June 28, 2024

Submitted via CISA Comments Portal

Director Jen Easterly
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Re: Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Reporting Requirements

Dear Director Easterly,

The American Bankers Association (the "ABA"),[1] Bank Policy Institute (the "BPI"),[2] Institute of International Bankers (the "IIB"),[3] and the Securities Industry and Financial Markets Association ("SIFMA")[4] (together, "the Associations") appreciate the opportunity to comment on the Cybersecurity & Infrastructure Security Agency's ("CISA" or the "Agency") rule proposal on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the "Proposal" or "Proposed Rule") on behalf of the financial services industry.

[1] The American Bankers Association is the voice of the nation's $24 trillion banking industry, which is composed of small, regional, and large banks that together employ approximately 2.1 million people, safeguard $19 trillion in deposits, and extend $12.4 trillion in loans.

[2] The Bank Policy Institute is a nonpartisan public policy, research, and advocacy group that represents universal banks, regional banks, and the major foreign banks doing business in the United States. The Institute produces academic research and analysis on regulatory and monetary policy topics, analyzes and comments on proposed regulations, and represents the financial services industry with respect to cybersecurity, fraud, and other information security issues. Business, Innovation, Technology and Security ("BITS"), BPI's technology policy division, provides an executive-level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud, and improve cybersecurity and risk management practices for the financial sector.

[3] The IIB represents the U.S. operations of internationally headquartered financial institutions from more than 35 countries around the world. The membership consists principally of international banks that operate branches, agencies, bank subsidiaries, and broker-dealer subsidiaries in the United States. The IIB works to ensure a level playing field for these institutions, which are an important source of credit for U.S. borrowers and comprise the majority of U.S. primary dealers.

[4] SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation, and business policy affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry-coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association ("GFMA").

The Associations recognize the benefits of sharing threat intelligence and incident information that will enable CISA to provide valuable tools and information to help defend the nation's critical infrastructure. The Associations appreciate CISA's objective to introduce clearly defined reporting requirements that will support trend analysis, vulnerability identification, provision of early warnings, and other key national security purposes.

However, the Proposal extends beyond the authorities granted to it under the statute and departs substantially from what Congress intended when it enacted CIRCIA. At that time, Congress was careful to note that CIRCIA sought to strike "a balance between getting information quickly and letting victims respond to an attack without imposing burdensome requirements."[5] Congress also reiterated that CIRCIA should be implemented "in a way that accounts for the practical needs of industry."[6] The Proposed Rule falls short of these critical considerations.

The Proposal itself requires reporting of more detailed and expansive data elements than observed in any of the current cyber regulatory reporting requirements, thereby prioritizing routine government reporting over more critical and impactful response and remediation work and potentially increasing operational risks. The proposed reporting requirements essentially mean that Congress's intention to create a "substantially similar" exception for reporting to other regulators was simply ignored. Congress clearly envisioned more limited reporting given that Congress believes there would be some exempted reporting due to existing regulations. In addition, provisions in the proposed ***substantial cyber incident*** definition create an unnecessarily low threshold for reporting, which will likely cause a flood of reports on low-risk incidents that will provide limited value to the government but will be a great cost to the reporting entities. Providing the requested information will divert attention from incident response teams during the most consequential phase of an incident. The Proposed Rule will, in its current form, also add overly burdensome obligations to an already sizeable incident reporting compliance apparatus.[7]

---

[5] Press Release, U.S. Sen. Homeland Sec. Comm., Peters & Portman Landmark Provision Requiring Critical Infrastructure to Report Cyber-Attacks Signed into Law as Part of the Funding Bill (Mar. 15, 2022), https://www.hsgac.senate.gov/media/dems/peters-and-portman-landmark-provision-requiring-critical-infrastructure-to-report-cyber-attacks-signed-into-law-as-part-of-funding-bill/.

[6] Press Release, U.S. H. Comm. on Homeland Sec., Clarke, Thompson, Katko, Garbarino Introduce Bipartisan Cyber Incident Reporting Legislation (Oct. 1, 2021), https://democrats-homeland.house.gov/news/legislation/clarke-thompson-katko-garbarino-introduce-bipartisan-cyber-incident-reporting-legislation-.

[7] The Associations' members already, or will soon be required to, comply with a number of cyber incident reporting obligations on the federal, state, and international levels. *See, e.g.*, 12 CFR § 53.3; 12 CFR § 225; 12 CFR § 304 [hereinafter, collectively, the US Interagency Cybersecurity Notification Requirement]; 17 CFR § 229.106; 23 NYCRR § 500 [hereinafter NYDFS Part 500]; EU Regulation 2022/2554 [hereinafter Digital Operation Resilience Act ("DORA")]; U.S. Dep't Hous. & Urb. Dev., Mortgagee Letter 2024-10 (May 23, 2024). There are also a number of pending rules from the Securities and Exchange Commission ("SEC") that would require cybersecurity incident reporting, including the proposed Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities

There are areas where CISA can enhance the Proposed Rule to allow for reporting requirements that support CISA's stated goals without creating overly burdensome reporting obligations during the critical early stages of incident response. As described further below, we respectfully offer the following recommendations for further revision.

- Refine the applicability of the Proposed Rule and the scope of reportable incidents to focus on substantial incidents that impact critical services and harmonize with existing regulations.

- Refine and limit the proposed reporting requirements to information directly related to an actionable purpose, such as detecting signs of a widespread vulnerability, so CISA can provide early alerts to critical infrastructure sectors. Narrowing reporting requirements in this way would be consistent with Congress's intent that some existing reporting requirements be captured by CIRCIA's "substantially similar" exception. CISA should also ensure that covered entities are able to exercise the substantially similar exception by publishing guidance on data sharing agreements.[8]

- Clarify and reduce the supplemental reporting requirements applicable to covered entities.

- Reduce the recordkeeping burden for incident information.

We hope that this feedback will help CISA refine the Proposed Rule's reporting requirements in a way that provides critical infrastructure entities with timely and actionable information that will make a meaningful difference in a coordinated cyber incident response.

Discussion

I. Refine Applicability of the Proposed Rule and Definition of *Substantial Cyber Incident* to Focus on Substantial Incidents Impacting Critical Services.

As drafted, the Proposed Rule will cover incidents that fall well under CIRCIA's desired threshold of *substantial* incidents for two reasons: first, the Proposed Rule applies to both the

Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, Release No. 34–97142, 88 Fed. Reg. 20212 (proposed Apr. 5, 2023) [hereinafter Rule 10 Proposal].

