Martin Boer
Senior Director
Regulatory Affairs

November 14th, 2022

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

Re: Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Docket ID: CISA-2022-0010)

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 develops proposed regulations on cyber incident reporting pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).[2]

At the outset, we would like to commend CISA for its efforts in developing and refining guidance on cyber incident reporting obligations for critical infrastructure providers since the passage of CIRCIA. Cybersecurity threats and incidents pose an ongoing risk to the public and private sectors and market participants and as noted in the RFI, are "one of the most serious economic and national security threats facing our nation." The IIF and its members recognize the severity of the threat, and the significant role of financial institutions in providing timely, accurate, and decision-useful information on cybersecurity incidents in their capacity as vital components of the nation's critical infrastructure. We also value information sharing, both with authorities and across the financial sector, and recognize the important role that CISA and other authorities play in sharing information about indicators of compromise, tactics, techniques, procedures, and best practices to reduce the risk of a cyber incident propagating within and across sectors.

[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] CISA 2022. "Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022" September 12, 2022.

We are strongly supportive of CIRCIA's reporting requirements within 72 hours of a "covered cyber incident" and that ransomware payments should be reported within 24 hours, so that CISA can render assistance and disseminate actionable, anonymized cyber threat information to the appropriate stakeholders. We also want to underscore the importance of the provision that the 72-hour deadline for reporting should be initiated only once the covered entity makes the determination that a covered cyber incident has occurred.

Information-sharing is critical, especially at the beginning of an attack, and we appreciate CISA supporting the overall cyber resilience of the financial sector. We propose several recommendations that we hope will clarify the requirements and ultimately increase the cybersecurity of national critical infrastructure in the U.S., and across jurisdictions.

The IIF believes that financial firms are uniquely positioned to play a vital role in supporting and protecting the overall cyber resilience of the financial system. Cyber incident reporting can be a beneficial tool that helps protect the overall financial system by making the U.S. government aware of specific incidents and alerting them to issues that could impact other parts of the financial system or other critical infrastructure sectors. Depending on how the U.S. government responds to the information, it can also help firms recover faster and prevent other organizations from being impacted by that same (or similar) cyber incident. In practice, however, and as has been detailed in an IIF Staff Paper[3], cyber incident reporting is less effective than it can be due to ambiguity around how firms and regulatory authorities define what constitutes a cyber incident, as well as differing approaches and reporting requirements.

Given that cyber incidents often take place simultaneously across multiple jurisdictions, we support efforts by CISA and other U.S. agencies to propose rules and guidance that are consistent with those being drafted by global standard-setting bodies, especially the Financial Stability Board (FSB), which has indicated that greater harmonization of regulatory reporting of cyber incidents would promote financial stability across jurisdictions.[4] We support efforts by global standard-setting bodies such as the FSB to help achieve greater convergence across jurisdictions, and are responding to the FSB's own consultative document on achieving greater convergence in cyber incident reporting, which includes recommendations for how authorities can streamline their processes, establish terminologies, and develop a common format for incident reporting.[5]

Lastly, it is important to highlight that government reporting and regulatory reporting have two significant differences, which may create challenges for alignment:

- Government reporting focuses on attribution to the threat actor conducting the attack, whereas regulatory reporting focuses on the incident impact regardless of knowledge of the exact threat actor (e.g., internal); and,
- Government reporting focuses on 'malicious intent' whereas regulatory reporting focuses on both malicious and unintentional (e.g., operator error) intent.

---

[3] IIF 2021. "IIF Paper on the Importance of More Effective Cyber Incident Reporting" June 10, 2021.

[4] FSB 2021. "Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence" October 19, 2021

[5] FSB 2022. "Achieving Greater Convergence in Cyber Incident Reporting – Consultative document" October 17, 2022

As such, information that would be of relevance to a government agency may not always be relevant to a financial authority, and vice versa, which may lead to differences in the data that is collected and reported.

Collaborating with private sector-led cyber incident reporting initiatives

It should also be acknowledged that while cybersecurity threats represent a new challenge for many critical infrastructure operators, the financial services industry has long been a target of malicious cyber threats. As such, the sector has long understood the importance of providing robust and timely disclosures about material cybersecurity incidents and vulnerabilities, and has invested considerably in measures to prevent, detect, and respond to cyber threats. This includes the creation of the Financial Services Information Sharing and Analysis Center (FS-ISAC), an industry consortium that has been a pioneering model for voluntarily sharing cyber threat intelligence.

