JENNER & BLOCK

CISA Announces Proposed Cyber Incident Reporting Rule

Client Alerts

04/02/2024
By: Shoba Pillay, Madeleine Findley, Zoë Higgins Reinstein

On March 27, 2024, the Cybersecurity and Infrastructure Security Agency (CISA), an operational component of the Department of Homeland Security (DHS), posted for public inspection its long-anticipated notice of proposed rulemaking for a cyber incident response rule (the Proposed Rule). The Proposed Rule is scheduled to be published to the Federal Register on April 4, 2024.

Under the Proposed Rule, a broad range of "covered entities" would be required to report significant cyber incidents within 72 hours of discovery, report ransom payments within 24 hours, and retain material relevant to making the report. The Proposed Rule authorizes CISA to compel information disclosure by covered entities it suspects failed to report a cyber incident or made a ransom payment.

The Proposed Rule significantly expands the scope of cyber incident reporting requirements under federal law without harmonizing with other, existing federal reporting obligations. It brings more private sector industries and more incidents under CISA's jurisdiction with an unprecedented reporting period.

CISA estimates that, by 2033, the Proposed Rule may cover 316,000 entities, with a total cost of compliance of approximately $1.4 billion.

Regulatory Landscape: CIRCIA

The Proposed Rule fulfills a mandate in the Cyber Incident Reporting for Critical Infrastructure Act of 2022, 6 U.S.C. §§ 681–681(g) (CIRCIA), which requires CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransom payments to CISA.

The cyber incident reporting landscape currently consists of dozens of federal, state, local, tribal, and territorial cyber incident reporting requirements. In the two years since CIRCIA was enacted, multiple federal agencies, including the SEC, FCC, and HHS have adopted their own cyber incident or breach reporting requirements. The Proposed Rule is intended to supplement these reporting requirements by helping CISA identify cyber incident patterns in real-time, fill critical information gaps, rapidly deploy resources to help victims of cyber-attacks, inform others who could potentially

be affected, and prevent future incidents. Prior to CIRCIA, there was no federal statute or regulation requiring cross-sector reporting of cyber incidents to the federal government. According to CISA Director Jen Easterly, "CIRCIA is a game changer for the whole cybersecurity community, including everyone invested in protecting our nation's critical infrastructure."

Highlights of the Proposed Rule

Under the Proposed Rule (§ 226.1; § 226.13), "covered entities" (defined below) will be required to:

- Report to CISA "substantial" cyber incidents (defined below) within **72 hours** of discovery;
- Report to CISA ransom payments within **24 hours** of payment; and
- Retain information relevant in making the report for **two years**.

The Proposed Rule grants CISA power to subpoena covered entities that it suspects failed to report a substantial cyber incident or ransom payment.

The reports submitted under the final rule will often include sensitive security, business, or other confidential information. CIRCIA requires the rule to include procedures for protecting data subjects consistent with the Cybersecurity Information Sharing Act of 2015. 6 U.S.C. § 1504(b). The Proposed Rule includes a draft privacy and civil liberties guidance document that would apply to CISA's retention, use, and dissemination of personal information contained in a company's report to CISA and provide guidance to other federal agencies with whom CISA shares such reports. Further, CIRCIA incident reports will only be shared with "appropriate or entities," though the Proposed Rule does not clarify whether this includes non-federal stakeholders as well as federal agencies.

Covered Entities: Sector & Size Thresholds

CIRCIA defines a "covered entity" based on the critical infrastructure sectors identified in Presidential Policy Directive 21 (PPD-21). PPD-21 designates 16 critical infrastructure sectors, including communications, education, emergency services, financial services, public health, IT, and transport. However, CIRCIA requires CISA to further clarify the meaning of the term.

CISA's 2015 Sector-Specific Plans indicated that some non-obvious entities may qualify as critical infrastructure, and CISA has indicated that it will publish reference materials on the entities covered in tandem with the final rule. Further, the Proposed Rule offers supplemental sector-based criteria for specific industries: chemicals, communications, critical manufacturing, defense contracting, emergency services, financial services, government facilities, healthcare and public health, IT, nuclear, transportation, and water and wastewater. As a result, the Proposed Rule will significantly expand federal incident reporting requirements to a wide array of industry sectors and businesses, including those subject to existing federal sector-specific reporting obligations.

The Proposed Rule only covers entities that exceed the small business size standard specified by the US Small Business Administration's Small Business Size Regulations. 13 C.F.R. part 121.