[8] U.S. S. Comm. on Homeland Sec. and Gov't Affs., Cyber Incident Reporting for Critical Infrastructure Act, at 1 (Dec. 17, 2021), https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Overview%20of%20Cyber%20Incident%20Reporting%20Legislation.pdf (saying CIRCIA "exempts entities that already have to report to another Federal agency from also having to report to CISA.").

critical aspects of a business and the non-critical aspects of a business; and second, the definitions for "substantial cyber incident" are overly broad.

a. The scope of reportable incidents should only cover incidents impacting critical services provided by U.S.-based entities within critical infrastructure sectors.

The scope of reportable incidents should be limited to those likely to result in substantial harm to critical infrastructure services. However, the Proposed Rule will apply to all incidents impacting covered entities in critical infrastructure, without distinguishing between incidents impacting critical versus non-critical services at the entity.[9] For example, an incident solely affecting a covered entity's non-critical marketing arm would be a reportable incident, even if it did not present a significant risk of harm to critical infrastructure.

The Proposed Rule is not clear about how covered entities should view their reporting obligations with respect to incidents at a covered entity's subsidiary or affiliate where the subsidiary or affiliate does not operate in a critical infrastructure sector and as such is not a covered entity itself. For example, there may be instances where a subsidiary or affiliate provides certain services to the covered entity that are unrelated to critical infrastructure (e.g., marketing or internal employee information). Given the breadth of potential covered entities and reportable incidents, the Associations urge CISA to narrow the Proposed Rule's applicability and limit the reporting of substantial cyber incidents and ransomware payments to the covered entity itself, rather than any of the covered entity's non-covered affiliates.

The Proposed Rule also does not address how a covered entity would apply the reporting analysis if its subsidiary or affiliate operating wholly outside of the United States experiences an incident and the impact of the incident occurs wholly outside of the United States. This affects a significant number of domestic covered entities with multijurisdictional operations and the U.S. operations of foreign banks. Given the breadth of potential covered entities and reportable incidents, the Associations urge CISA to narrow the Proposed Rule's applicability and limit the reporting of (i) substantial cyber incidents and (ii) ransomware payments to domestic covered entities only.

The Proposed Rule moreover does not limit reporting obligations to incidents affecting the critical infrastructure sectors listed in § 226.2(b). For example, an entity that triggers a sector-based criterion under § 226.2(b) due to its ownership of another entity may also have unrelated operations or activities that are wholly outside the scope of § 226.2.

The definition of substantial cyber incident should be limited to cyber incidents that affect the entity's critical infrastructure sector operations. For this purpose, critical infrastructure

[9] Proposed Rule § 226.1. Conversely, certain existing incident reporting obligations for critical infrastructure sectors are limited to critical services or lines of business. *See, e.g.*, U.S. Interagency Computer-Security Incident Notification Requirement, 86 Fed. Reg. 66424, at 66430 (explaining that the banking agencies intend the definition of "notification incident" to align with an entity's "core business lines" and "critical operations").

sector operations would be limited to operations that trigger one or more sector-based criteria in § 226.2(b) of the rule.

In light of the forgoing, the Associations recommend that CISA revise § 226.2 of the Proposed Rule to read:

> "This part applies to *the critical services, processes, or systems* of a~~n~~ domestic entity in a critical infrastructure sector that either …"

Further to the above, the Associations recommend that § 226.1 of the Proposed Rule be revised to read as:

> "(6) The term 'substantial cyber incident' does not include:
>
> (…)
>
> *(iv) Any event that does not affect the covered entity's operations that trigger one or more sector-based criteria in § 226.2(b); or*
>
> *(v) Any event that solely affects a non-U.S. covered entity's non-U.S. operations.*"

b. The Proposal's "substantial cyber incident" definition should have a higher threshold.

In addition to narrowing the reporting obligations by focusing on applicability, the Associations believe that refining the definitions would better align the Proposed Rule with the aims of CIRCIA. The Associations urge CISA to revise its proposed "substantial cyber incident" definition to require impact to a "critical" portion of a covered entity's business or operations.

i. A "substantial cyber incident" should require impact to a critical portion of a covered entity's business.

The Cyber Incident Reporting Council ("CIRC") Report recommended a more uniform definition and threshold for reportable cyber incidents.[10] However, rather than adopting the CIRC's recommendations, CISA's proposed "substantial cyber incident" definition adds another broad term with a reporting threshold well below many other existing requirements.

First, the Proposed Rule's definition of "substantial cyber incident" is ambiguous as to the meaning of the terms "substantial" in subsection (1) and "serious" in subsection (2) of its

[10] Department of Homeland Security, Harmonization of Cyber Incident Reporting to the Federal Government (Sept. 19, 2023), https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf, at Appendix F [hereinafter CIRC Report].

definition.[11] CISA provides that the Proposed Rule intentionally does not define the terms "substantial" or "serious," and instead provides explanatory guidance that a substantial cyber incident is one that accounts for a variety of factors that consider the type, volume, impact, and duration of the loss.[12] Left to interpret the intended meaning of and distinction between the terms, we know from experience that entities tend to over-report, fearing subsequent second-guessing by authorities. For example, in drafting the final rules on cybersecurity risk management, strategy, governance, and incident disclosure for issuers, the SEC explained that it did not anticipate many incident reports under the rules, given that most incidents would likely not meet the rules' materiality threshold and the definition in law.[13] But in practice, since the rules went into effect on December 18, 2023, covered entities have consistently reported incidents that objectively fall well below the threshold, forcing the SEC to clarify that there is another mechanism by which to disclose incidents.[14] CISA's Proposed Rule will likely lead to the same result, with covered entities proactively reporting incidents not meeting the threshold for a covered cyber incident. This will not necessarily alleviate the burden of determining whether certain systems, networks, or technologies are critical and will instead create a different burden of compiling the information required by a Covered Incident Report, even where not necessary.[15]

Second, under CIRCIA, CISA is required to "make efforts to harmonize the timing and contents of any [reports] to the maximum extent practicable."[16] Many covered entities subject to the Proposed Rule comply with numerous cybersecurity reporting obligations. For financial

[11] Proposed Rule § 226.1.

[12] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644, at 23662 [hereinafter Proposing Release].

