The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE
1401 H Street, NW, Washington, DC 20005 USA

July 3, 2024

Ms. Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Sent via the Federal eRulemaking Portal
http://www.regulations.gov

Re: *Docket Number CISA-2022-0010*

Dear Director Easterly:

The Investment Company Institute[1] is writing to provide its views on the notice of proposed rulemaking on *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements* from the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security (CISA).[2] Many of our members—investment companies and investment advisers registered with or regulated by the Securities and Exchange Commission ("SEC Registrants")—are financial services companies that exceed the proposed "small business size standard" and, thus, are within the proposal's ambit.[3] At the same time, the SEC has issued a proposal that, if adopted, will require SEC Registrants to establish cybersecurity risk management programs and make cyber incident reports that would overlap with CISA's

[1] The Investment Company Institute (ICI) is the leading association representing the asset management industry in service of individual investors. ICI's members include mutual funds, exchange-traded funds (ETFs), closed-end funds, and unit investment trusts (UITs) in the United States, and UCITS and similar funds offered to investors in other jurisdictions. Its members manage $35.2 trillion invested in funds registered under the US Investment Company Act of 1940, serving more than 100 million investors. Members manage an additional $9.4 trillion in regulated fund assets managed outside the United States. ICI also represents its members in their capacity as investment advisers to certain collective investment trusts (CITs) and retail separately managed accounts (SMAs). ICI has offices in Washington DC, Brussels, and London and carries out its international work through ICI Global.

[2] *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.

[3] *See* proposed Section 226.2 (setting forth the criteria for "covered entities" required to file cyber incident reports with CISA).

proposed incident reports.[4] We support the proposal's goals and appreciate CISA's intent to fully harmonize reporting requirements among agencies, but we strongly encourage CISA to work together with the Department of the Treasury in its role as the sector risk management agency (SRMA) for the financial sector and with federal financial regulators, like the SEC, to establish one central government repository to collect these cyber incident reports and, to the extent possible, relieve SEC Registrants from having to file redundant multiple reports with multiple agencies.[5] Doing so would most efficiently and effectively serve the goal of CIRCIA and the proposal to protect national and economic security and public health and safety from cyberattacks and better enable a coordinated, informed US response to the foreign governments and criminal organizations conducting these attacks.

We provide our recommendations below to help establish CISA as the single repository for cyber incident reports. Achieving this will satisfy these important goals in a manner that would relieve investment advisers and investment companies from the burden of reporting duplicative information to more than one regulator.[6]

In addition, we provide comments on other portions of the rulemaking. Our comments are organized in five sections: (1) Require Covered Entities to Provide a Single Report to One Central Government Repository; (2) Clarify CISA's Role and Justify the Prompt Response Periods; (3) Appropriately Calibrate the Content and Scope of Required Filings; (4) Require Third-Party Reporting for Substantial Cyber Incidents Facilitated Through Cloud Service Providers, Managed Service Providers, and Third-Party Data Hosting Providers; and (5) Ensure the Confidential Nature of Reports.

---

[4] *See Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, Investment Company Act Rel. No. 34497, 87 Fed. Reg. 13524 (Feb. 9, 2022) ("SEC IA/IC Proposal"), *available at* https://www.govinfo.gov/content/pkg/FR-2022-03-09/pdf/2022-03145.pdf. The SEC reopened the comment period for the SEC IA/IC Proposal in March 2023, when it proposed to require broker-dealers, transfer agents, and other entities to have cybersecurity risk management programs. *See Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period,* Investment Company Act Rel. No. 34885 (Mar. 15, 2023). ICI filed comment letters in response to each of these releases. *See* Letters from Susan M. Olson, General Counsel, ICI, to Ms. Vanessa Countryman, Secretary, SEC, dated April 11, 2022 ("April 2022 ICI Letter") and May 22, 2023 ("May 2023 ICI Letter"), *available at* https://www.sec.gov/comments/s7-04-22/s70422-20123076-279408.pdf and https://www.sec.gov/comments/s7-04-22/s70422-191859-382242.pdf.

[5] We believe that CISA should cooperate with all agencies to eliminate requirements that covered entities file multiple reports across agencies. For purposes of this letter, however, at times, we simply reference the need for CISA to work with the *SEC*, to highlight the reporting burdens on our members—investment advisers and investment companies.