The Proposed Rule exempts federal agencies, the Internet Corporation for Assigned Names and Numbers (ICANN), and the American Registry for Internet Numbers (ARIN). § 226.4.

Substantial Cyber Incidents

Covered entities must report "substantial" cyber incidents. § 226.1. A cyber incident is "an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually jeopardizes, without lawful authority, an information system."

Regardless of its cause, a cyber incident would be "substantial" if it leads to:

- 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) a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or (b) a supply chain compromise.

Examples of substantial cyber incidents include: (1) a denial-of-service attack that renders the covered entity's service unavailable to customers for an extended period of time; (2) a cyber incident that encrypts one of the covered entity's core business systems or information systems; or (3) unauthorized access to the covered entity's business systems using compromised credentials from a managed service provider.

However, a substantial cyber incident need not be reported if the entity is legally required to report substantially similar information within a substantially similar timeframe. The other federal agency must have entered a "CIRCIA agreement" with CISA providing for an inter-agency information-sharing mechanism. Upon promulgation of the final rule, CISA will maintain an accurate catalog of all CIRCIA agreements on its website.

The following cyber incidents are not substantial and need not be reported:

- Any lawfully authorized activity of a US government entity or state, local, tribal, or territorial government entity, including activities undertaken pursuant to a warrant or other judicial process;
- Any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; or
- The threat of disruption is extortion under 6 U.S.C. §650(22).

Examples of non-substantial cyber incidents include: (1) a denial-of-service attack 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; (2) cyber incidents that result in minor disruptions or the compromise of a single user's credential; or (3) malicious software is downloaded but anti-virus software successfully precludes it from executing.

Data Retention and Recordkeeping

After making a report of a substantial cyber incident or ransom payment, the Proposed Rule would also require covered entities to preserve materials used to file the report. § 226.13. This information includes:

- Any communications with a threat actor, including copies of actual correspondence, notes taken during any interactions, and so forth;
- Indicators of compromise;
- Relevant log entries and forensic artifacts;
- Data and information that may help identify how a threat actor compromised or potentially compromised an information system;
- System information that may help identify exploited vulnerabilities;
- Information about any exfiltrated data;
- All data or records related to the disbursement or payment of any ransom payment, including but not limited to pertinent records from financial accounts associated with the ransom payment; and
- Any forensic or other reports concerning the incident, whether internal or prepared for the covered entity by a cybersecurity company or other third-party vendor.

Enforcement Power

The Proposed Rule grants CISA the authority to subpoena covered entities to compel disclosure "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." § 226.14(d). Further, CISA can refer the

inquiry to the US Department of Justice to bring a civil action or pursue acquisition penalties, suspension, or debarment if the entity fails to comply or provides an inadequate or false response.

Interim Voluntary Reporting

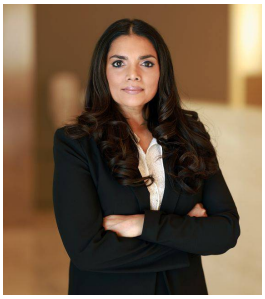
Under CIRCIA, the final rule must be published within 18 months of publication of the Proposed Rule, or October 4, 2025. While covered entities will not be required to report covered cyber incidents or ransom payments until the final rule goes into effect, CISA has encouraged all entities to voluntarily share this information with CISA in the interim.

Conclusion

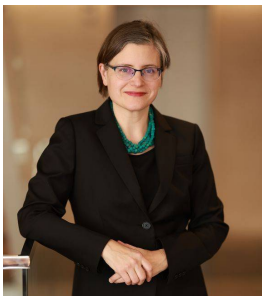
CISA's proposed cyber incident reporting rule would be a substantial shift in the cyber regulatory landscape. The Proposed Rule significantly expands the scope of cyber incident reporting requirements under federal law without harmonizing with other, existing federal reporting obligations. It covers more private sector industries and more incidents than ever before, with a shorter reporting period.

The Proposed Rule will be published in the Federal Register on April 4, 2024. Comments must be submitted through the Federal Rulemaking Portal at Regulations.gov by June 3, 2024.

Related Attorneys



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605



Madeleine Findley

Partner
mfindley@jenner.com
+1 202 639 6095

Zoë Higgins Reinstein

Associate
zreinstein@jenner.com
+1 312 840 7420

Related Capabilities

Data Privacy and Cybersecurity

Stay Informed →