[13] SEC Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 17 C.F.R. Parts 229, 232, 239, 240, and 249, at 140 ("We expect that the overwhelming majority of registrants will not experience a material breach and will not need to disclose cybersecurity incidents and incur the ongoing associated costs.").

[14] *Form 8-K, Item 1.05—Historical Filings*, DEBEVOISE & PLIMPTON LLP (May 10, 2024), https://www.debevoisedatablog.com/wp-content/uploads/sites/2/2024/05/8-K-Item-1-05-%E2%80%93-Material-Cybersecurity-Incidents-Tracker-5.10.pdf (last visited May 24, 2024); Erik Gerding, *Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents*, SEC. EXCH. COMM. (May 21, 2024), https://www.sec.gov/news/statement/gerding-cybersecurity-incidents-05212024 (indicating that companies are overreporting incidents where they have either (i) not yet made a materiality determination or (ii) determined such incidents to be immaterial).

[15] *See* Proposing Release, at 23665.

[16] Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 116th Cong. (2022), § 2242(C)(7)(B) [hereinafter CIRCIA]; *see also Cyber Regulatory Harmonization: Hearing Before the S. Comm. on Homeland Sec. & Gov't Affs.,* 118th Cong. (2024) (statement of Gary Peters, Chairman, S. Comm. on Homeland Sec. & Gov't Affs.), https://www.hsgac.senate.gov/wp-content/uploads/Opening-Statement-Peters-2024-06-05.pdf ("harmonizing these guidelines will make our government more efficient, help businesses compete on the global stage, and ensure we're addressing cybersecurity threats in the most effective way").

services entities, those promulgated by the Office of the Comptroller of Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Securities and Exchange Commission, the U.S. Department of Housing and Urban Development, and the Commodity Futures Trading Commission all require reporting of incidents falling under a heightened standard of harm to the organization or its systems or data.[17] Beyond financial services, other sectors' incident reporting obligations have heightened thresholds.[18] By implementing a heightened reporting standard, CISA will better allow covered entities to satisfy multiple reporting obligations concurrently.

Third, as written, prongs (3) and (4) of the definition of "substantial cyber incident" do not provide an impact threshold, and would therefore capture a broad range of incidents that fall below CIRCIA's intended scope. For example, under prong (3), a "disruption of a covered entity's ability to engage in business or industrial operations" would include de minimis operational outages to non-critical services. Under prong (4), the Proposed Rule sets no impact threshold for incidents occurring at a third-party or supply chain provider that impacts a covered entity's operations, and the reporting of *any* unauthorized access facilitated through or caused by the compromise of a cloud service provider, managed service provider, or other third party will overwhelm CISA with reports on incidents that have immaterial impacts on the covered entity and fall below CIRCIA's intended "substantial" threshold. Other financial authorities have intentionally limited the scope of covered information and systems to avoid overreporting on insignificant incidents[19] and CISA has authority to do the same under CIRCIA, which merely set

[17] *See, e.g.*, US Interagency Computer-Security Incident Notification Requirement ("[A] notification incident is a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade …"); NYDFS Part 500 (a cybersecurity incident is defined, in part, as a cybersecurity event that "has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity"); U.S. Dep't of Housing & Urban Dev., Significant Cybersecurity Incident (Cyber Incident) Reporting Requirements, Mortgagee Letter 2024-10 (2024) (defining a "significant cybersecurity incident" as "an event that actually or potentially jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies and has the potential to directly or indirectly impact the FHA-approved mortgagee's ability to meet its obligations under applicable FHA program requirements"); CFTC System Safeguards for Derivatives Clearing Organizations, 17 C.F.R. § 39 (2024) ("A derivatives clearing organization shall notify staff… promptly of … any hardware or software malfunction, security incident, or targeted threat that materially impairs, or creates a significant likelihood of material impairment, of automated system operation, reliability, security, or capacity.").

[18] *See generally* CIRC Report.

[19] *See, e.g.*, U.S. Interagency Computer-Security Incident Notification Requirement, §53.2(b)(7) (scoping a notification incident to one that has or is reasonably likely to "materially disrupt[] or degrade[]" an organization's operations or business lines, the failure of which "would pose a threat to the financial stability of the United States"); NYDFS Part 500, § 500.1(g) ("Cybersecurity incident means a cybersecurity event that…has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity.").

minimum considerations for determining when a covered cyber incident occurs.[20] As such, CISA has the ability to require higher thresholds for covered cyber incidents and should thus set impact thresholds under each prong.[21]

Further, the burden on covered entities under prong (4), as written, will exacerbate concerns discussed below at Section III.c around the difficulties in obtaining sufficient reporting information from third parties and duplicative reporting from both third-party providers and users reporting the same incidents.

Overall, given the breadth of the proposed substantial cyber incident definition, the Associations believe CISA severely underestimates how many incident reports it would receive under the Proposed Rule. CISA estimates it would receive 15,812 incident reports through 2033.[22] Without heightened impact thresholds for this definition, CISA would be inundated with reports on immaterial incidents far exceeding that number, making it more difficult to separate the terabytes of "noise" from actionable threat information that could prevent further harm across critical infrastructure.

ii. A "substantial cyber incident" should be defined to require substantial impact to a critical portion of a covered entity's network or business.

As proposed, the "substantial cyber incident" definition is not limited to specific entity businesses or networks, and it therefore does not exclude incidents impacting non-critical portions of the covered entity's business or network. This is inconsistent with existing incident notification regulations that limit covered incidents to those involving critical aspects of the business or otherwise specify covered systems and information.[23] Similar to the lack of impact thresholds described above, the failure to limit substantial cyber incidents to those impacting critical business operations and services will likely provide CISA with large quantities of inconsequential information that offer little benefit to reduce cyber risk.

In light of the foregoing sections, the Associations recommend that the Proposed Rule's definition of "substantial cyber incident" be revised to read:[24]

---

[20] 6 U.S.C. § 681b(c)(2)(A).

[21] 6 U.S.C. § 681b(c)(2)(A) (requiring CISA to define covered cyber incidents that "at a minimum" require certain prerequisites).

[22] Proposing Release, at 23744.

[23] *See, e.g.*, NYDFS Part 500, § 500.1 (defining a cybersecurity incident as a cyber event that that "has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity").

[24] Proposing Release, at 23661.

