wiley

ALERT

CISA's Proposed Cyber Incident Reporting Requirements Would Hit a Range of Industries and Sectors

March 29, 2024

The U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is publishing a proposed rule (Proposal or NPRM) that will require broad segments of industry to meet onerous and quick reporting requirements following certain cyber incidents. This new incident reporting framework – if adopted as proposed – would mark a sea change in the already complicated cybersecurity incident reporting landscape. Put simply, CISA proposes to require reporting of many incidents, on a very short timeframe by larger segments of the private sector than are currently required to make reports under U.S. cybersecurity and incident reporting laws. In taking a broad view of its authorities and the goals that Congress sought to promote in the law, CISA has proposed a complex and sweeping regulatory regime that has not been harmonized with existing federal cyber incident reporting requirements.

At a high level, the Proposal – issued at the direction of Congress in the Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) – would require a broad array of newly "covered entities" to report to CISA, within prescribed deadlines and on an ongoing basis, detailed information about covered cyber incidents and ransom payments. It also creates new data retention requirements and subpoena authorities for the government. The devil, however, is in the details; and this Proposal provides 447 pages worth of details.

In this Alert, Wiley's cybersecurity team – which has been involved in incident reporting proposals, mandates, and compliance for more than 15 years – unpacks this complex NPRM and identifies

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Sydney M. White
Special Counsel
202.719.3425
swhite@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

preliminary issues and observations to help as companies begin to work through all of these details.

What Are the Key Takeaways?

The NPRM proposes a reporting framework that would require broad segments of industry to meet onerous and rapid reporting requirements following certain cyber incidents. Of particular note:

- ***An array of companies will qualify as covered entities***. CISA's new rules are focused on the 16 Critical Infrastructure Sectors derived from Presidential Policy Directive-21 Critical Infrastructure Security and Resilience (February 12, 2013), which is currently being re-written by the Biden Administration, and includes the Communications Sector, the Defense Industrial Base Sector, the Information Technology Sector, and the Transportation Systems Sector, to name a few. CISA is proposing to apply CIRCIA reporting requirements to (1) all entities within Critical Infrastructure except small businesses; and (2) all entities that meet one or more sector-based criteria, including providing wire or radio communications services, providing operationally critical support to the Department of Defense, owning or operating financial services sector infrastructure, providing support to elections processes through information and communications technology, or providing essential public health-related services.
- ***A broad range of incidents may be reportable.*** CISA's approach to covered cyber incidents is limited to "substantial" cyber incidents, but the term substantial has been construed broadly and leaves certain ambiguities. CISA frequently acknowledges the larger reach of its proposed regulations but says that broader coverage may be warranted for those sectors or industries that have been historically targeted by malicious cyber actors or where there is a greater likelihood of significant national security, economic security, or public health and safety consequences associated with the disruption of the reliable operation of Critical Infrastructure. And aspects of CISA's Proposal raise operational questions and ambiguities. For example, CISA's definition of "third party" incidents — that is, incidents involving vendors or suppliers of covered entities – as currently drafted could be read broadly.
- ***Reporting timelines will be short***. Covered cyber incident reports will be due within 72 hours after a covered entity reasonably believes a covered incident has occurred, and ransom payment reports are due within 24 hours of a ransom payment being made.

Additionally, with this Proposal, CISA has attempted to address a myriad of issues including ***data preservation and recordkeeping requirements*** for covered entities, ***ensuring protections*** for covered entities regarding the information they report – including liability protections as well as confidentiality protections, and ***enforcement mechanisms*** for CISA.

As companies begin to work through all of these details, it will be important to assess whether your organization fits within the broad scope of the proposed definition of "covered entity;" how your organization would be able to operationalize these comprehensive, onerous, and fast reporting requirements for "covered cyber incidents" and ransom payments; and how such requirements harmonize – or create tension – with your organization's current regulatory and contractual incident reporting requirements. Understanding these and other issues will help to measure the impact of this proposed new framework on your organization, as well as to inform any potential engagement with CISA, as the agency is inviting comments on its NPRM by **June 3,**

2024.

What Prompted CISA's New Proposal?

CISA's proposed new cyber incident reporting framework was mandated by Congress under the Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Signed into law on March 15, 2022, CIRCIA directed CISA to (1) issue a Notice of Proposed Rulemaking (NPRM) by March 15, 2024, and (2) issue a final rule within 18 months of publication of the NPRM, which will likely be on or about **October 4, 2025**.

CISA's NPRM – which was issued after the March 15 deadline – follows a Request for Information that CISA issued in September 2022, and several Listening Sessions hosted by CISA on this topic. While the concept of new incident reporting mandates was mandated by Congress, CISA here has taken an expansive approach that may go beyond what Congress envisioned and that clearly overlaps with pre-existing cyber incident reporting obligations already issued by the Department of Defense, the Federal Communications Commission, the Securities and Exchange Commission (SEC), the Food and Drug Administration, and Department of Energy, to name a few.