[6] In this regard, as further discussed in Section 1, CISA should work with the SEC to agree to terms in which the filing of an initial CIRCIA Report and related updates would meet the SEC's cyber incident reporting requirements.

1. Require Covered Entities to Provide a Single Report to One Central Government Repository

As CISA acknowledges, several entities that would be required to file CIRCIA Reports about cyber incidents to CISA must also report cyber incidents to other agencies.[7] CISA seeks to harmonize CIRCIA with these other federal reporting regimes and highlights its commitment to working with financial services federal regulatory agencies (*e.g.*, the SEC) to enable, to the extent practicable, entities subject to both CIRCIA and another reporting requirement to comply with each regime through the submission of a single report to the federal government.[8] Consistent with this approach and CIRCIA, CISA proposes to except covered entities from filing CIRCIA Reports and subsequent updates to CISA when certain conditions are met (the "reporting exception"), including that the covered entity file a substantially similar cyber incident report with another agency within a substantially similar timeframe.[9] Further, CISA would impose a responsibility on covered entities to confirm that the conditions of the reporting exception are met, including confirming that an information sharing agreement that CISA enters into with a federal agency is applicable to the covered entity and that the specific reporting obligation the covered entity seeks to satisfy qualifies for the exception.[10]

1.1. Designate CISA as the Single Government Repository to Collect All Cyber Incident Reports

We strongly encourage CISA to follow through on its commitment to have a covered entity file a single report with the federal government for each cyber incident to fulfill all of its related regulatory obligations. The proposed reporting exception as drafted, however, will not achieve this laudable goal. Instead, it would require a covered entity to both comply with the cyber incident requirements of the SEC and meet the conditions of the exception (*e.g.*, monitoring the status of information sharing agreements). Rather than requiring covered entities to comply with multiple sets of cyber incident reporting requirements, an alternative way to harmonize the reporting requirement would be to create one central repository to which each covered entity would submit all of its federally-required cybersecurity incident reports. Recognizing that CISA

---

[7] A "CIRCIA Report" would include cyber incident reports, ransom payment reports, joint cyber incident/ransom payment reports, and supplemental reports filed with CISA.

[8] *See* proposal at 23690.

[9] To rely on the proposed reporting exception, among other things: (i) CISA must determine that the other reporting requirement contains substantially similar information to that required in a CIRCIA Report; (ii) CISA must be able to obtain the report in a substantially similar timeframe as it would a CIRCIA Report; (iii) CISA and the federal agency must have signed an information sharing agreement that satisfies the requirement of 6 U.S.C. 681(g)(a); (iv) CISA and the federal agency must have a mechanism in place by which the federal agency can share the report with CISA within the required timeframe; and (v) the federal agency must require the covered entity to file the report pursuant to a legal, regulatory or contractual obligation. *See proposed* Section 226.4. *See also* proposal at 23708.

[10] *See* proposed Section 226.4(a). CISA proposes only to enter into agreements with federal agencies and permit covered entities to rely on the reporting exception when it determines that the agency receiving the cyber incident reports does so pursuant to a legal, regulatory, or contractual obligation, and that such reporting obligation requires the submission of substantially similar information in a substantially similar timeframe. *See* proposal at 23708.

does not have authority over other agencies' regulations,[11] CISA should work with the SEC to agree to terms in which the filing of an initial CIRCIA Report and related updates would meet the SEC's cyber incident reporting requirements.[12] Designating one agency to which covered entities would file all cyber incident reports and that would house reports for the federal government would eliminate the need for agencies to continuously compare cyber incident reporting requirements and would streamline a covered entity's compliance and reporting functions. Covered entities would no longer need to consider reporting to multiple agencies and would not need to evaluate information sharing agreements.[13]

1.2. Alternatively, CISA Should Clarify Which Covered Entities are Excepted from Some or All of CIRCIA Reporting

We understand that the SEC and other agencies have already imposed some cybersecurity reporting requirements that, having been formally adopted, would be hard to eliminate. Unless and until a single federal government repository for collecting cyber incident reports is designated, CISA should use the reporting exception to except *specified* covered entities subject to other agencies' requirements from having to file CIRCIA Reports and detail whether the exception covers the entire CIRCIA reporting requirement or just certain portions thereof.