(1) A substantial loss of confidentiality, integrity or availability of a *critical portion of a* covered entity's information system or network *required for the provision of products or services by that covered entity*;

(2) A ~~serious~~ *substantial* impact on the safety and resiliency of a *critical portion of a* covered entity's operational systems and processes *required for the provision of products or services by that covered entity*;

(3) A *substantial* disruption of a covered entity's ability to engage in *a critical portion of* business or industrial operations~~, or deliver goods or services~~ *required for the provision of products or services by that covered entity*;

(4) Loss due to unauthorized access *and interruption, disruption or destruction of* ~~to~~ *a critical portion of* a covered entity's information system or network *required for the provision of products or services by that covered entity*, or ~~any~~ *critical* 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.

The Associations encourage CISA to institute a two-year lookback period to revisit the above definitions to account for any unintended consequences. The Associations stress that our proposed definition serves to clarify the scope and materiality of the incidents to be reported. Further, the Associations believe that given the challenges outlined in greater detail in Section III.c., CISA should take this into account and place the burden on providing information to covered entities and directly reporting to CISA for incidents that occur wholly within the managed service provider or third-party data hosting provider.

II. Refine Reporting Requirements to Focus on Information Directly Related to an Actionable Purpose and Reasonably Available within the First 72 Hours of an Incident.

a. The Proposed Rule exceeds the actionable information CISA needs to protect critical infrastructure.

The Associations are concerned that the extensive and detailed reporting requirements in the Proposed Rule would undermine CISA's goal of "achieving a proper balance among the number of reports being submitted, the benefits resulting from their submission, and the costs to both the reporting entities and the government of the submission, analysis, and storage of those reports." By CISA's own admission, the elements required in the proposed Covered Cyber Incident Report exceed the statutory requirements in CIRCIA.[25] While a broad set of facts may

[25] *See* Proposing Release, at 23720–23721.

enhance CISA's understanding of the incident as a whole,[26] CISA should not require information beyond what CIRCIA mandates and that does not directly support CISA's mission to provide timely information to protect critical infrastructure. To do otherwise would place an unnecessary burden on covered entities.

The Associations acknowledge CISA's desire "to identify trends and track cyber threat activity."[27] However, the level of technical detail outlined in the Proposed Rule's reporting requirements exceeds that of all other existing government reporting requirements. For example, CISA's own Incident Reporting System, used by the TSA-regulated entities to report cyber incidents, requires only a "brief description of the incident" and some details about the timing, number of users impacted, how the incident was detected, and the systems and functions that were impacted.[28] The NERC reporting form requires only the attack vector, functional impact, and level of intrusion of the incident.[29] Similarly, the CIRC Report's Model Cybersecurity Form, which takes into account queries with respect to critical infrastructure operators, also requires significantly less information than does the Proposed Rule.[30] With that being the case, the Associations urge CISA to use similar data elements for CIRCIA reporting and avoid holding private entities to a higher set of requirements than federal agencies that may operate national critical infrastructure.

To further harmonize with CISA's stated objectives, the Associations request that CISA strike at least the following information requests in the Proposed Rule that go beyond statutory requirements and create more burden for covered entities than any benefit CISA can derive from this information.

- "A timeline of compromised system communications with other systems and a description of any unauthorized access, regardless of whether the covered cyber incident involved an attributed or unattributed cyber intrusion, and identification of any

[26] *See* Proposing Release, at 23721.

[27] Proposing Release, at 23649.

[28] CISA, *Incident Reporting System*, https://www.cisa.gov/forms/report; TSA, Security Directive Pipeline-2021-01B, Enhancing Pipeline Cybersecurity (May 29, 2022), https://www.tsa.gov/sites/default/files/sd_pipeline-2021-01b_05-29-2022.pdf.

[29] NERC, Cyber Security – Incident Report (Jan. 2019), https://www.nerc.com/pa/Stand/Project%20201802%20Modifications%20to%20CIP008%20Cyber%20Secur/CIP_Technical_Rationale_for_CIP-008_Final%20Ballot_Clean_01152019.pdf.

[30] CIRC Report; *see also* FIN. STABILITY BD., FORMAT FOR INCIDENT REPORTING EXCHANGE (FIRE): A POSSIBLE WAY FORWARD 5–6 (2023) (noting that the Foreign Stability Board's common format for incident reporting exchange ("FIRE"), which aims to reduce operational challenges for financial institutions and enhance information sharing among regulators, offers "a single, but flexible, set of data fields that could satisfy the reporting needs of multiple [regulatory] stakeholders").

informational impacts or information compromise and any network location where activity was observed."[31]

i. This information often requires forensic analysis of the incident and a review of all impacted systems and data. These reviews can take weeks or even months to complete and may include highly sensitive information about a covered entity's network. The Associations believe that this level of detail is not necessary for CISA to protect critical infrastructure.[32]

- "A description of any vulnerabilities exploited, including, but not limited to, the specific products or technologies and versions of the products or technologies in which the vulnerabilities were found."[33]

i. Vulnerabilities can impact numerous instances of a specific hardware or software product.[34] Additionally, information on vulnerabilities, and the products they impact, is freely available. Requiring response personnel to expend valuable time and resources compiling reports on these vulnerabilities would provide no new relevant information to CISA.

- "An assessment of the effectiveness of response efforts in mitigating and responding to the covered cyber incident."[35]

i. The Associations believe this information is subjective to the covered entity and will not provide actionable detail on the incident. Further, because information is only due if it exists, it may incentivize companies not to conduct and document such assessments, which will hinder the overall goal of improving response efforts. Additionally, these assessments are often not conducted right away and their results are not known until later stages of the incident response effort. This sets the stage for companies to file multiple supplemental reports. Finally, an assessment of a company's response to an incident is not directly germane to

[31] Proposed Rule §§ 226.8(a)(3)(iv), 226.8(a)(2).

[32] *See* CYBER SAFETY REVIEW BOARD, REVIEW OF THE SUMMER 2023 MICROSOFT EXCHANGE ONLINE INTRUSION 1-3, https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf (discussing the detailed timeline of Microsoft's investigation of an intrusion, which lasted several weeks).

[33] Proposed Rule § 226.8(c).

[34] *See* CYBER SAFETY REVIEW BOARD, REVIEW OF THE DECEMBER 2021 LOG4J EVENT 5-9, https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf (discussing the global scale of the Log4j vulnerability).

[35] Proposed Rule § 226.8(a)(4)(i)(2).

information about the actual causes of the incident or trends in the threat environment. As such, the Associations believe this information is unnecessarily burdensome and will not further CISA's objective to protect critical infrastructure.