What Are the Key Elements of CISA's Broad New Proposal?

Overall, the Proposal outlines CISA's rules to implement CIRCIA's requirement for "covered entities to report to CISA within certain prescribed timeframes any covered cyber incidents, ransom payments made in response to a ransomware attack, and any substantial new or different information discovered related to a previously submitted report." NPRM at 14. To accomplish this, CISA is proposing a new 20-part rule, including:

- Section 226.1, which defines **key terms**, including "covered cyber incident," "covered entity," "personal information," and "substantial cyber incident," "cybersecurity threat," "information system," "personal information," "supply chain compromise," among others.
- Section 226.2, which describes the **applicability of the rules** to certain entities within Critical Infrastructure Sectors – i.e., those that are considered to be "covered entities." The rules will apply based on a size-based criteria (e.g., the entity exceeds the small business size standard) or a sector-based criterion because CISA says that an entity's size does not necessarily reflect criticality. CISA lays out specific-sector based criteria for each sector in Critical Infrastructure.
- Section 226.3, which details the **circumstances that trigger mandatory reports**, including when a covered entity experiences a covered cyber incident, makes a ransom payment, has another entity make a ransom payment on its behalf, or acquires substantial new or different information after submitting a previous CIRCIA Report.
- Section 226.4, which **outlines exceptions to reporting requirements**, which are proposed as:
    - An exception for a covered entity that must report "substantially similar information within a substantially similar timeframe" to another federal agency, provided that federal agency has an information sharing agreement in place with CISA;

  - An exception for multi-stakeholder entities that manage the Domain Name System, such as Internet Corporation for Assigned Names and Numbers (ICANN) or the Internet Assigned Numbers Authority (IANA);
  - An exception for federal agencies that must already report incidents to CISA under the Federal Information Security Modernization Act of 2014 (FISMA); and
- Section 226.5, which lists the **four main mandatory report types and the deadline for each**, including:
  - Covered Cyber Incident Reports – due no later than 72 hours after the covered entity reasonably believes the covered cyber incident has occurred;
  - Ransom Payment Reports – due no later than 24 hours after the ransom payment has been paid;
  - Joint Covered Cyber Incident and Ransome Payment Reports – due no later than 72 hours after the covered entity reasonably believes the covered cyber incident has occurred; and,
  - Supplemental Reports – due "promptly", which CISA interprets as within 24 hours of the event or new information that triggers the supplemental report.
- Section 226.6, which proposes the **manner and form of the reports**, which CISA contemplates primarily as a web-based submission through a form on CISA's website that will collect standardized information through a dynamic interface that will be tailored based on the type of report the covered entity seeks to submit and the information provided. CISA plans to allow alternative methods of reporting including telephone as a backup, and to maintain flexibility in case the web-based form is unavailable.
- Sections 226.7-226.11, which list the **content requirements** for the four main report types.
- Section 226.12, which allows for a covered entity to utilize a **third party to submit reports on its behalf**, and outlines the rules around that process, both for covered entities and third-party reporters.
- Section 226.13, which **outlines data preservation and recordkeeping requirements** for covered entities related to covered cyber incidents or ransom payments.
- Sections 226.14-17, which outline **enforcement mechanisms for CISA** to obtain information from a covered entity about a covered cyber incident or ransom payment that the covered entity does not report – including issuing a request for information, a subpoena to compel disclosure, making a referral to the Attorney General for a civil enforcement action, and launching acquisition, suspension, and debarment procedures.
- Section 226.18-226.19, which detail **various protections related to reporting requirements**, including requirements related to the treatment and restrictions on the use of CIRCIA reports for information clearly designated as commercial, financial, or proprietary; an exemption from disclosure under the Freedom of Information Act; protection for legal privileges; restrictions on the use in regulatory actions; limited liability protection; steps to minimize the collection of personal information; and other procedures intended to protect privacy and civil liberties.
- Section 226.20, which includes procedural provisions related to **enforcement and severability**, including penalties for false statements and representations.

What Industries and Sectors Will Likely Be Impacted by the New Framework?

In Section 226.2 of the Proposed Rules, CISA proposes applying the reporting requirements to "covered entities," defined as all entities in one of the Critical Infrastructure sectors that exceed a small business size standard or meet one or more of designated sector-based criteria. The small business size standard is specified by the North American Industry Classification System Code in the U.S. Small Business Administration's Small Business Size Regulations set forth in 13 CFR part 121. For example, a large chain of retailers would be covered because it is part of the "Commercial Facilities" sector and exceeds the small business threshold.

In addition, entities that meet a "sector-based" criterion would be covered entities, even if they do not exceed the size standard. Some categories include organizations "involved with" certain functions, while others are more narrowly focused on those that own or operate certain infrastructure.