CISA should clearly specify which covered entities are excepted from the CIRCIA reporting requirements, because it may be difficult for a covered entity, which remains responsible for confirming that it meets the reporting exception, to determine whether it is covered under a CISA/federal agency agreement. In this regard, CISA proposes to enter into agreements with other federal agencies and permit covered entities to rely on the reporting exception only when it determines that a covered entity is under some obligation to submit the cyber incident report, and

---

[11] *See* proposal at text surrounding n. 319.

[12] In this regard, CISA could work with the SEC and other agencies that have not yet finalized rules on cyber incident reporting (*e.g.*, the SEC's IA/IC Proposal) to ensure that covered entities are excepted from filing cyber incident reports if they file CIRCIA Reports with CISA.

[13] Although we generally are agnostic as to which agency serves as the government repository, it may make sense for CISA to do so to best fulfill Congress' intent to have CISA serve as the "newly minted central repository for cyber incident reporting." *See* proposal at 23704. With CISA's ability to monitor cyber incidents across industries, it is in the best position to identify areas undergoing cyberattacks and assist the US government and various industries in addressing them. In addition, with its focus and expertise in cybersecurity, CISA also can partner with hacked firms to counter cyberattacks. By contrast, other agencies, including SRMAs, may not be focused solely on cybersecurity and may have different rationales for adopting their cyber incident reporting requirements. For example, the SEC's proposed rules governing cybersecurity risk management for investment advisers and investment companies are intended for more limited purposes (*i.e.*, to inform the Commission in its oversight role to better understand the nature and extent of cybersecurity incidents at investment advisers and funds, how firms respond to such incidents to protect clients and investors, and how cyber security incidents affect the financial markets more generally). *See* SEC IA/IC Proposal at 13526. *See also* May 2023 ICI Letter at 12-14 (recommending that the SEC's proposed cybersecurity risk management rule for investment advisers and funds exclude SEC notification requirements when, among other things, the investment adviser or fund files a cyber incident report with CISA).

that such report contains substantially similar information and is filed in a substantially similar timeframe as a CIRCIA Report.[14] Determining the scope of CISA/federal agency agreement, however, may be difficult when an agency oversees multiple types of covered entities and imposes substantially similar but somewhat differing requirements for each. For example, last year, the SEC adopted cyber incident reporting requirements for public companies.[15] The SEC also proposed cyber incident reporting requirements for SEC-registered broker-dealers.[16] Further, we understand that the SEC may soon adopt similar requirements for registered investment advisers and funds.[17] With multiple sets of registrants adhering to potentially different cyber incident reporting requirements, it may be unclear whether an agreement with an agency covers all or only a subset of registrants. We therefore urge CISA to separately identify each type of covered entity an agreement covers and which types of entities it would except under the reporting exception (*e.g.*, public companies, SEC-registered broker-dealers, SEC-registered investment advisers, SEC-registered investment companies, business development companies).

Absent a full exception, CISA should explain what reported items, in particular, overlap between the other agency's cyber incident reports and the CIRCIA Report and what, if any, specific items specific groups of covered entities need to report separately to CISA.[18] The identification of regulatory reporting gaps, which CISA should undertake when considering whether to sign an

---

[14] *See supra* note 10. To reduce multiple filings, we suggest that CISA *flexibly* evaluate whether an agency's cyber incident report contains "substantially similar" information as that required in a CIRCIA Report. This would alleviate the risk of covered entities being subject to multiple reporting requirements solely because of subtle or technical differences (*e.g.*, "significant fund cybersecurity incidents" in the SEC IA/IC Proposal versus "substantial cyber incidents" under the proposal). Additionally, CISA should aim to avoid imposing new requirements on covered entities that already are subject to cyber incident reporting. Rather, it should aim to efficiently use the information already required from existing regulatory regimes.

[15] *See Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Securities Act Rel. No. 11216, 88 Fed. Reg. 51896 (Aug. 4, 2023), *available at* https://www.govinfo.gov/content/pkg/FR-2023-08-04/pdf/2023-16194.pdf.