- "For ransom payment reports, outcomes associated with making the ransom payment, including, but not limited to, whether any exfiltrated data was returned or a decryption capability was provided to the covered entity and, if so, whether the decryption capability was successfully used by the covered entity."[36]

    i. The Associations believe this information is highly sensitive to the covered entity and not necessary to CISA's objective to protect critical infrastructure. Furthermore, this information is, by its nature, not available during the first 72 hours, which would likely lead to companies filing multiple supplemental reports every 24 hours as they obtain more information.

Additionally, the Associations ask that CISA leverage the CIRC Report's Model Cybersecurity Form, or alternatively the Federal Incident Notification Guidelines to harmonize reporting requirements and facilitate the submission effort.

b. The Proposed Rule requires report details that for most incidents will not be available within the first 72 hours and is not consistent with other incident reporting requirements.

The Associations are concerned that the Proposed Rule creates an unduly burdensome reporting requirement that would divert key resources away from important work during the critical stages of a covered entity's incident response. The Associations are similarly concerned the Proposed Rule seeks information often not available within the first 72 hours of an incident, and sometimes never even in the later phases of the incident response effort. In addition, requiring extensive information early in the incident increases the risk of inadvertent reporting errors. We urge CISA to appreciate that any additional information CISA requires increases the cost of compliance, both monetarily and, perhaps more importantly, by taking critical incident responders away from incident remediation efforts to collate the detailed information required under the Proposed Rule.

The information required in the proposed §§ 226.8 and 226.9 is more appropriately gathered at the conclusion of an incident rather than over the course of an incident, and often takes weeks, or even months, to produce. For example, a "timeline of compromised system communications with other systems" and a "description of the type of incident and the tactics, techniques, and procedures used to perpetrate the covered cyber incident," as required by proposed §226.8(a)(3)(iv) and proposed §226.8(e), respectively, require a detailed forensic

[36] Proposed Rule § 226.9(1).

analysis of impacted systems, usually conducted after the initial incident is contained. And while the Proposed Rule requires entities to only submit information "to the extent such information is available and applicable,"[37] such an onerous list of reporting elements would require covered entities to submit numerous Supplemental Reports over the course of an incident to meet the reporting requirements and timelines outlined by the Proposed Rule.

In the event certain incident-related information is available during the first hours of an incident, compiling that information exclusively for compliance purposes would unnecessarily burden the personnel remediating the incident. CISA must appreciate the tremendous work each report will require of senior information security staff. This is a challenge because those individuals also lead incident response activities and, given the respective criticality of the services each covered entity provides, the incident response teams are focused on recovering those services critical to the security and well-being of the U.S.

Accordingly, to harmonize with other federal reporting requirements, and to lower the burden on response personnel during the critical early stages of an incident, the Associations request that CISA revise proposed § 226.8 such that it reads:

> "A covered entity must provide all the information identified in § 226.7 and the following information in a Covered Cyber Incident Report, to the extent such information has already been identified or ~~is available and applicable~~ determined as part of the entity's response to the covered cyber incident…"

We likewise propose that CISA make the analogous change to proposed § 226.9, such that it reads:

> "A covered entity must provide all the information identified in § 226.7 and the following information in a Ransom Payment Report, to the extent such information has already been identified or ~~is available and~~ ~~applicable~~ determined as part of the ransom payment..."

c. The Proposed Rule does not meet CIRCIA's mandate to create a substantially similar exception.

CISA has failed to meet its obligations to create a substantially similar exception, as mandated by CIRCIA.[38] CIRCIA states that where there is an agreement in place with another Federal Agency that satisfies the reporting requirements under CIRCIA, covered entities shall not have to submit reports to CIRCIA if they are required to submit a report to the other Federal

[37] Proposed Rule § 226.7.

[38] 6 U.S.C. § 681b(a)(5)(B).

Agency in a substantially similar time frame.[39] However, CISA has not yet established agreements with other Federal Agencies with reporting requirements, nor indicated which Federal Agencies it will establish agreements with, and has thus far not met its obligations as set forth in CIRCIA.

Congress would not have included this explicit language describing a substantially similar reporting exception in the statute if it did not intend that at least a portion of existing government reporting requirements be captured by the exception. In fact, Congress affirmatively stated this expectation by saying CIRCIA "exempts entities that already have to report to another Federal agency from also having to report to CISA."[40] This interpretation is consistent with CIRCIA's requirement that CISA harmonize reporting requirements "to the maximum extent practicable."[41] It also supports the view that Congress intended this exception to be construed more expansively than CISA suggests in the Proposed Rule when it states that other reporting requirements should include "functionally equivalent" information to CISA's proposed data elements to be considered substantially similar.[42]

CISA's expansion beyond all other reporting requirements is significant because it effectively negates the availability of CIRCIA's "substantially similar" exception.[43] For its own purposes though, CISA seems to adopt an expansive view of the exception in the Proposed Rule when exempting Federal agencies from CIRCIA's requirements. This is based on the understanding that agency reporting obligations under the Federal Information Security Modernization Act ("FISMA") are substantially similar to those CISA proposes for private sector reporting under CIRCIA.[44] Reporting under FISMA is dictated by Office of Management and Budget Guidance and requires that agencies report incidents to CISA in accordance with the

[39] *Id.*

[40] U.S. S. Comm. on Homeland Sec. & Gov't Affs., Cyber Incident Reporting for Critical Infrastructure Act, at 1 (Dec. 17, 2021), https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Overview%20of%20Cyber%20Incident%20Reporting%20Legislation.pdf.

[41] 6 U.S.C. § 681g(b).

[42] Proposing Release, at 23709.

[43] 6 U.S.C. § 681b(a)(5)(B).

[44] Proposing Release, at 23712.

Federal Incident Notification Guidelines.[45] Those guidelines, however, only require information on an incident's functional, information, and systems impact.[46]

To align with CIRCIA, the Associations request that CISA draft clear guidelines for how information will be shared via information sharing agreements, outline with which agencies the information will be shared, and ensure that the sharing agreements are enacted promptly in relation to the finalization of the Proposed Rule.

d. The Proposed Rule allows CISA to further modify required data fields beyond the regulation without any additional rulemaking.