The FS-ISAC network consists of nearly 16,000 users, representing cybersecurity professionals across 65 countries, who are committed to reducing cyber risk in the global financial system. The FS-ISAC also maintains a Global Intelligence Office (GIO), responsible for coordinating and disseminating analysis of member-submitted intelligence as well as threat alerts to its member financial institutions around the world. GIO regularly issues reports and convenes member calls as well as spotlight calls on emergent issues to ensure members are prepared for current threats. GIO also coordinates with other cybersecurity organizations, companies, and agencies around the world to ensure that actionable and timely cyber intelligence is disseminated.

Since its formation in 1999, the FS-ISAC model has been replicated by other industries, including other critical service providers. In addition to making cyber incident reporting interoperable with other state and federal government regulations, we believe that CISA's rulemaking should wherever possible align its reporting requirements – including materiality thresholds, processes, and procedures – with the existing frameworks under the various ISACs. The ISAC model has been successful in disseminating information in a timely and confidential manner to industry stakeholders, albeit on a voluntary basis. Incorporating established reporting practices can help strengthen the overall resilience of our critical infrastructure system, especially for providers with fewer resources and at different stages of cybersecurity maturity. We urge CISA to collaborate with the ISACs of critical service providers and replicate those successes in its own rulemaking. We see alignment both with and between the ISACs as a key area where CISA can meaningfully contribute by facilitating the transmission of threat information across sectors. CISA should also clarify whether reporting to a sector-based ISAC will continue to count as reporting the incident to CISA for those sectors where such reporting has been the standard in the past.

Ongoing cooperation and collaborative efforts between financial services firms and various federal law enforcement and regulatory agencies is important, given their shared mission of strengthening the resiliency of the financial system against cyber threats and incidents. To successfully combat cyber risk, U.S. public and private sector entities need to collaborate with trusted stakeholders within the industry, as well as actively participate in global information and intelligence sharing arrangements. CISA should establish and strengthen public and private partnerships through joint tabletop exercises and relationship building with its international counterparts. CISA should also consider developing an international public-private sector forum to address the transnational nature of cyber threats.

Harmonization of reporting requirements

With the proliferation of cybersecurity incident reporting requirements over the years, CISA's rulemaking enters a diverse reporting environment for cyber incidents. This ecosystem is particularly complicated for financial service providers, which often face multiple 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 international regulatory bodies. Given this complex reporting and compliance landscape, the IIF and its member organizations have worked collaboratively with federal, state, and international authorities to promote the harmonization of reporting requirements, and to achieve an appropriate balance between the benefits of incident reporting and the risks, harms, and operational burdens that may be associated with reporting.

We fully endorse CISA's objective of enhancing and standardizing disclosures from covered entities about material cybersecurity incidents and those entities' mitigation efforts. In particular, we welcome the creation of the Cyber Incident Reporting Council (CIRC) pursuant to CIRCIA, and its attendant responsibilities to "coordinate, deconflict, and harmonize" cyber incident reporting requirements across federal agencies. Many covered entities are already subject to mandatory cyber incident reporting requirements, at both the federal and state levels. Companies may struggle to navigate overlapping, and often conflicting, requirements from multiple federal agencies on top of state law data breach and/or data privacy notification requirements, especially when remediation efforts are still underway following a cyber incident. We recommend that CISA expand its harmonization efforts to include alignment not just across the federal reporting regime, but also seek to align state level notification requirements.

Given the international nature of cyber threats, and as underscored above, we would recommend that CISA work in coordination with its international counterparts to promote common global reporting standards. Cyber threats and contagion are borderless, and the attack surface only continues to grow as companies become increasingly digitized in the wake of the COVID-19 pandemic and with continued innovation in financial services. The global financial system is particularly multinational and interconnected, with firms maintaining foreign subsidiaries, cross-border operations, and relying on offshore third-party vendors and supply chains. A major cyberattack could unfold simultaneously across multiple jurisdictions and create a "cyber incident" for the same organization in several countries at once. As such, international regulatory and supervisory fragmentation is a considerable concern to the financial services industry, in part because different approaches can combine to slow down the process to provide authorities with quick, useful, and actionable information.[6]

Ultimately, CISA's rulemaking should be aligned with leading global best practices, which would help address regulatory and supervisory fragmentation. We have provided comments below to

[6] Consider this example regarding a global systemically important bank (G-SIB) with large operations in Europe and the U.S. from the FSB 2022 consultation reference above. In the event of a cyber incident which triggers reporting requirements in all jurisdictions that the G-SIB operates, the G-SIB, in the first 72 hours, has to verbally contact five or more authorities, issue between 7-13 written notifications, complete and submit 12-14 initial incident report forms and enter details into 5-9 online reporting portals. Each notification is edited and reviewed by incident response teams to ensure it is technically accurate according to the latest information as more details of the incident emerge, which is particularly dynamic in the first 24 hours of an incident.

address the main areas of discussion in the RFI and look forward to continued collaboration with CISA throughout the final rulemaking process.