[16] *See Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents*, Securities Exchange Act Rel. No. 97142, 88 Fed. Reg. 20212 (Apr. 5, 2023), *available at* https://www.govinfo.gov/content/pkg/FR-2023-04-05/pdf/2023-05767.pdf.

[17] *See* SEC IA/IC Proposal. As the SEC finalizes its SEC IA/IC Proposal, we encourage CISA to coordinate with them to either allow CISA to serve as the point of contact for cyber incident reports or to assist in the development of congruous reporting requirements consistent with its intent to develop harmonized reporting requirements that would enable CISA to determine that the SEC's regulations for advisers and funds are "substantially similar." *See* proposal at 23669 (discussing efforts to harmonize cyber incident reporting practices).

[18] It is not entirely clear whether CISA would allow a covered entity to use the reporting exception to satisfy portions of a CIRCIA Report, but proposed Section 226.4(a) indicates that it should: "A covered entity is responsible for confirming that a[n agreement between CISA and another agency] is applicable to the covered entity ***and the specific reporting obligation it seeks to satisfy*** under this part, and therefore, qualifies for this exemption." *See* proposed Section 226.4(a) (emphasis added).

agreement with the other agency, would provide clarity and reduce compliance questions for all covered entities in an industry. Reducing compliance questions and burdens and freeing up resources is critical, especially during a cybersecurity incident when firms should be focused on resolving the issue expeditiously and not on analyzing the specific reporting differences one regulator has as compared to another.

2. Clarify CISA's Role and Justify the Prompt Response Periods

CIRCIA and the proposal would require covered entities to file CIRCIA Reports within 72 hours after a covered entity reasonably believes a substantial cyber incident has occurred and 24 hours after a ransom payment has been made.[19] CISA indicates that the two major principles that heavily influenced the design of these proposed rules were the need to receive a multitude of reports and the importance of timeliness in both the receipt of reports and in CISA's ability to analyze and share information gleaned from those reports.[20]

We agree that reporting and timeliness can be important, but CISA must make certain that CIRCIA's required reporting and condensed reporting timeframes are in line with CISA's use of information to the benefit of critical infrastructure sectors and their underlying firms. The 72- and 24-hour reporting periods will tax firm resources, especially during the heat of a cyberattack response. CISA should better explain what it will do with the information received immediately after receiving it by establishing and publishing a fixed process and guidelines to expeditiously assist impacted firms and others.

The guidelines should clarify the additive role CISA will play in combatting cyber threats and how it will work in conjunction with already well-established entities that serve similar functions

---

[19] *See* proposed Section 226.5. Joint cyber incident reports covering both cyber incident and ransom payments must be filed within 72 hours after the covered entity reasonably believes a cyber incident has occurred, and supplemental reports must be filed promptly or no later than 24 hours after a ransom payment has been disbursed.

[20] *See* proposal at 23652-23. CISA notes that to achieve many of the regulation's goals—such as identifying adversary tactics, techniques, and procedures, and providing early warnings to enhance situational awareness of cyber threats—it needs to receive a sufficient quantity of CIRCIA Reports. *See* proposal at 23652. It notes that timeliness is necessary to achieve the important early visibility and warning aspects of this regime and to increase the likelihood that covered entities can address identified vulnerabilities and secure themselves. *See* proposal at 23653. CISA adds that it will use the timely information obtained from CIRCIA Reports to help critical infrastructure sectors learn about and defend themselves against cyber threats. For example, CISA states that:

> . . . the CIRCIA regulations will help improve the nation's cybersecurity posture in various ways, such as by allowing CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and share that information with network defenders so that they may take actions as they deem necessary to [protect] themselves from becoming victims of similar incidents.

See CISA, CIRCIA FAQs – For use during the Public Comment Period, *available at* https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/circia/faqs (in response to "What are the Purposes of CIRCIA Regulations?").

for the financial services industry (*e.g.*, the Financial Services–Information Sharing and Analysis Center (FS-ISAC) and the Financial Services Sector Coordinating Council (FSSCC)). These industry groups were created for the purpose of actively sharing cyber threat/cyberattack information and strengthening resilience among financial institutions and in collaboration with government entities have functioned effectively for over two decades. To leverage the benefits provided by these entities, CISA should clarify how its expected role and responsibilities differ from these organizations, and detail how it will work with those organizations in real time to provide mutual support and engage in information sharing.