The Proposed Rule states that CISA can require any information it would like to receive in the future by adding new requirements to the web-based form.[47] We ask CISA to strike the language in proposed §§ 226.8(j), 226.9(n), and 226.11(a)(4) given CIRCIA's requirement that the rule have "a *clear description* of the *specific required* contents of a report."[48] In addition, the unconstrained ability to add required information without additional rulemaking or articulating how said information advances CISA's mission would create undue operational burdens and uncertainty. CIRCIA's and the Proposed Rule's existing language is broad enough to adapt the report submission form to incident developments over time, and as such, provisions §§ 226.8(j), 226.9(n), and 226.11(a)(4) are unnecessary to meet CISA's stated objectives.

III. Clarify Reporting Obligations and Facilitate the Efficient Closure of the Reporting Process.

The Associations seek further clarity on (i) the triggers for when supplemental reporting is required; (ii) when a covered entity's reporting obligations conclude; and (iii) how a covered entity can comply with the Proposed Rule when a third party holds relevant information.

a. CISA should clarify triggers and the timeline for supplemental reporting to avoid burdensome overreporting.

Cybersecurity incidents often evolve quickly and the Associations understand that a financial institution's reporting obligations may apply before all facts required under the

[45] OFFICE OF MGMT. & BUDGET, M-24-04, FISCAL YEAR 2024 GUIDANCE ON FEDERAL INFORMATION SECURITY AND PRIVACY MANAGEMENT REQUIREMENTS 13 (2023); U.S. DEP'T OF HOMELAND SEC., US-CERT FEDERAL INCIDENT NOTIFICATION GUIDELINES, https://www.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf.

[46] U.S. DEP'T OF HOMELAND SEC., US-CERT FEDERAL INCIDENT NOTIFICATION GUIDELINES 2, https://www.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf.

[47] *See, e.g.*, Proposed Rule § 226.8(j).

[48] Proposing Release, at 23678.

Proposed Rule are available. Accordingly, the Associations appreciate that CISA's reporting form allows covered entities to provide that certain facts are "unknown at this time." The Proposed Rule provides that supplemental reports are required "promptly" when "substantial new or different information" becomes available[49] and CISA presently expects covered entities to submit a supplemental report if the initial report was "incomplete in some manner."[50] It is unclear whether covered entities need to provide a supplemental report each time a previously unanswered data field becomes known and what constitutes "different" versus "new" information. In early stages of an incident investigation, a supplemental report could, in theory, be required daily.

The Associations are concerned that financial institutions will be expected to make numerous supplemental reports over an extended incident lifecycle consuming finite incident response resources without adding information CISA needs to execute its mandate under CIRCIA. CISA estimates that supplemental reports will be filed in roughly half of the instances.[51] Given the breadth and detail of the proposed reporting elements—many of which are customarily unknown prior to the 72-hour reporting deadline—the Proposed Rule's supplemental reporting figures are likely to be required in virtually every incident. For example, if CISA maintains the requirement to report on effectiveness of response efforts, every incident will require a supplemental report. To remove this ambiguity and provide discretion to covered entities to prioritize incident response efforts, the Associations recommend adjusting the supplemental reporting requirement in proposed § 226.3(d) to read:

"Supplemental Reports must be ~~promptly~~ submitted by the covered entity if substantial new ~~or different~~ information becomes available, promptly upon cessation of critical response activities."

Regardless of the above revisions to the proposed § 226.3(d) and to avoid confusion, CISA should further clarify that covered entities be allowed to submit corrections via supplemental reports rather than using a separate form.

b. CISA should clarify when a covered entity can state that an investigation has concluded.

CISA indicates that an incident will be considered closed only when an entity has completed an investigation of the incident, gathered all "necessary" information, and

[49] Proposed Rule § 226.3(d).

[50] Proposing Release, at 23726.

[51] Proposing Release, at 23744 ("CISA assumes 25% of entities submitting Covered Cyber Incident Reports and Joint Covered Cyber Incident and Ransom Payment Reports for the low estimate, 50% for the primary estimate, and 75% for the high estimate [will be required to submit supplemental reports].").

documented "all relevant" aspects of the incident.[52] In light of the Proposed Rule's requirements, many covered entities, including our member financial institutions, will not be able to meet this standard in certain cases. In practice, for a variety of reasons (e.g., threat actors obfuscating their movement and actions), some reporting details proposed by CISA may never be confirmed, or minor, immaterial developments may come to light months later. This creates uncertainty surrounding incident closure and risks an overly lengthy reporting cycle. We propose that CISA add a mechanism by which a covered entity through its Supplemental Report (e.g., a check box) can conclude an incident by indicating the covered entity does not anticipate making any further updates nor does it anticipate discovering any substantial new information.

c. CISA should acknowledge that covered entities might be unable to obtain the required information from third parties.

Under the proposed § 226.1, a broad range of incidents arising at third parties will be in scope for reporting and will require significant information sharing and coordination between a covered entity and the third party beyond what typically occurs today. Because the covered entity will, in many instances, need to rely on the third party to provide the high degree of technical detail required by the Proposed Rule, and the covered entity retains the obligation to comply with the reporting requirements, further instruction is needed for how a covered entity can comply with its obligations where a third party is not cooperating with the covered entity's requests. The issue of downstream cooperation is further complicated by incidents where a covered entity will need to rely on service providers to service providers (i.e., fourth parties) for the technical detail required by the Proposed Rule, given that the covered entity may not have a direct relationship with the entity who experienced the incident. Despite its best efforts, it may not be possible for a covered entity to obtain all (or even most) information required by the Proposed Rule in a supply chain incident. Where certain of a covered entity's systems are managed by a critical service provider and a global cyber incident occurs for this service provider, by virtue of the number of affected entities during the incident, no individual entity will have direct access to the required information about the incident it needs to complete its Covered Cyber Incident Report, and the critical service provider will not readily be able to manage requests from all affected entities asking for information. Because of this, Covered Cyber Incident Report submissions for third-party incidents will almost certainly vary in terms of completeness and accuracy, with the potential for varying accounts of the same incident. Thus, service provider and third-party cooperation is essential to ensure the consistency and accuracy of information reported to CISA.

Given that CIRCIA already binds third parties to advise covered entities in their obligations under certain circumstances,[53] the Associations request that CISA extend obligations

[52] Proposing Release, at 23727.

