code of Federal Regulations, Sections 236.1-236.7.[9]

The DFARS 7012 clause and Section 236.2 impose requirements on contractors to report certain cyber incidents to the U.S. Department of Defense within 72 hours. Commenters have identified the DFARS 7012 clause as one of those existing reporting obligations considered to include substantially similar information.[10]

CISA states it is "committed to working with DOD to explore the applicability of the substantially similar reporting exception."[11]

Even if an information sharing agreement is finalized, companies should still closely review the definitions in both the original applicable reporting requirements and the new CISA

regulations. For example, there may be differences in the definition of defense industrial base entities in both the DFARS and the proposed rule.[12][13]

3. If my company is a public company, will I have to think about this reporting requirement and the SEC cybersecurity incident disclosure requirement?

The U.S. Securities and Exchange Commission cybersecurity incident disclosure requirement that took effect on Dec. 18, 2023, requires public companies that experience a "material" cybersecurity incident to file an 8-K within four business days of determining that the incident is material. The 8-K should include the "material aspects of the nature, scope, and timing of the incident," and the "material impact or reasonably likely material impact on the registrant, including on the registrant's financial condition and results of operations."[14]

The mere nature of a public disclosure, as compared to a private report, makes these two requirements fundamentally different.

Form 8-K filings are public documents prepared for the benefit of a company's investors, whereas the CISA reporting requirements will be confidential. CISA's reporting requirements are aimed at allowing the federal government to monitor and assist with cybersecurity incidents, whereas the SEC's requirements are intended to protect investors and increase transparency. These different forms and purposes may put the requirements at odds for harmonization.

That does not mean, however, that all in-scope material cybersecurity incidents will be reported to CISA within 72 hours on a private basis and publicly announced on an 8-K only one day later to the public.

On Dec. 12, 2023, the U.S. Department of Justice announced guidance on seeking delays of cyber incident disclosures as required by the SEC.[15] This guidance was promulgated ahead of the Dec. 18 implementation date of the SEC's final rules.[16] Under the guidance, the registrant may request within that four-day time frame that the attorney general determine that disclosure would pose a "substantial risk to national security or public safety" to receive a delay.[17]

4. What will I need to report to CISA?

Covered entities will need to report substantial cyber incidents and ransom payments made in connection with ransomware attacks. A substantial cyber incident is defined as an incident that causes a substantial loss of confidentiality, affects a company's operational safety, disrupts a company's ability to conduct its business, or compromises a company's cloud services or supply chain.[18]

As discussed above, exceptions to reporting exist for substantially similar incidents reported to other federal agencies pursuant to CIRCIA agreements.

Covered entities that experience a significant cyber incident or ransomware attack will need to provide detailed information regarding the incident, including, for example, when the incident occurred, how the company became aware of the incident, a description of the company's security measures in place, the amount of any paid ransom, and any identifying information regarding the actor reasonably believed to be responsible for the incident, among other information.[19] This information will need to be submitted using a web-based CIRCIA incident reporting form.[20]

After an initial incident report has been filed, covered entities have an ongoing obligation to promptly submit supplemental reports as additional information becomes available or if a ransom payment is made.[21]

5. Will CISA keep my company's information confidential?

Reports submitted to CISA will be provided with various legal protections.

CISA will keep all information submitted confidential. The agency will delete all personal information it deems is not directly related to a cybersecurity threat, and it will anonymize all personal information in the instance such information is shared outside the federal government. Information contained in reports will also be exempt from disclosure under the Freedom of Information Act.

Additionally, CISA indicates that a cause of action cannot stand if it is predicated solely on the submission of a report under this requirement. Likewise, a regulator may not use information obtained solely through a CIRCIA report in an enforcement action or to otherwise regulate the relevant entity.

Under the proposed rule, the information provided in these reports may not be subject to discovery, received in evidence, or otherwise used in a legal proceeding. Furthermore, under the proposed rule, a covered entity would not waive any applicable privilege or protection provided by law, including trade secret protections, as a consequence of submitting a report to CISA.

