The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 35770

July 12, 2024

ICI Files Comment Letter on CISA's Cyber Incident Reporting Proposal

[35770]

July 12, 2024

TO: ICI Members
Chief Compliance Officer Committee
Chief Information Security Officer Committee
SEC Rules Committee
Technology Committee SUBJECTS: Compliance
Cybersecurity RE: ICI Files Comment Letter on CISA's Cyber Incident Reporting Proposal

Last week, ICI filed the attached comment letter on the notice of proposed rulemaking on Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements from the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security.[1] The proposal would require a "covered entity"[2] in one of sixteen critical infrastructure sectors (including the financial services sector) to file cyber incident reports to CISA within 72 hours after the covered entity reasonably believes a "substantial cyber incident"[3] has occurred or within 24 hours of a ransomware payment, and to provide updates within 24 hours if new or different information becomes available or if a ransom has been paid (collectively, "CIRCIA Reports").[4] In addition, the proposal sets forth the reportable items each CIRCIA Report must contain, data and record preservation requirements for each covered entity, reporting exceptions, and how CISA may use the information received.[5]

ICI's comment letter makes five main recommendations.

First, the letter strongly encourages CISA to work with federal financial regulators, like the Securities and Exchange Commission (SEC), to relieve investment advisers and investment companies registered or regulated by the SEC from having to file multiple cyber incident reports with multiple agencies. In this regard, it strongly recommends that CISA work with other agencies to agree that the filing of an initial CIRCIA Report and any related updates would satisfy the other agencies' cyber incident reporting requirements. Designating a single agency to collect cyber incident reports would eliminate the need for agencies to continuously compare cyber incident reporting requirements and would streamline a covered entity's compliance and reporting functions by eliminating the need for the covered entity to consider reporting to multiple agencies and monitor compliance with a reporting exception.[6] Alternatively, the letter asks CISA to clarify with specificity which

covered entities are excepted from CISA reporting and from which specific provisions they are excepted.

Second, the letter asks CISA (i) to clarify how it will supplement the work of already well-established entities that act in a similar capacity, and (ii) to establish guidelines to quickly assist an impacted critical infrastructure sector or covered entity in a manner that justifies the proposal's burdensome requirements to promptly file CIRCIA Reports.

Third, it highlights specific information in CIRCIA Reports that are unnecessary, subjective, or that may require constant updating and asks that CISA refine its requirements to ensure that each piece of required disclosure is necessary, will help the impacted firm and other firms combat cyber threats, and substantiates the costs it would impose to produce. The letter also asks CISA to exclude foreign subsidiaries from the final rule's purview.

Fourth, the letter asks CISA to require a third party to report a covered entity's cyber incidents when those incidents are facilitated through the third party's data hosting networks. Those third parties would have access to better information about the root cause of the intrusion and would be in a better position to describe the unauthorized access and extent of the issue. The third party data hosting providers also could reduce the number of reports filed by filing only one report when a cyber incident impacts several covered entities.

Finally, the letter states that CISA and other agencies that would have access to the CIRCIA Reports must ensure that the information from those reports remains confidential. It recommends that CISA and those agencies leverage industry best practices as a resource for effective safeguarding policies and procedures and that they employ, among other things, access controls on information, continued information security assessments against objective metrics, and independent evaluations from inspector generals and other third parties. Ensuring confidentiality, anonymization of data, and data security will give critical infrastructure sectors more confidence and trust in CISA and will lead to covered entities furnishing more and better data.

Kenneth Fang
Associate General Counsel

Notes

[1] See Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Docket No. CISA-2022-0010, 89 Fed. Reg. 23644 (Apr. 4, 2024) ("proposal"), available at https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf. CISA subsequently extended the proposal's comment period for an additional 30 days. See Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements; Extension of Comment Period, Docket No. CISA-2022-0010, 89 Fed. Reg. 37141 (May 6, 2024), available at https://www.govinfo.gov/content/pkg/FR-2024-05-06/pdf/2024-09505.pdf.

[2] A "covered entity" would include entities in a critical infrastructure sector that exceed certain small business sizes, which for companies in the business of "Portfolio Management and Investment Advice" are those that exceed $47 million in assets. See proposed Section

226.2(a).

[3] A "substantial cyber incident" is a cyber incident that leads to one of four items:

- A substantial loss of confidentiality, integrity or availability of an information system or network.
- A serious impact on the safety and resiliency of operational systems and processes.
- A disruption of an entity's ability to engage in business or industrial operations, or deliver goods or services.
- Unauthorized access to an entity's information system or network, or any non-public information contained therein, that is facilitated or caused by: (i) a compromise to a third party in one's digital ecosystem (e.g., a cloud service provider, managed service provider, or other data hosting provider); or (ii) a supply chain compromise.

See proposed Section 226.1 (defining "substantial cyber incident").

[4] See proposed Sections 226.3 to 226.5 (setting forth requirements to report substantial cyber incidents and related timeframes).

[5] See proposed Sections 226.7 to 226.11 (setting forth information that each CIRCIA Report would require); proposed Section 226.13 (setting forth data and record preservation requirements); proposed Section 226.4 (setting forth reporting exceptions); and proposed Sections 226.18 and 226.19 (setting forth limitations on the treatment and use of the information received and procedures for protecting privacy).

[6] In addition, designating CISA as the central repository makes sense, given its capacity to identify critical infrastructure sectors undergoing cyberattacks, its focus and expertise in cybersecurity, and its ability to partner with hacked firms to counter cyberattacks.
