July 2, 2024

Director Jen Easterly
Cybersecurity and Infrastructure Security Agency (CISA)
Department of Homeland Security
245 Murray Lane
Washington D.C. 20528-0380
(submitted electronically)

INSTITUTE OF INTERNATIONAL FINANCE

Re: Proposed Rule for Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (Docket No. CISA-2022-0010) (Proposed Rule or NPRM)

Dear Director Easterly,

The Institute of International Finance (IIF)[1] and its member firms welcome the opportunity to contribute to the work of the Cybersecurity and Infrastructure Security Agency (CISA) as it finalizes its rule on cyber incident reporting pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).[2] The proliferation of cyber incidents is one of the most critical economic and national security threats facing our country. As such, cybersecurity is a shared priority of the public and private sectors and is an essential means of maintaining confidence in the nation's critical infrastructure, of which financial services represent a key part.

The IIF recognizes the importance of CIRCIA's primary purpose to help preserve national security, economic security, and public health and safety in the face of an increasingly sophisticated threat landscape. The evolving threat landscape underscores the importance of threat intelligence and incident information sharing. The financial sector recognizes the significant benefits of sharing cyber incident and threat intelligence information and accordingly, has established entities such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Analysis and Resilience Center for Systemic Risk (ARC) to facilitate the voluntary sharing of sensitive cyber threat intelligence. There are also strategic initiatives, such as the Financial Services Sector Coordinating Council (FSSCC), another industry-led organization, which coordinates critical infrastructure and homeland security activities within the financial services industry and works closely with its government counterpart – the Financial and Banking Information Infrastructure Committee (FBIIC) – to enhance the overall resiliency of the financial sector.

As CISA acknowledges in the supplementary information to the Federal Register Notice, the Proposed Rule enters a diverse and increasingly crowded reporting landscape at the state, national, and international levels. As discussed in the DHS's report, "Harmonization of Cyber Incident

[1] The Institute of International Finance (IIF) is the global association of the financial industry, with about 400 members from more than 60 countries. The IIF provides its members with innovative research, unparalleled global advocacy, and access to leading industry events that leverage its influential network. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial, and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, professional services firms, exchanges, sovereign wealth funds, hedge funds, central banks, and development banks.

[2] DHS 2024. "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements" April 4, 2024.

Reporting to the Federal Government," there are 52 cyber incident reporting requirements either in effect or proposed across the federal government with 45 requirements currently in effect across 22 agencies.[3] The financial sector alone is already subject to multiple regulatory frameworks with varying reporting requirements,[4] including eight federal agencies that require cyber incident reporting,[5] as well as state-based requirements, such as those from the New York Department of Financial Services (NYDFS).[6] The growing number of state cybersecurity regulations and incident reporting rules pose a particular challenge for the insurance industry, as the U.S. insurance industry is regulated at the state level.

We commend the establishment of a Cyber Incident Reporting Council (CIRC) for coordinating, deconflicting, and harmonizing existing and future federal cyber incident reporting requirements. We also commend CISA for leveraging the Council's findings and efforts to improve cybersecurity and reduce reporting burdens by adopting common reporting standards.

In the IIF's response[7] to CISA's initial RFI on CIRCIA, we urged greater consistency with international cyber incident reporting requirements and terminology. We also requested that CISA focus on only the most material, and malicious, cyber incidents, to ensure that both covered entities and government authorities can prioritize those cyber incidents that need to be addressed quickly, in an anonymized, non-attributable manner. If properly scoped, the final rule could fortify collective cyber defenses in several key respects, particularly by enhancing visibility into the cyber threat environment, including potential supply chain disruptions that may impact multiple covered entities. The IIF proposes several additional recommendations to streamline and clarify the Proposed Rule, and to better align its reporting requirements with the operational realities of entities subject to those reporting requirements, while meeting the important objectives of CIRCIA.

Key Challenges and Recommendations

Adopt a more risk-based approach to cyber incident reporting by clarifying in the final rule the CIRCIA definition of a 'substantial cyber incident' as those having substantial impacts on critical services or processes. In developing CIRCIA, Congress's intent was to create a compulsory cyber incident notification program that imposes reporting obligations on covered entities, while not inundating CISA with incident data that is immaterial. In order for CISA and other relevant stakeholders to receive reports on the incidents most likely to be harmful to economic and national security interests, reporting should be focused on substantial cyber incidents with a reasonable likelihood of demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the