[53] *See* Proposed Rule § 2242(d)(4), which states that "[a]ny third party used by a covered entity that knowingly makes a ransom payment on behalf of a covered entity impacted by a ransomware attack shall advise the impacted covered entity of the responsibilities of the impacted covered entity regarding reporting ransom payments under this

on service providers and third parties where covered entities would reasonably be expected to rely on service providers and third parties for information required by a Covered Cyber Incident Report. As such, the Associations propose the following with respect to third-party incident reporting:

- Provide a mechanism in the report template, and guidance for covered entities, that would allow covered entities to certify that they made reasonable best efforts to obtain the information needed from their service provider, and any other third or fourth party.

- Revise the Proposal to require service providers to cooperate with covered entities in their reporting obligations.[54]

IV. Clarify Protections and Exemptions for Shared Sensitive Information.

The Associations appreciate protections to maintain the confidentiality of CIRCIA reports and other submitted information, but request clarification on FOIA protection, arbitration, and how CISA will safeguard reported information.

a. CISA should clarify FOIA protections.

While the Proposed Rule notes that CIRCIA reports and responses are exempt from FOIA requests, it goes on to state that, in the event CISA receives a FOIA request, it "will apply all applicable exemptions from disclosure, consistent with 6 CFR part 5."[55] The FOIA exemption in the CIRCIA statute is clear, so adding this language is either redundant or creates uncertainty around whether an exemption will apply in all cases.[56] For clarity, we request that CISA strike the last sentence from proposed § 226.18(b)(2) to read:

---

section." Thus, where a covered entity requires information from service providers or third parties for other aspects of its incident response effort, it would be reasonable that CISA also require service providers or third parties to advise the impacted covered entity.

[54] Certain state privacy laws require service provider cooperation in the event of a data breach and provide useful language for consideration. *See, e.g.*, Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1305(2)(b); Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-579(2) (providing that processors "shall assist the controller" by "helping to meet the controller's obligations in relation … to the notification of a breach of [security]" and "providing information to the controller necessary to enable the controller to conduct and document any data protection assessments").

[55] Proposed Rule § 226.18(b)(2).

[56] 6 U.S.C. § 681(e)(b)(2) ("Reports describing covered cyber incidents or ransom payments submitted to the Agency in accordance with section 681b of this title … shall … be exempt from disclosure under [FOIA and all similar laws]"). Other regulations that provide for FOIA or equivalent exemptions in the context of cyber incident reports have equally strong language outlining the protections. For example, the NAIC Insurance Data Security

> CIRCIA Reports submitted pursuant to this part and responses provided to requests for information issued under § 226.14(c) are exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(3), and under any State, Local, or Tribal government freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records.

b. CISA should expand the protections for CIRCIA Reports to include arbitrations.

We support the proposed § 226.18(c)(2)(ii) that CIRCIA reports "may not be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof." Given the high number of arbitration matters related to cybersecurity and data privacy that financial institutions face, we request that CISA explicitly include arbitrations in this exemption in furtherance of CISA's goal of protecting the confidentiality of CIRCIA reports.

c. CISA should clarify technical and anonymizing protections for shared information.

CIRCIA reports and related data sharing will contain highly sensitive information, for which CISA will become the custodian. We agree with and support CISA's efforts to have "physical and cybersecurity measures in place to prevent illicit unauthorized access to the information CISA receives" pursuant to proposed § 226.18(b) and that those measures will adhere to the Federal Information Processing Standard Publication 199.[57] However, we request that CISA provide additional clarity as to what specific controls will be in place to protect information shared with CISA and information shared within DHS and with other agencies, such as the Department of Treasury.[58] For example, CISA should consider appointing an individual in charge of developing procedures for and overseeing the privacy and security of CIRCIA Reports, and creating a procedure for the investigation and reporting of misuse.[59] Additionally, CISA

Model Law, which has been adopted by 23 states, provides that documents, materials or other information provided in accordance with the law "shall not be subject to" state open records, freedom of information, sunshine or other appropriate laws. *See, e.g.*, Virginia Insurance Data Security Act, Va. Code Ann. § 38.2-628(a); Delaware Insurance Data Security Act, 18 Del. Code § 8608(a)(1).

[57] Proposing Release, at 23741.

[58] *See* EXEC. OFFICE OF THE PRESIDENT, NATIONAL SECURITY MEMORANDUM ON CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (2024), https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/ (discussing the Department of Treasury's role in cybersecurity and resilience coordination for financial institutions).

[59] *See* 6 C.F.R. § 29.6 for specifications for the Protected Critical Infrastructure Information (PCII) Program, which requires a Privacy Officer who oversees the privacy of information reported voluntarily under the PCII program.

should clarify whether information shared with other agencies will be anonymized, particularly where an agency is not a covered entity's sector risk management agency, and under what circumstances covered entities may be permitted to request anonymity. Finally, the Associations recommend that the Proposed Rule provide a mechanism for sharing incident-related information with private entities should CISA's own network be compromised.

V. Lessen the Recordkeeping Obligations and Provide Covered Entities with Flexibility and Discretion.

While the Associations understand the importance of incident recordkeeping, the Proposed Rule's obligations would be operationally onerous and costly. We recommend (i) decreasing the required recordkeeping timeframe and permitting less costly storage options, and (ii) narrowing the records retention scope.

a. CISA should shorten the recordkeeping period and provide flexibility for record storage.

CISA's estimated $700–$1,300 annual preservation cost range[60] significantly undercounts the expected actual costs considering the duration, manner, and volume of records captured by the Proposed Rule. For example, CISA's proposal requires covered entities to store incident records in their original format, in a "readily accessible" manner, with sufficient safeguards.[61] These requirements will in some cases preclude using secured archive or cold storage options, which would be less costly than hot or active storage options. They would also prevent covered entities from migrating data to a less costly, alternative format. The volume of retained data pursuant to the Proposed Rule could easily be measured in terabytes. The estimated base cost of storing two terabytes of covered incident data with Google Cloud Storage is $10,488 for 24 months of storage.[62] This estimate does not take into account pricing for data transfer, CPU processing cycle fees, or any other cost associated with such data storage.

Accordingly, we propose that CISA (i) shorten the recordkeeping period to one year to account for the operational burden and cost of holding voluminous forensics data for two years or (ii) permit covered entities to delete stored data in a phased approach, if, for example, CISA has made no request for any information about the incident within six months or one year of filing the incident report. Additionally, the Associations request that CISA remove the original format requirement under proposed § 226.13(d) and instead permit covered entities to store data in an archived format that is both more secure and less costly than active data hosting.

---

[60] Proposing Release, at 23746.

[61] Proposed Rule § 226.13(d)–(e).