A non-exhaustive selection of CISA's sector-based criteria includes:

- Communications Sector: Entities that provide "communications services by wire or radio," including telecommunications carriers, internet service providers, broadcasters, cable providers, and satellite providers;
- Defense Industrial Base Sector: Entities that provide operationally critical support to the U.S. Department of Defense or process, store, or transmit covered defense information;
- Financial Services Sector: Entities that own or operate a financial services entity including banks, certain savings and loan companies or credit unions, and select entities regulated by the SEC;
- Information Technology Sector: Entities that provide or support IT services for the federal government;
- Transportation Sector: Entities such as freight and passenger rail, public transit, bus operators, pipeline facilities, air carriers and airports, or entities regulated under the Maritime Transportation Security Act or already subject to Transportation Security Administration cybersecurity reporting requirements;
- Government Facilities, Election Infrastructure Subsector: Entities that manufacture, sell, or provide IT or communications technologies specifically used to support election processes or report state and local election results; and
- Healthcare and Public Health Sector: Entities that provide essential public health-related services including owning or operating certain hospitals or manufacturing certain classes of drugs.

In conjunction with the sector specific criteria, CISA has proposed that the covered entity is "the entire entity … not the individual facilities or functions" that meet the sector-specific criteria. As a consequence, a substantial cyber incident experienced by a non-critical part or facility of the entity would still need to be reported.

What Types of Cyber Incidents Will Trigger Reporting Requirements?

CISA proposes to define a "covered cyber incident" that must be reported as a "substantial cyber incident" experienced by a covered entity. CISA provides minimum requirements for the types of substantial cyber incidents that qualify as covered cyber incidents. CISA proposes that the term substantial cyber incident means a cyber incident that leads to any of the following:

- A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
- A serious impact on the safety and resiliency of a covered entity's operational systems and processes;
- A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; or,
- 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: (i) compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or (ii) supply chain compromise.

CISA offers additional explanation of assessing whether an incident meets those criteria, such as 1) the "type, volume, impact, and duration of the loss" of confidentiality, integrity, or availability; 2) the scale and duration of impacts to safety and resiliency; and, 3) the scope and nature of the disruption to business operations.

However, for incidents in which the covered entity's information system or network, or the nonpublic information on it, are accessed without authorization through a cloud, managed-service, or third-party data hosting provider or supply chain compromise, CISA proposes to omit the impact thresholds. There is significant ambiguity as to the scope of the proposed definition, which could be read to sweep broadly. Given the ubiquity of the use of third-party hosting providers and services, CISA's proposed definition could pose significant challenges for Critical Infrastructure companies in determining whether a covered cyber incident has occurred.

CISA expressly excludes from the term "substantial cyber incident" any lawfully authorized activity of a United States Government entity or SLTT Government entity (including activities undertaken pursuant to judicial process) and any event where the cyber incident is perpetuated in good faith by an entity in response to a specific request by the owner or operator of the information system. Because CISA is focusing on actual impact, the threat of disruption as extortion (e.g., threats associated with a ransomware attack) is not considered a substantial cyber incident. In other words, being the victim of a ransomware attack where disruption is threatened doesn't count, but a ransomware attack that causes actual disruption must be reported to CISA as a substantial cyber incident if suffered by a covered cyber entity.

What Are Examples of Incidents That Likely Would Qualify as Substantial Cyber Incidents?

CISA advises that the following are examples of incidents that would likely qualify as a substantial cyber incident:

- A distributed denial-of-service attack that renders a covered entity's service unavailable to customers for an extended period of time.

- Any cyber incident that encrypts one of a covered entity's core business systems or information systems.
- A cyber incident that significantly increases the potential for a release of a hazardous material used in chemical manufacturing or water purification.
- A cyber incident that compromises or disrupts a Bulk Electric System (BES) cyber system that performs one or more reliability tasks.
- A cyber incident that disrupts the ability of a communications service provider to transmit or deliver emergency alerts or 911 calls, or results in the transmission of false emergency alerts or 911 calls.
- The exploitation of a vulnerability resulting in the extended downtime of a covered entity's information system or network.
- A ransomware attack that locks a covered entity out of its industrial control system.
- Unauthorized access to a covered entity's business systems caused by the automated download of a tampered software update, even if no known data exfiltration has been identified.
- Unauthorized access to a covered entity's business systems using compromised credentials from a managed service provider.
- The intentional exfiltration of sensitive data in an unauthorized manner for an unauthorized purpose, such as through compromise of identity infrastructure or unauthorized downloading to a flash drive or online storage.

What Are Examples of Incidents That Likely Would Not Qualify as Substantial Cyber Incidents?

