November 14, 2022

Via electronic submission

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

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

Dear Director Easterly:

The Bank Policy Institute ("BPI"), American Bankers Association ("ABA"), Institute of International Bankers ("IIB"), and Securities Industry and Financial Markets Association ("SIFMA") (together, "the Associations")[1] appreciate the invitation to contribute comments to the Cybersecurity and Infrastructure Security Agency's ("CISA") request for information ("RFI") on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") requirement to develop regulations related to critical infrastructure cyber incident reporting.

The Associations applaud CISA's early and frequent communications signaling an intent to work with critical infrastructure entities to craft an effective rule and welcome the efforts evident through this engagement and ongoing public listening sessions. We share a mutual commitment to cybersecurity and the value in sharing threat and incident information, and support efforts to fortify CISA as a leader in this

[1] BPI is a nonpartisan group representing the nation's leading banks. BPI members include universal banks, regional banks, and the major foreign banks doing business in the United States. Collectively, BPI members hold $10.7 trillion in deposits in the United States; make 68% of all loans, including trillions of dollars in funding for small businesses and household mortgages, credit cards, and auto loans; employ nearly two million Americans and serve as a principal engine for the nation's financial innovation and economic growth. 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.

The ABA is the voice of the nation's $23.7 trillion banking industry, which is composed of small, regional, and large banks that together employ more than 2 million people, safeguard $19.6 trillion in deposits, and extend $11.8 trillion in loans.

IIB represents internationally headquartered financial institutions from over thirty-five countries around the world doing business in the United States. Its members consist principally of international banks that conduct U.S. operations through branches and agencies, bank subsidiaries, and broker-dealer subsidiaries. The mission of the IIB is to help resolve the many special legislative, regulatory, and tax issues confronting internationally headquartered financial institutions that engage in banking, securities and/or insurance activities in the United States.

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)

space while minimizing the shared burden to actively defending critical infrastructure systems. The financial services sector is one of the few critical infrastructure sectors that has had mandatory cybersecurity and incident reporting requirements in law and regulation for over 20 years. In addition to a long history of complying with a variety of cybersecurity and incident reporting requirements, the financial services sector has been voluntarily sharing cyber threat information when appropriate and in accordance with relevant legal authorities, with the Federal Bureau of Investigation ("FBI"), the U.S. Secret Service, and Department of Homeland Security ("DHS"), to facilitate the federal government's interdiction of malicious cyber activity. The Associations also share information when appropriate with a wide range of partners via the Financial Services Information Sharing and Analysis Center ("FS-ISAC"), which shares cyber threat information and best practices among nearly 7,000 members across the globe, including 4,600 U.S. financial institutions. The FS-ISAC was one of the first ISACs created in 1999 and is widely recognized as the gold-standard that other sectors have worked to replicate.

We agree with CISA's assertion that the proliferation of cyber incidents is one of the most critical economic and national security threats facing our nation. Effective visibility, awareness, and coordinated information sharing between the public and private sectors is critical during a cyber incident, and reasonable incident reporting to government entities can help disrupt attackers and assist affected firms with protection, mitigation, and response. We understand that the ability to attribute cyber incidents to an entity or entities is key to supporting other important policy objectives including holding malicious actors accountable for their nefarious activities. However, there are multiple policy objectives at play across the incident reporting landscape, such as providing early warning with actionable information and voluntary supplemental information sharing as the incident unfolds. We urge CISA to recognize this as an opportunity to demonstrate needed leadership and ensure that where there are requirements for incident reporting, they are simple, tied to an actionable purpose and broadly useful.

As a critical infrastructure sector that regularly reports cyber incidents to a variety of financial regulators, both domestic and international, the effectiveness of this rule largely depends on CISA requiring a high threshold of severity for the incidents required to be reported. Thousands of cyber events – system changes that may have an impact on organizational operations (including mission, capabilities or reputation)[2] - occur daily, and critical infrastructure entities are constantly monitoring and evaluating for signals of intensified or malicious events that may turn out to be precursors to serious cyber incidents. If the incident threshold is set too low, the amount of information reported will be so voluminous as to render the reporting exercise useless in the context of the CISA mission. It will also impose an unnecessary burden on companies that in many instances already have a sizeable cyber incident reporting compliance obligation in addition to their ongoing need to focus resources on critical network defense efforts.

We strongly believe that the cyber incident information required to be reported should be tightly linked with an actionable purpose and would appreciate further clarity from CISA on how it will utilize the reported incident information in furtherance of that purpose. Additionally, we call on CISA to provide clear principles regarding how the reported information will be stored, secured and transmitted, both within the agency as well as shared with, or accessed by, other government entities and other covered entities. It is critical that CISA appropriately balances the need to get information into the right hands quickly without creating noise in the reporting channel that could be both a distraction for CISA and a burden to the cyber teams of covered entities. We hope that this feedback will help CISA develop workable reporting requirements that create confidence that the information required to be reported to CISA makes a meaningful difference in a coordinated cyber incident response.