[62] *Google Cloud Storage Pricing*, https://cloud.google.com/products/calculator.

b. CISA should reduce the volume of bulk forensic data storage requirements.

Certain recordkeeping requirements included in the Proposed Rule are overly burdensome, cover information that is not customarily stored for two years for the scope of incidents contemplated, and will not provide substantial value to CISA following a reportable incident. While requiring covered entities to retain relevant live memory captures, forensic images, and system information that *may* help identify exploited vulnerabilities[63] *might* provide CISA with relevant information in some cases, holding all of this data will be costly and create a disproportionate burden on covered entities not commensurate with the value CISA would receive. This will be particularly true in cases where the covered entity is already required to provide such information to CISA in a CIRCIA report, and the data is therefore already in CISA's possession.[64] Note that CISA itself recognizes the costs of maintaining such information.[65] Additionally, apart from the cost, certain large or particularly sensitive data would not ordinarily be stored for this period of time because it would increase an organization's attack surface; entities would instead retain a detailed report of the incident. CISA should revise the Proposed Rule to provide covered entities discretion to preserve the information an incident investigation determines valuable and proportionate to the covered entity's storage costs and security concerns.

VI. Enhance Flexibility for Responding to Requests for Information and Alleviate Concerns about Criminal Penalties.

a. CISA should provide greater flexibility for responding to requests for information.

The Associations appreciate the discretionary element to the required timeline for complying with a request for information ("RFI") but are concerned that RFIs sent pursuant to voluntarily reported submissions will produce a chilling effect on future voluntary submission. The Associations encourage CISA to provide greater flexibility for entities responding to such RFIs and to consider exercising discretion in limiting the ability to send RFIs in response to a voluntary submission. Under the Proposed Rule, RFIs cannot be appealed[66] and responses must

[63] Proposed Rule § 226.13(b)(1)(iv), (vii).

[64] *Compare* Proposed Rule § 226.13(b)(vii) (requiring retention of "[s]ystem information that may help identify exploited vulnerabilities, including but not limited to operating systems, version numbers, patch levels, and configuration settings"), *with* § 226.8(c) (requiring in CIRCIA reports "[a] description of any vulnerabilities exploited, including but not limited to the specific products or technologies and versions of the products or technologies in which the vulnerabilities were found").

[65] *See* Proposed Release, at 23732 (noting that "the costs for preserving data increase the longer the data must be retained" and expressing CISA's intent "to limit costs of compliance with CIRCIA where possible without sacrificing the ability to achieve the purposes of the regulation").

[66] Proposed Rule § 226.14(b)(2)(c)(5).

be made "in the manner and format, and by the deadline, specified by the Director."[67] The Proposed Rule, however, does not specify how much time the Director can give RFI recipients to comply. Nevertheless, failure to respond by the deadline set, or providing an inadequate response, which is not defined, can each immediately trigger the issuance of a subpoena.[68]

Given the complexity of many cyber incidents, the significant documentation and data required to respond, and potential time passed since the incident occurred, recipients may need significant or additional time to comply with the request. Additionally, the recipient may not have the information requested, including circumstances where the information is held by a third party, or the recipient may not believe it is a covered entity or that it experienced a qualifying reporting event.

We encourage CISA to affirmatively allow recipients to provide reasoning as to why they should not have to or need additional time to comply with the RFI, to ask follow-up questions about the basis for and scope of the RFI, and that such correspondence will not be deemed an "inadequate" response under proposed § 226.14(d)(1), rather than immediately issuing a subpoena.

b. CISA should issue statements clarifying intended use of criminal penalties.

CIRCIA and the Proposed Rule allow for criminal penalties under 18 U.S.C. § 1001, as discussed in the proposed § 226.20. This is a dramatic shift from CISA's approach to information collection to date. Consequently, covered entities and individuals tasked with filing reports to CISA will fear individual criminal liability under the Proposed Rule and will likely over-scrutinize any draft CIRCIA report or submission to a level that detracts from essential incident response efforts and delays information sharing to the detriment of CISA's goals. This includes CISOs, who may be driven away from leadership roles for fear of such criminal prosecution, adding to the potential disincentives created by the Proposed Rule. The Associations request that CISA issue clear statements explaining that the use of its authority to refer matters for criminal prosecution will be under extreme and rare circumstances.

***

CIRCIA represents a unique opportunity to enhance the analysis and assessment of emerging cyber threats. Congress entrusted CISA with developing an appropriately calibrated approach to implementing CIRCIA and bringing coherence to the highly fragmented cyber regulatory landscape. The Associations fully recognize the challenges associated with developing a single standard across 16 critical infrastructure sectors. Nevertheless, the extensive requirements in the Proposed Rule would not accomplish the coherence Congress envisioned but instead could increase operational risks by requiring front-line cyber personnel to spend more time on reporting requirements than critical security operations. The Associations are committed

[67] Proposed Rule § 226.14(d)(4).

[68] Proposed Rule § 226.14(d)(1).

to working with CISA to develop a balanced approach that achieves CIRCIA's primary goal to share actionable cyber threat information and improve critical infrastructure security, and recommend that CISA maintain an open dialogue with the critical infrastructure sectors regarding the Rule's effectiveness both before and after the Rule's finalization. If you have any questions, or would like to discuss these comments further, please reach out to John W. Carlson at jcarlson@aba.com, Heather Hogsett at heather.hogsett@BPI.com, Michelle Meertens at mmeertens@iib.org, and Melissa MacGregor at mmacgregor@sifma.org.

Respectfully submitted,

/s/ John W. Carlson
John W. Carlson
Senior Vice President, Cybersecurity Regulation and Resilience
American Bankers Association

/s/ Heather Hogsett
Heather Hogsett
Senior Vice President, Technology & Risk Strategy, BITS
Bank Policy Institute

/s/ Patrick Warren
Patrick Warren
Vice President, Regulatory Technology, BITS
Bank Policy Institute

/s/ Beth Zorc
Chief Executive Officer
Institute of International Bankers

/s/ Melissa MacGregor
Melissa MacGregor
Deputy General Counsel & Corporate Secretary
Securities Industry and Financial Markets Association

/s/ Thomas M. Wagner
Thomas M. Wagner
Managing Director, Financial Services Operations
Securities Industry and Financial Markets Association

cc: Erez Liebermann, Gabriel A. Kohan, HJ Brehmer, Stephanie Thomas
Debevoise & Plimpton LLP
Counsel to the Associations