Definitions, Criteria and Scope of Regulatory Coverage

Covered Entity

The definition of a covered entity should be risk- and principles-based rather than set on fixed, specific criteria. The definition should also indicate the difference or similarities between a covered entity and a firm designated as a Section 9 entity. The U.S. Executive Order 13636 tasked the Department of Homeland Security (DHS) to annually identify and maintain a list of critical infrastructure entities.[7] A Section 9 entity is defined as, "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economy security, or national security."

Finally, ensuring that every organization knows whether it is a covered entity is a difficult challenge. CISA should consider an awareness campaign to make sure organizations deemed to be covered entities are aware of their obligations. Further, we would anticipate that some organizations may ask CISA to determine whether they are a covered entity, in which case it would be useful to create a channel for organizations to contact CISA regarding this point.

Covered Cyber Incident vs Substantial Cyber Incident

In recent years, there has been an expanding set of definitions introduced by different regulatory bodies across jurisdictions on what constitutes an "incident," as well as what constitutes a "material" or "substantial" incident. The ambiguity around definitions has created regulatory fragmentation across global financial services firms, which must navigate and reconcile these different terms and their attendant reporting requirements. This leads to increased complexity in reporting often at a time when teams need to dedicate their resources to responding to an incident.

The IIF recommends that the definition of an incident refrain from including ambiguous words such as "potential" and "imminent," and should instead focus on the occurrence of actual harm to the confidentiality, integrity or availability of an information system or the information that the system processes, stores, or transmits. We also believe that CISA should focus on cyber incidents where there is actual harm to organizations, so that CISA is alerted to those substantial cyber incidents that should be prioritized and responded to most urgently. Therefore, it would make sense, also given the objectives of CISA, to focus exclusively on substantial cyber incidents, given they are the ones that require the most urgent attention.

For these reasons, we would encourage CISA to take an outcomes-focused view when developing its definition of "substantial cyber incidents." This would allow organizations to apply their own criteria for determining materiality within the bounds established by CIRCIA. Flexibility in applying materiality thresholds is particularly important, given that a one-size-fits all approach is not possible for each sector or across sectors. We would encourage CISA to consider the process undertaken by the federal banking agencies when defining the Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers

[7] The White House 2013. "Executive Order -- Improving Critical Infrastructure Cybersecurity." February 12, 2013.

rule ("Computer-Security Incident Notification rule")[8]. Ultimately, the definition largely spares subjective language on what constitutes an incident. This type of approach could help enable covered entities to focus on sharing the most elevated incidents with CISA.

Malicious vs non-Malicious incidents

Another important distinction is between malicious and non-malicious incidents. We believe that the definition of a "cyber incident" should be limited only to malicious incidents, and that a "substantial cyber incident," should in turn be limited to malicious incidents of a high materiality threshold. Non-malicious incidents tend to be technology or operational disruptions which, while important, should be excluded from the scope of substantial cyber incidents to which CISA would likely want to address and respond. These non-malicious technological or operational disruptions can be shared through existing platforms, such as the FS-ISAC, to make other organizations aware of such issues. Given that this RFI is aimed at all critical sectors, we would encourage other sectors to also maximize the use of ISACs, which can be great resource for information-sharing between firms, and with the public sector.

Finally, we urge CISA to include examples of covered cyber incidents once its definition is finalized. This was an approach taken by the federal banking agencies, which provided several examples of what they and the financial services industry would generally consider to be an incident requiring notification. Such examples will help each sector better understand how to apply the definition and criteria and help prevent under or over reporting.

Report Contents and Submission Procedures

Initial Incident Report Contents

Given the nature of CISA's mission and how its objectives are different from regulatory and supervisory authorities, the necessary content of an incident report to CISA would likely differ from reports sent to regulators. We believe CISA's overall objective in obtaining cyber incident reporting information is to strengthen national resiliency and drive a common analysis and action across critical infrastructure sectors and therefore, differentiates the type of incident that would be reported to CISA compared to regulators. Specifically, we believe sharing incident information with CISA will help to:

- Analyze potential patterns of successful attacks on critical infrastructure firms to better identify weaknesses that need to be addressed;
- Conduct attribution on attacks that occur on our most critical national infrastructure to thwart future malicious actors;
- Act as a conduit for sharing pertinent threat intelligence with private sector critical infrastructure stakeholders to potentially prevent attacks from occurring or from causing catastrophic harm; and,

[8] Under the Computer-Security Incident Notification rule, a "notification incident" is defined as a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade a banking organization's business line, including associated operations, services, functions, and support, and would result in material loss of revenue, profit, or franchise value or operations of a covered entity, the failure or discontinuance of which would pose a threat to national security, economic security, or public health and safety. US Treasury, Federal Reserve, FDIC 2021. "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers" November 17, 2021.