[3] DHS 2023. "Harmonization of Cyber Incident Reporting to the Federal Government," September 19, 2023.
[4] The varying reporting requirements within the U.S. are greatly compounded internationally, where the lack of coordination among regulators has resulted in fragmented reporting requirements that may require the firm to provide authorities with different data sets and/or granularity of information. The Financial Stability Board has highlighted significant overlap in cyber incident reporting requirements across G-20 jurisdictions and has put forward recommendations for authorities to explore opportunities for further convergence through the development of a common reporting format that can help enhance global cyber incident reporting practices, such as the FSB's Format for Incident Reporting Exchange (FIRE) project. DHS has similarly acknowledged the overlap in international reporting requirements, including in its report, "Comparative Assessment of the DHS Harmonization of Cyber Incident Reporting to the Federal Government Report and the Rules on Incident Reporting in the EU Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS 2 Directive)."
[5] Ibid.
[6] NYDFS 2023, "Part 500 Cybersecurity Regulations" November 1, 2023.
[7] IIF 2022 "IIF Response to US CISA request for information on Cyber Incident Reporting" Nov. 15, 2022

American people.[8] As such, we encourage CISA to couple in its definition of a covered incidents as those with substantial impacts on critical services or processes. A more risk-based definition based on CIRCIA will enhance economic and national security outcomes as well as promote proportionality and efficiencies for covered entities.

By extension, the IIF encourages CISA to include a materiality element to each prong of its definition for substantial cyber incident. Not doing so could lead to an overgeneralized interpretation of what is considered substantial and create a landscape where almost any cyber incident could be deemed reportable, whether or not the incident is likely to lead to material harm to the U.S. economy or national security situation.

For instance, the third prong, *Disruption of Ability To Engage in Business or Industrial Operations*, "would require a covered entity to report an incident that results in a disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services. The IIF recommends modifying the definition to, "A ***substantial*** disruption of a covered entity's…" This modification will help to ensure the scope of reporting is limited to more significant incidents and would allow covered entities to more clearly understand their reporting obligations.[9]

Requirements for third-party reporting should be minimized. The IIF acknowledges CISA's concerns regarding incidents originating at third parties or through supply chain compromises given recent high-profile attacks. However, the fourth prong of the definition for a substantial cyber incident[10] may lead to covered entities facing challenges in obtaining detailed incident information from third parties, particularly when such information is not contractually required. This lack of enforceability may hinder covered entities from obtaining necessary information, making it challenging to comply with CIRCIA's incident reporting rules. Additionally, without a materiality component, covered entities would need to collect information from their third-party and supply chain vendors even for minor incidents.

The IIF recommends that CISA clarify in the final rule that covered entities would not be required to obtain information from any third party in order to complete the covered cyber incident report. Rather, CISA would seek such information directly from the impacted third-party. In the event a third-party entity is not covered under CIRCIA, CISA should coordinate with federal and/or state agencies that possess a mandate for collecting such incident information.

If CISA determines to retain the third-party reporting requirements, it should consider narrowing the scope of information required to be reported to that which is critical to CISA's mandate for protecting economic and national security interests. Any third-party reporting should be limited to available and material information that is needed by the covered entity to complete the incident report or place the incident in the proper context.

---

[8] 6 USC 681(16).

[9] The insurance industry has been a leader in developing legally unambiguous definitions and frameworks related to cyber incidents and materiality thresholds. We encourage CISA to collaborate and coordinate with leading cyber insurers and relevant working groups, such as CyberAcuview, whose members represent almost 70% of gross written premiums (GWP) in the U.S. market.

[10] The fourth prong of the proposed substantial cyber incident definition would require a covered entity to report an incident that results in unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a compromise of a CSP, managed service provider, other third-party data hosting provider, or by a supply chain compromise. This prong reflects criteria enumerated in 6 U.S.C. 681b(c)(2)(A)(iii).

Covered entities should be limited to those that perform a critical function. The Proposed Rule suggests that the definition of a covered entity would apply at the group or holding company level, rather than at the level of the entity performing the critical function. We believe that CISA should consider separately each entity in a corporate group and avoid an interpretation that would result in defining as a covered entity the parent organization or holding company as a result of one or more of its subsidiaries or affiliates being deemed a covered entity. We believe that such an approach would be overbroad and would run counter to CISA's definition of National Critical Functions, as "[t]he functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[11] Moreover, an overbroad scope of covered entities could result in the reporting of information to CISA that is superfluous.

We support CISA's determination to define entities within a critical infrastructure sector consistently with the sector-specific profiles outlined under the Critical Infrastructure Sector Profiles.[12] We also urge CISA to regularly update its Sector-Specific Plans.[13]

Refine the scope of data requested in the first 72 hours. The reporting requirements under the Proposed Rule could distract incident response teams from incident investigation and containment efforts during the critical initial phase following the discovery of an incident. The information needed for many proposed data fields often becomes available only after business operations have returned to normal and incident response and investigation have been well advanced. For example, an assessment of response effectiveness and a detailed timeline of system communications may not be feasible within the initial 72-hour timeframe; these details could be provided in a final report, as discussed below.