The guidelines also should serve to quickly escalate, inform, and assist impacted firms to help thwart and manage the incident and should dictate how CISA will circulate its findings. For example, the guidelines could require CISA to anonymize, aggregate, and immediately circulate cyber incident information to peers of the victim(s) within a set number of hours following receipt. Ensuring a concrete, real time response to cyber incidents would provide value to impacted firms to offset the excessive burdens they face by complying with expedited filing requirements. Without some established course of immediate action to help publicize or combat the cyber incident, it would make no difference whether CISA receives the information two hours after a firm reasonably believes that a cyber incident has occurred or two weeks after a cyber incident concludes.[21]

3. Appropriately Calibrate the Content and Scope of Required Filings

CISA proposes to require covered entities to provide detailed information on several items in their initial CIRCIA Reports and subsequent updates.[22] Among other things, a covered entity would need to provide in its cyber incident reports both (1) its "assessment of the effectiveness of response efforts in mitigating and responding to the covered cyber incident;"[23] and (2) "a timeline of compromised system communications with other systems."[24] In addition, CISA proposes that the entire entity (*e.g.*, the corporation or organization) serve as the covered entity for CIRCIA reporting purposes and be required to report on any cyber incidents and ransomware payments.[25]

---

[21] CISA also should conduct post-incident evaluations to ensure that the timeliness of the information is not wasted. For example, it should monitor how efficient it has been in timely circulating cyber incident updates to critical infrastructure sectors and how effective it has been in providing impacted covered entities with immediate cyber incident assistance.

[22] *See* proposed Sections 226.7 through 226.11.

[23] *See* proposed Section 226.8(i)(2).

[24] *See* proposed Section 226.8(a)(3)(iv).

[25] *See* proposal at 23684.

On both the required content and the scope of required reporting, we endorse the comments submitted by the FSSCC.[26] Specifically, the FSSCC contends that reporting on the effectiveness of a covered entity's mitigation responses is unnecessary and subjective. It also asserts that a timeline of compromised system communications with other systems is unlikely to be available within CISA's initial 72-hour cyber incident reporting window and would require constant updating to ensure it is complete. Consistent with the FSSCC's comments, we recommend that CISA refine its disclosure requirements to ensure that each piece of requested information is necessary and will help the impacted firm and other firms within its sector combat cyber threats, and that the benefits of its use substantiate the costs it would impose to produce.

On the scope of a "covered entity," the FSSCC raises concerns that large, global entities might have numerous foreign subsidiaries, each subject to their own cyber incident reporting under the related entity's relevant foreign regulator. It expects that foreign regulators might in turn request similar information about U.S.-domiciled affiliates, potentially causing international jurisdictional struggles and making reporting more burdensome. We therefore recommend that CISA narrow the scope of what it deems to be a covered entity to exclude foreign subsidiaries from its purview.[27]

4. Require Third-Party Reporting for Substantial Cyber Incidents Facilitated Through Cloud Service Providers, Managed Service Providers, and Third-Party Data Hosting Providers

As proposed, covered entities would be required to file and would be responsible for filing cyber incident reports for each substantial cyber incident that occurs. These would include any cyber incident that leads to any of the following:

---

[26] *See* FSSCC Response to CISA's CIRCIA Notice of Proposed Rulemaking from Debbie Guild, PNC Financial Services, FSSCC Chair, Financial Services Sector Coordinating Council, dated July 3, 2024 ("FSSCC Letter"), *available at* https://www.regulations.gov/comment/CISA-2022-0010-0326. ICI participates in the FSSCC and generally agrees with each of the points in the FSSCC letter. The FSSCC was created in 2002 by financial institutions to work collaboratively with key government agencies while coordinating critical infrastructure and homeland security activities within the financial services industry. It is an industry-led non-profit organization with a mission to bring together members from financial services, trade associations, and other industry leaders to assist the sector's response to natural disasters, threats from terrorists, and cybersecurity issues of all types. For more information about the FSSCC, see https://fsscc.org/about-fsscc-13/.