CISA indicates that the following examples would likely not qualify as substantial cyber incidents:

- A denial-of-service attack or other incident that only results in a brief period of unavailability of a covered entity's public-facing website that does not provide critical functions or services to customers or the public.
- Cyber incidents that result in minor disruptions, such as short-term unavailability of a business system or a temporary need to reroute network traffic.
- The compromise of a single user's credential, such as through a phishing attempt, where compensating controls (such as enforced multifactor authentication) are in place to preclude use of those credentials to gain unauthorized access to a covered entity's systems.
- Malicious software is downloaded to a covered entity's system, but anti-virus software successfully quarantines the software and precludes it from executing.
- A malicious actor exploits a known vulnerability, which a covered entity has not been able to patch but has instead deployed increased monitoring for tactics, techniques, and procedures (TTPs) associated with its exploitation, resulting in the activity being quickly detected and remediated before significant additional activity is undertaken.

Does CISA Propose Protections for Covered Companies That Submit Reports?

CISA proposes to adopt several protections, as outlined in CIRCIA, for information reported and for entities and persons described in the reports. CISA would allow covered entities to mark reports as protected commercial, financial and proprietary information, exempt them from Freedom of Information Act requests, maintain privileges such as attorney-client privilege, and waive any ex parte communications rules.

CISA also proposes, consistent with the underlying statute, regulatory and liability protections for covered entities. For example:

- The NPRM proposes to prohibit federal and state, local, tribal, and territorial government from using information obtained solely through a CIRCIA report to regulate or conduct an enforcement proceeding against the covered entity making a report. However, such protection would not apply if the government agency in question has separate regulatory authority and allows covered entities to use CIRCIA reports to comply with the agency's own, independent reporting requirement.
- The NPRM also proposes liability protections from litigation based solely on submission of a CIRCIA report or response to a CISA request for information about the report, and a broad evidentiary and discovery protection prohibiting the use in litigation of CIRCIA reports and communications created for the sole purpose of preparing, drafting, or submitting such reports. As such, CISA will not provide CIRCIA reports in response to third-party discovery requests.
- The Proposal also contemplates limitations on federal government use of CIRCIA reports that are generally consistent with those applicable to voluntary reports made under the Cybersecurity Act of 2015. The federal government can use CIRCIA reports for cybersecurity purposes, including investigating, disrupting, or prosecuting a crime arising out of the covered cyber incident, as well as other limited exceptions for responding to specific threats of physical, "serious economic" harm, fraud, identity theft, espionage or theft of trade secrets.

CISA's proposed protections do not, however, protect a reporting company from civil or criminal actions arising out of the underlying cyber incident, nor do they apply if a company receives a subpoena from CISA demanding information about a cyber incident.

How Does CISA Attempt to Harmonize Its New Proposed Rules with Other Existing Requirements?

Congress provided CISA with a significant tool for reducing duplication in federal cyber incident reporting in CIRCIA by granting CISA authority to accept an incident report filed with another federal agency in lieu of a CIRCIA report. As noted earlier, in Section 226.4, CISA proposes parameters surrounding when it will accept a report made to another agency in satisfaction of CIRCIA's reporting requirements. CISA will enter into an agreement with a federal agency when CISA has determined the agency requires cyber incident reporting on "substantially similar information in a substantially similar timeframe" and the agency has "committed to providing the covered entity's report to CISA within the relevant deadlines." In the NPRM, CISA commits to working in good faith with other federal agencies "to have CIRCIA [interagency] Agreements finalized before the effective date of the final rule."

CISA contributed to the congressionally authorized and DHS-chartered Cyber Incident Reporting Council (CIRC) tasked with examining and making recommendations on harmonization of cyber incident reporting. In the NPRM, CISA proposes a reporting form which includes the majority of content included in the Council's model reporting form but varies to the extent CISA sees as required by CIRCIA. CISA proposes to incorporate portions of the Council's definition of "substantial cyber incident" into CISA's definition. However, CIRCIA's statutory requirement for the incident to take place and the impact to have occurred, prevents CISA from using the entire model definition.

After examining other agencies' definitions of a covered cyber incident in addition to the CIRC, CISA concludes the most effective approach to harmonization is for other agencies to use the CIRC's model definition of covered cyber incident to the extent possible by revisiting current rules or applying it in future rulemakings.

How Can Interested Stakeholders Get Involved as CISA Continues to Consider This Proposal?

There are important areas of law and policy that merit careful consideration and presentation to CISA as it evaluates next steps. CISA is accepting public comments on these complex and detailed proposed rules. Comments will be due 60 days after the NPRM is published in the Federal Register. If the Proposal is published – as planned – on April 4, 2024, then comments will be due by **June 3, 2024.**

***

Wiley's Privacy, Cyber & Data Governance team has helped companies of all sizes from various sectors proactively address risks and compliance with new cybersecurity laws and requirements. Our team has been actively involved in advocacy to CISA on these new rules. Please reach out to any of the authors with questions.