- Conduct policy or other government measures needed to lower the number of threats and threat actors conducting cyber operations against critical infrastructure.

Generally, information provided to regulators and supervisors around the world does not include all information CISA identified in section 2242(c)(5). However, we believe there are benefits to sharing additional, sanitized information with CISA, where applicable and available, to support CISA's mission and objectives. The reports should not be required to include any information that could potentially disclose specific and technical information about covered entities' systems, response measures, or vulnerabilities in such a manner that would impede a covered entity's response or remediation efforts.

Supplemental Reporting

We appreciate CISA's efforts to balance providing situational awareness with the ability of a covered entity to conduct cyber incident response and investigation, as well as its work towards harmonizing supplemental reporting information. IIF members support sharing supplemental information to aid in CISA's objective and recommend defining "substantial new or different information" in way that ensures a reduced burden on firms.

We would suggest that substantial new or different information should be submitted if circumstances related to the incident have changed materially. These could include but not be limited to:

- Changes to the scope of type (e.g., PII, MNPI) or data stolen or altered, or the number or type of systems impacted;
- Changes to the timeframe of the attack (e.g., earlier indications of compromise);
- Updates to information regarding the tactics, techniques, and procedures (TTPs) used in the attack; and,
- Updates to malicious IPs used in the attack.

New information could be available quickly and facts may change many times during the course of an incident investigation. To prevent firms from having to submit numerous supplemental reports, supplemental reports should be submitted upon the determination by the covered entity that material changes were identified during incident investigations.

Submission Formats and Procedures

CISA should develop a limited, core set of questions that every reporting entity must answer. Beyond the core questions, the reporting form should have different questions depending on the incident being reported. Formats should also be expandable to include additional technical questions, based on criteria such as the size and/or technical capability of the reporting entity, the severity of the reported incident, or other factors.

When it comes to the impact of a widespread third-party incident, it would be useful for covered entities to submit their own reports on the respective impact on their organization. That would allow CISA to benefit from seeing the specific impacts on different covered entities, which could provide a more meaningful overall impact of such an event. Whenever such information is shared across authorities, it is critical that it is done so in an anonymized manner, with sufficient protections in place that promotes confidence in the confidentiality of the disclosed information. The implementing regulation should also clarify that third parties have no obligation to report a cyber incident independent of the covered entity.

Finally, to the extent allowable under statute, CISA should make clear that filing an incident report under this regulation does not automatically trigger any other reporting action or obligation. Organizations will have to determine whether to file reports with other oversight bodies or agencies based on those reporting requirements, not just because the incident qualified for a report under this statute, given the differences in government reporting and regulatory reporting we highlighted above.

Safe harbor provisions

We applaud CISA's emphasis on the confidentiality throughout the RFI, as we believe mandatory reporting should be designed to contribute to a culture of transparency, openness, and accountability.

We also agree with the proposed safe harbor provisions for covered entities who may be unable to include all required disclosures. Safe harbor protections should incentivize proactive reporting and transparency and strengthen sound cyber risk management practices. Covered entities reporting under the forthcoming rule should be seen as victims of a cyber incident; protections should not be designed to penalize or publicly shame companies. We also call on CISA to take appropriate steps to secure the incident reporting system and associated data, including minimization, anonymization, and aggregation when appropriate.

Concluding remarks

Thank you for the opportunity to share our feedback with you on this important work being undertaken by CISA. As noted above, the IIF and its members are strong supporters of information-sharing and appreciate all the efforts being undertaken by the CISA and other authorities to protect and safeguard the overall financial system, and other critical infrastructure. Given the substantial amount of information sharing requirements already in place, both domestically and internationally, we strongly urge CISA to be consistent with international standards in the way it defines terms and what type of information is required to be submitted.

Given that government reporting and regulatory reporting are often focused on different motivations, we urge CISA to 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 as quickly as possible, in an anonymized, non-attributable manner. Other types of cyber incidents, and technological and operational incidents, should continue to be covered under existing government and regulatory frameworks, and shared across information-sharing platforms such as FS-ISAC.

We thank CISA for its consideration of our comments. If you have any questions, 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)