[27] We further note that covered entities must file CIRCIA Reports to CISA through the web-based CIRCIA Incident Reporting Form that will be available, but that has not been posted yet, on CISA's website. Although a similar cyber incident reporting mechanism currently is available on CISA's website, it is not clear whether this is the actual CIRCIA Incident Reporting Form that will be used upon adoption of the final rules. Without confirming the actual format of these filings, the use of the CIRCIA Incident Reporting Form could raise additional issues. CISA should consider potentially allowing covered entities and others to comment on the format of the reports once a draft version is available.

> (A) a substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
>
> (B) a serious impact on the safety and resiliency of a covered entity's operations systems and processes; or
>
> (C) a disruption of a covered entity's ability to engage in business or industrial operations or deliver goods or services.

CISA would require covered entities to report these events regardless of cause, including but not limited to, those "caused by a compromise of a [cloud service provider], managed service provider or other third-party data host provider, a supply chain compromise, a denial-of-service attack, a ransomware attack, or exploitation of a zero-day vulnerability."[28] CISA also would require covered entities to report on cyber incidents involving unauthorized access through a cloud service provider, managed service provider, another third-party data hosting provider, or by a supply chain compromise.[29] CISA proposes these requirements to avoid the creation of a "blind spot" where "the covered entity experiences a substantial cyber incident but escapes required reporting based on the manner in which the incident was initiated or perpetrated" (*e.g.*, through a third party's website).[30]

When a single incident impacts multiple unaffiliated covered entities, each covered entity that experiences a substantial cyber incident must submit a CIRCIA Report to CISA.[31] In these cases, a third party may file the CIRCIA Report on the covered entity's behalf,[32] and the third party may submit a single report on behalf of multiple covered entities "if the circumstances leading to the reporting requirement for the various covered entities is similar enough to be reported collectively."[33] For example, if a single cyber incident perpetrated against a cloud service provider, managed service provider, or other third-party service provider impacts a number of the service provider's customers in a similar fashion and those customers are covered entities, the service provider *may* submit a single report.[34]

We generally agree that a covered entity should ensure that at least one CIRCIA Report is filed when it experiences a substantial cyber incident, regardless of cause. Imposing this responsibility

---

[28] *See* proposal at 23665-66.

[29] *Id*. at 23665.

[30] *Id*. at 23666.

[31] *Id.* at 23707.

[32] *Id.* at 23706-07. *See also* proposed Section 226.12 (setting forth requirements for third parties to file on behalf of covered entities).

[33] *See* proposal at 23729.

[34] *Id.*

on covered entities would eliminate the "blind spot" issue that CISA was concerned with when it proposed requiring covered entities to file.

We urge CISA, however, to *require* a cloud service provider, managed service provider, or other third-party data hosting provider to file the actual CIRCIA Report on behalf of the covered entity when that cyber incident arises from a compromise at the third party.[35] The third-party data hosting provider 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 the extent of the issue.

To the extent that a cyber incident facilitated by a third-party data hosting provider impacts multiple covered entities, requiring the third party to file the CIRCIA Report also might make more efficient and effective the filing and review of CIRCIA Reports filed, as the third party could make, and CISA could receive, one filing covering the single incident. For example, if a cloud service provider (*e.g.*, Amazon or Microsoft) or an exchange (*e.g.*, the New York Stock Exchange) experiences a cyberattack or data breach, then hundreds or even thousands of impacted companies might file reports about the incident. Requiring the entity suffering the breach in the first instance to instead file the CIRCIA Reports would result in one consolidated filing and reduce, or even eliminate, filing of duplicative information, which could free up resources and enable CISA to pursue its mission more effectively.[36]

If CISA does not require third-party data hosting providers to file the CIRCIA Reports in these situations, at the very least, it should demonstrate that the cost of data collected from multiple sources is outweighed by the benefit. In making this determination, it could conduct a redundancy check to determine how much information from the multiple reports it receives on a single incident is duplicative information. Doing so would allow it to assess the efficiency of its proposed multiple reports requirement.