CIRCIA Agreements, while laudable in concept, may be difficult to implement. Given the granularity of the incident information requirements under the Proposed Rule and the lack of overlap with existing U.S. state and federal incident reporting requirements, it would be difficult to meet the "substantially similar information" threshold contained in the Proposed Rule. Greater harmonization of the cyber incident reporting obligations could enhance the ability of CISA to enter into CIRCIA Agreements. The IIF requests that CISA consider reviewing the proposed data fields in order to identify potential areas to harmonize the cyber incident reporting requirements with the information and timeframes established by other U.S. authorities so that information can meet the substantially similar information and substantially similar timeframe criteria.[14]

Supplemental reporting obligations should be replaced with an obligation to final a single final report. The IIF is concerned that the granular level of information proposed to be reported within 72 hours may lead to covered entities submitting numerous supplemental reports. The IIF acknowledges that covered entities must provide the requested data fields in the covered cyber incident report "***to the extent such information is available and applicable to the covered cyber incident.***" However, the covered cyber incident data elements may not be available for weeks or

[11] https://www.cisa.gov/topics/risk-management/national-critical-functions#:~:text=National%20Critical%20Functions%20(NCFs)%20are,safety%2C%20or%20any%20combination%20thereof.
[12] Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," February 12, 2013.
[13] Ibid.
[14] 6 U.S.C. 681g(a)(5)(C)

months after the substantial cyber incident. Given that, under the Proposed Rule. new information must be reported within 24 hours of discovery, covered entities may find themselves submitting numerous supplemental reports in order to adhere to the reporting requirements. The IIF understands and agrees that much of the information requested as part of the Proposed Rule will assist CISA with gaining deeper insights to those cyber incidents that are impacting critical infrastructure operators. However, we urge CISA to modify its current requirements in order to allow the federal regulatory agencies to meet the ***substantially similar information*** and ***substantially similar timeframe*** criteria, which will allow CISA to obtain initial and interim reporting of the substantial cyber incident.

For the more granular parts of the Covered Cyber Incident Report, the IIF encourages CISA to allow for the submission of a final report. The final report should include data fields that typically only become available once business operations have resumed to normal levels and firms have conducted further analysis to uncover incident details and attempted to determine the source of the incident . Covered entities typically contract a cybersecurity firm to assist with identifying tactics, techniques and procedures used, description of the malicious software, and malicious actor identities and contact information. Covered entities should be allowed the time that is needed to produce accurate and complete reports and to prioritize incident investigation and recovery.

Leverage harmonization to maximize efficiency of reporting. The IIF appreciates the acknowledgement in the Proposed Rule of the numerous existing state and federal reporting requirements to which critical service providers may be subject. Establishing harmonized reporting thresholds across the sixteen (16) critical infrastructure sectors is a challenging endeavor, particularly given the multitude of existing reporting mandates with differing standards. Regulators are increasingly imposing more expansive reporting frameworks with shorter response timeframes.[15]

While IIF members broadly support the need for enhanced cybersecurity regulation to protect critical infrastructure, there is significant concern about the current patchwork of incident reporting rules. The financial services sector has long been one of the most heavily regulated among the critical service sectors and is one of the few to have mandatory cybersecurity, operational resilience, and incident reporting requirements in force over the past two decades. In the U.S., firms must comply with cyber incident frameworks and reporting requirements across existing federal laws, state privacy and incident reporting requirements, agency and sector-specific guidelines and regulations and, for businesses with foreign subsidiaries, the standards and guidance of foreign regulators and global standard setting bodies.

Covered entities should be limited to U.S. domiciled firms and U.S.-based subsidiaries. CISA should also consider limiting the scope of its reporting requirements to substantial cyber incidents occurring at U.S. subsidiaries and ransom payments to those made by U.S. subsidiaries. Requiring the reporting of incidents that occur within international jurisdictions by U.S. subsidiaries operating abroad might establish a difficult precedent, prompting other governments to mandate similar reporting requirements for their domestic entities with respect to their U.S.-based counterparts. This could further complicate global regulatory compliance and lead to a convoluted global regulatory

[15] See, for instance the Federal Housing Administration (FHA) Mortgagee Letter (ML) 2024-10, *Significant Cybersecurity Incident (Cyber Incident) Reporting Requirements,* which as of May 24, 2024 requires FHA-approved mortgagees to report cyber incidents within 12 hours of detection.

environment, creating an untenable position for multinational organizations as they navigate differing international cybersecurity reporting obligations.