6. What happens if a company does not comply?

In cases of noncompliance, the proposed rule would authorize the CISA director to issue a request for information to a covered entity if there is "reason to believe that the entity experienced a covered cyber incident or made a ransom payment but failed to report the incident or payment."[22]

A request for information is not appealable, and if an entity fails to reply, the director may issue a subpoena to compel disclosure.[23] Like other regulatory subpoenas, noncompliance could result in civil contempt proceedings. Noncompliance could also be referred to the U.S. Department of Homeland Security Suspension and Debarment Program and to cognizant contracting officials or the attorney general for civil or criminal enforcement.[24]

7. What will this new rule mean for my incident response plan?

Companies that believe they may be covered by the proposed rule should start thinking through how to build these new reporting requirements and deadlines, including supplemental reporting requirements, into their incident response plans or applicable procedures.

Depending on a company's existing incident response plan and incident response teams, this may mean setting up a new or separate escalation path or indicating that specific individuals in the legal department or management require more information about an incident at earlier stages. If dealing with duplicative reporting requirements, finding synergies in those escalation, evaluation or decision-making processes could be advantageous.

Companies should make sure the relevant internal stakeholders, including executives,

cybersecurity and incident response teams, and communications teams, are aware of disclosure timelines. In-house legal counsel and incident response teams should also familiarize themselves with the details required for initial and supplemental reporting. Reporting requirements should be built into incident response training and testing, such as tabletop exercises.

8. Will I need to keep records to comply with the proposed rule?

Yes. The rule requires companies to retain covered data and records for two years.[25] Preparing to comply with the two-year data retention mandate may require additional coordination with legal and information technology teams.

Conclusion

The rules proposed by CISA are complex and likely have broad applicability. Legal and cybersecurity leaders in critical infrastructure sectors should familiarize themselves with this proposed rule to determine its applicability, and should begin considering how these new reporting obligations fit into existing incident response procedures.

Companies that have not previously considered themselves a part of critical infrastructure should revisit whether they qualify as a covered entity under the proposed rule. Companies should not wait until the requirements take effect or a cyber incident occurs to consider how they will comply with the proposed rule.

Arianna Evers is special counsel and Shannon Togawa Mercer is counsel at WilmerHale.

WilmerHale associates Meredith P. Yates and Shervin Z. Taheran contributed to this article.

[1] https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements.

[2] https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

[3] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=126.

[4] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

[5] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[6] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=124.

[7] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=126.

[8] https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-

252.2/section-252.204-7012.

[9] https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-M/part-236?toc=1.

[10] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=16.

[11] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=45.

[12] The Defense Industrial Base Sector-Specific Plan ("DIB SSP"), created by the DoD as a federal-government wide initiative to assess the risk management of critical infrastructure, identified the DIB sector as "government and private sector organizations that can support military operations directly" and perform certain activities "intended to satisfy U.S. military national defense requirements.'' The proposed rule would include in this sector any DFARS 7012 contractor or subcontractor and also those contractors and subcontractors who provide "operationally critical support" to DoD or process, store, or transmit covered defense information. The description of those who provide "operationally critical support" would include entities in one or more critical infrastructure sectors who are not generally considered part of the DIB as described in the DIB SSP.

[13] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=44.

[14] https://www.sec.gov/corpfin/secg-cybersecurity.

[15] Department of Justice Material Cybersecurity Incident Delay Determinations, Dep't of Just. (Dec. 12, 2023), https://www.justice.gov/opa/media/1328226/dl?inline.

[16] Press Release on SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, Securities & Exchange Commission (July 26, 2023), https://www.sec.gov/news/press-release/2023-139.

[17] Question 104B.01, Section 104B. Item 1.05 Material Cybersecurity Incidents, Exchange Act Form 8-K: Questions and Answers of General Applicability, U.S. Securities and Exchange Commission (last updated December 14, 2023), https://www.sec.gov/divisions/corpfin/guidance/8-kinterp.htm.

[18] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=124.

[19] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=127.

[20] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=127.

[21] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=129.

[22] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=130.

[23] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=130.

[24] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=132.

[25] https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf#page=129.