Published on *The National Law Review* https://natlawreview.com

Newly Proposed Rule Expanding Cyber Incident Reporting to Affect Financial Services Companies

Article By:

Jon K. Jurva

D. Reed Freeman Jr.

Matthew W. Kulju

Recently, the US Department of Homeland Security's (DHS) Cybersecurity & Infrastructure Security Agency (CISA) issued a notice of proposed rulemaking (NPRM) which, if adopted, would require "covered entities" of critical infrastructure to report "substantial cyber incidents" to CISA within 72 hours, and to report ransomware payments within 24 hours.

The proposed rule defines the "critical infrastructure sector" to include "financial services," meaning banks, registered broker-dealers, and similar service providers would be subject to the rule. However, firms already obligated to report cybersecurity breaches to other federal agencies — such as the US Securities and Exchange Commission or Federal Trade Commission — would be exempt from reporting requirements under the proposed rule. The proposed rule implements the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CISA expects to publish a final rule by late 2025, with reporting likely beginning in 2026.

CISA estimates that the proposed rule may affect over 300,000 entities, which, according to CISA estimates, will submit more than 200,000 CIRCIA reports over the 11-year period of analysis, resulting in a $1.4 billion cost to the industry.

Covered Cyber Incidents

Importantly, not all cyber incidents are required to be reported. Under the proposed rule, covered entities would be required to report all "substantial" cyber incidents. For example, network traffic overload, successful antivirus software defense of downloaded malware, and successful single-user phishing attempts are not considered "substantial."

A “substantial” cyber incident is any event 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.
- Unauthorized access to a covered entity’s information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise.

Examples of substantial cyber incidents include a distributed denial-of-service (DDoS) attack that renders a service unavailable for an extended period of time, a cyber incident which encrypts business or information systems, or unauthorized access to an information system or network.

Compliance Requirements

Covered entities are obligated to:

- Report completed ransom payments within 24 hours and substantial cyber incidents within 72 hours of an entity’s reasonable belief that an incident has occurred through the web-based CIRCIA Incident Reporting Form available on CISA’s website.
- Describe the incident and perpetrator, vulnerabilities exploited, how the incident was carried out, and the covered entity’s security defenses and mitigation actions.
- Preserve data and records related to a covered incident or ransom payment for at least two years after an incident report was or should have been reported to CISA.

Failure to comply with reporting requirements may result in a referral to the attorney general for civil action, or for knowing and willful violations, criminal penalties under 18 U.S.C. §1001 for making false or fraudulent statements.

Takeaway

If the rule is adopted substantially as proposed, financial services entities will need to update their cybersecurity programs to comply with CISA’s reporting requirements in the event of a cyber incident. Although larger entities likely already have robust cybersecurity programs in place that can accommodate a reporting requirement, US Congress’ motivation behind mandated reporting is to better track the evolving nature of cyber-attacks for a broader group of covered entities.

ArentFox Schiff lawyers are available to assist information security personnel in reviewing their cybersecurity and compliance programs, assessing their vulnerabilities and risks, and implementing additional programs or controls to mitigate risks and ensure full compliance with applicable legal and notification requirements.

Additional research and writing from Jacob Blais, a 2024 summer associate.

National Law Review, Volume XIV, Number 179