Safe harbor and arbitration provisions should be included in the final rule. Under the Proposed Rule, covered entities are required to report ransom payments irrespective of whether the ransomware attack qualifies as a covered cyber incident. While this broad requirement can enhance the government's ability to respond to and mitigate ransomware threats, the current interpretation does not account for scenarios where firms unknowingly pay ransom to sanctioned entities. This gap underscores the need for safe harbor provisions to ensure that well-intentioned companies are not penalized for reporting when they have inadvertently made a ransom payment to a sanctioned entity.

Additionally, we encourage CISA to include mandatory arbitration in the event of liability arising from cyber incident reporting. This approach aims to encourage comprehensive and prompt reporting by providing a fair, efficient, and confidential resolution mechanism for disputes related to cyber incident reports.

Use reporting as a tool for mutual information sharing and collaboration. We encourage CISA to enhance transparency and openness with the 16 critical infrastructure sectors regarding its implementation plans, particularly in sectors like financial services, which already maintain significant expertise in cyber incident management and response. Sustaining an ongoing and iterative dialogue between CISA and critical infrastructure stakeholders could help promote the effectiveness of the final rule. Continued collaboration with industry partners not only aids in shaping a more balanced final rule but can also help maintain relationships between the intelligence and critical infrastructure communities. The White House's recent National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22) similarly emphasizes this notion by requiring the intelligence community to provide increased support and operational collaboration to critical infrastructure entities in response to escalating nation-state threats. [16]

Cybersecurity information sharing must be bidirectional. Cyber incident data that is reported to CISA needs to be promptly aggregated, anonymized, analyzed, and shared with critical infrastructure providers in order to foster the reduction and/or prevention of future cyber incidents. A persistent shortcoming experienced by businesses across many sectors is a lack of timely and effective action or feedback on cyber reports from government.

Stringent protection measures should be in place for reported information. Ensuring the confidentiality and integrity of reported data is paramount to maintaining trust and collaboration between industry and government. The Proposed Rule requires entities to provide detailed information that includes restricted data such as technical details of affected assets and security defenses. The Proposed Rule acknowledges the sensitivity of reported information and accordingly requires that CISA protect such information "at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199." [17] The IIF stresses the importance of CISA putting stringent security measures in place to protect reported information and reassure reporting entities about the confidentiality of their data.

[16] The White House 2024, "National Security Memorandum on Critical Infrastructure Security and Resilience" April 30, 2024.
[17] 6 U.S.C. § 681e(a)(4)

CISA should also provide clarity on how incident data will be shared with Sector Risk Management Agencies (SRMAs). For instance, CISA could consider designating all agency systems containing CIRCIA reports as High Value Assets in accordance with Office of Management and Budget (OMB) guidance,[18] which would allow for consistent implementation of security measures commensurate with the sensitivity of the data collected and the risk environment. This will also support CISA's key objective of mitigating spillover effects to other sectors and to the real economy.[19]

For the financial sector in particular, NSM-22 reaffirms the Treasury Department's primary role as the cybersecurity and resilience coordinator for financial institutions. Given Treasury's crucial role and established relationship with financial institutions and financial regulators, CISA and Treasury should establish a well-defined process for information sharing, including security measures and liability protections.

Conclusion

The IIF appreciates the opportunity to comment on the Proposed Rule. We fully support the goals and objectives of CIRCIA to enhance cyber incident reporting and improve national security. We recognize the critical importance of sharing cyber incident and vulnerability information with the public and private sectors and the IIF and its members have sought to contribute to these efforts in recent years. However, it is essential to balance the timing and content of cyber incident reporting requirements with the need for rapid response to an incident and the many practical considerations and operational realities faced by critical service providers as they respond to an unfolding cyber incident. We believe the proposed rule would benefit from further refinements to ensure its practicability and effectiveness for financial services critical service providers. We hope our comments and recommendations will help CISA as it develops a balanced approach that advances our shared goal of identifying and defending against cyber threats impacting critical service providers.

We look forward to continued collaboration with CISA in advancing effective incident reporting and enhancing the resiliency of our nation's critical infrastructure. If you have any questions or wish to discuss our response, please do not hesitate to contact Martin Boer at mboer@iif.com or Melanie Idler at midler@iif.com.

Sincerely,

Martin Boer
Senior Director, Regulatory Affairs
Institute of International Finance (IIF)

[18] OMB Memorandum M-19-03, "Management of High Value Assets," December 2018.
[19] The White House 2024, "National Security Memorandum on Critical Infrastructure Security and Resilience" April 30, 2024.