5. Ensure the Confidential Nature of Reports

Consistent with CIRCIA, CISA proposes to share information from CIRCIA Reports with appropriate SRMAs and federal agencies and will receive other federal agencies' cyber incident reports.[37] In addition, CISA must publish quarterly reports that are publicly available that describe aggregated, anonymized observations, findings, and recommendations.[38] It also may provide appropriate entities timely, actionable, and anonymized reports of cyber incident

[35] We recognize that CISA may not have authority to require certain third parties to comply with these requirements, but CISA could and should impose these requirements at the very least on third-party data hosting providers that are themselves "covered entities."

[36] Of course, third-party reporting also would depend on the third-party data hosting provider's ability to meet the requirements for third-party reporting procedures and requirements (*e.g.*, requiring a covered entity to give it authorization to report on its behalf and having the ability to provide all of the information that the covered entity customer would have had to submit on its own). *See* proposed Section 226.12.

[37] *See* 6 U.S.C. 681a(a)(10) and (b) and 6 U.S.C. 681g(a)(1). *See also* proposal at 23654.

[38] *See* 6 U.S.C. 681a(a)(8). *See also* proposal at 23654.

campaigns and trends, along with contextual information.[39] Outside of those exceptions, CISA generally will keep information from CIRCIA Reports confidential.[40]

We wholeheartedly agree that CISA should not make CIRCIA Reports and information within them public. Detailed information, such as a description of the cyber incident, technical details of networks, devices, information systems, or a description of exploited vulnerabilities, would provide a roadmap for bad actors to breach a covered entity's network or system. Other information, such as a description of the type of incident, the timeline of compromised system communications, and indicators of compromise might quickly become stale and need to be constantly updated.[41]

To ensure that the information from CIRCIA Reports remains confidential, CISA should leverage industry best practices as a resource for effective safeguarding policies and procedures. This would include implementing active controls to ensure that any received information is used only for the specific purposes set forth in the regulation.

For its public reports, this should include anonymizing and aggregating information and removing references to firms (especially the identity of the victims of reported cyber incidents).

In addition, to protect against cybersecurity breaches at their own agencies,[42] CISA and the government agencies with whom it shares CIRCIA Reports and other cyber incident reports must continue to employ controls and cybersecurity testing to include, 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, and data security will give each of the critical infrastructure sectors more confidence and trust in CISA, which in turn may lead covered entities to provide CISA with more and better data. Absent any of these protections, firms likely will

---

[39] *See* 6 U.S.C. 681a(a)(3).

[40] *See* proposed Section 226.18 (describing how CISA will treat information from CIRCIA Reports and setting forth restrictions on its use).

[41] CISA's approach significantly and, in a positive manner, differs from provisions in the SEC IA/IC Proposal that would adversely affect SEC Registrants through required public disclosure of "significant cybersecurity incidents." We continue to oppose the SEC's proposed requirements that would force SEC Registrants to publicly disclose any significant cybersecurity incident that has occurred over a fund's last two fiscal years. The SEC explains that this disclosure is intended to "provide investors a short history of cybersecurity incidents affecting the fund while not overburdening the fund with a longer disclosure period." SEC IA/IC Proposal at 13541. In addition, the SEC would require SEC Registrants to report to the SEC significant cybersecurity incidents through forms, parts of which would be publicly available. As discussed in detail in ICI's comment letters on the SEC IA/IC Proposal, ICI strongly opposes the SEC's plans to require SEC Registrants to publicly disclose this cybersecurity information. *See* April 2022 ICI letter at 26-32.

[42] *See*, *e.g.*, Letter from Susan M. Olson, General Counsel, ICI, to Vanessa Countryman, Secretary, SEC, dated June 12, 2023 (highlighting recent cybersecurity breaches and concerns at the SEC), *available at* https://www.sec.gov/comments/s7-04-22/s70422-205459-413122.pdf.

provide no more than the required information and will be reluctant to provide any enhanced intelligence, which will deprive CISA of important support from the critical infrastructure sector firms it hopes to help.

* * * * *

ICI and its members appreciate the opportunity to comment on the proposal. If you have any questions or require any further information, please contact Ken Fang, Associate General Counsel, at 202-371-5430 or kenneth.fang@ici.org or Peter Poulos, Senior Director – Information Security, at 202-326-8302 or peter.poulos@ici.org.

Sincerely,

/s/ Kenneth C. Fang

Kenneth C. Fang
Associate General Counsel