[2] https://csrc.nist.gov/glossary/term/cybersecurity_event

I. Definitions, criteria, and scope of regulatory coverage

a. The definition of covered entity should ensure that critical infrastructure entities are uniformly held to the same set of cross-sectoral reporting standards and focus on the materiality of the incident over the characteristics of the individual covered entity

As we have seen with recent events, a cyber incident need not originate from the largest or most dominant market participants to create severe consequences for critical infrastructure and national security. If compromised, entities within each of the sixteen critical infrastructure sectors currently identified by Presidential Policy Directive 21 ("PPD-21") could present a potential threat to our national security, economic stability, or public health and safety depending on the sophistication or novelty of the threat actor's approach, the data or systems involved and the number of impacted individuals or critical infrastructure entities. Financial institutions continue to expand their use of new and emerging technology to strengthen the resilience of their operations and deliver new products and services to meet customer needs. As the threat landscape continues to evolve and financial institutions improve the security and resilience of their technology infrastructure, threat actors are probing vulnerabilities in commonly-used third parties as they seek to disrupt critical services.

We encourage CISA to take a broad view in defining the universe of covered entities while also accounting for factors set forth in the CIRCIA statutory requirements including: the likelihood that an entity may be targeted; the consequences of an entity's disruption; and the extent to which the effects of the incident will disrupt the reliable operation of critical infrastructure. Still, there could be instances where an entity outside the PPD-21 designation provides critical or non-critical services to a PPD-21 -designated entity and becomes a novel vector for a threat actor to perpetrate a cyber incident. With this in mind, we urge CISA to consider an approach that prioritizes the materiality of the incident over the characteristics of the covered entity in determining which entities are obligated to report. For example, we recommend the inclusion of third parties with a material technology relationship to the critical infrastructure entity (including technology providers like cloud services and data aggregators that have access to large amounts of sensitive data) within the definition of covered entities. Finally, CISA should prioritize making the reporting process as simple and painless as possible to balance the need for a wide swath of critical infrastructure firms to be covered with the ability of smaller, less-sophisticated firms to easily comply.

b. Reportable cyber incidents to CISA should include only incidents of a particularly elevated severity and malicious intent that cause material harm to the critical infrastructure entity at the enterprise level

To move ever closer toward a more harmonized and consistent required incident reporting landscape, we encourage CISA to align the definition of a covered cyber incident as closely as possible with existing reporting requirements and frameworks, the majority of which use a NIST-based ("National Institute for Standards and Technology") definition. For example, recognizing the benefits of aligning to existing definitions, the federal banking agencies' Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers rule ("Computer-Security Incident Notification rule")[3] uses the NIST definition when requiring banks to notify their primary regulator within 36-hours of determining a notification-level cyber incident has occurred. The NIST definition is already in use across multiple critical infrastructure sectors and is also a component of the Federal Information Security Modernization Act's ("FISMA") definition of an incident.

[3] https://www.fdic.gov/news/board-matters/2021/2021-11-17-notational-fr.pdf at 66429.

In addition to basing the definition on existing NIST language, we encourage CISA to proceed in the spirit of the underlying CIRCIA law and focus on incidents where there is material harm to a covered entity. This ensures that CISA is purposefully alerted to incidents where its ability to quickly aggregate and analyze threats across multiple sectors and then provide early warning and risk mitigation measures to others can be fully leveraged without being overwhelmed with unusable or less-significant or impactful information.

While a harmonized NIST-based definition is useful as a baseline for alignment across the reporting landscape, CISA should also ensure that reported incidents are severe and threatening to critical infrastructure and are not mere technology outages or inconvenient service interruptions. It is also important to ensure that the covered entity is responsible for evaluating and determining the materiality relative to the attendant facts and circumstances of the incident across the enterprise. To accomplish this, we suggest including both motive-based characteristics such as a "malicious intent" element as well as appropriately calibrated severity characteristics so that covered entities do not report otherwise anodyne technology outages or other systems complications that, while potentially serious to the covered entity (such as a serious internal software update error), pose no wider threat to critical infrastructure or national security. Doing so will allow covered entities to focus their attention on response and remediation while also ensuring that CISA receives useful information aligned with its mission and any resulting actionable purpose.

We support CISA's focus on bringing malicious threat actors to justice[4] and as reflected above, urge the inclusion of a "malicious intent" element to distinguish the kind of incident and purpose for reporting to CISA from other required incident reporting to other regulators. To meet this specific threshold, it is important for covered entities to reasonably believe that the incident they are experiencing is the likely result of a malicious cyber actor's intentional actions. This differentiates the kind of incident that will be reported to CISA as one that presents a threat to critical infrastructure in a way that CISA is distinctively positioned to recognize, manage, and even marshal resources to respond.

Along with a "malicious intent" element, we encourage CISA to consider additional existing language found in the Computer-Security Incident Notification rule[5] to develop its severity characteristics and adopt parts (ii) and (iii) of the definition of a "notification incident" to more readily align with the type of "malicious notification incident" on which we believe that CISA should be receiving reported information. Modeling off the existing computer-security incident notification rule, CISA should seek reporting on incidents that, because of the actions of a malicious threat actor, a covered entity believes in good faith:

> are materially disrupting, degrading, or impairing a business line, including associated operations, services, functions, and support, or 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 critical infrastructure.

Adopting this high threshold will ensure that only the most critical and threatening incidents deserving of CISA's attention are reported for an actionable purpose. Basing the broader scope in a NIST-based definition will also contribute significantly to harmonization across various incident notification and reporting requirements for financial institutions, bringing much-needed efficiencies to the reporting process.

---

[4] https://www.govinfo.gov/content/pkg/FR-2022-09-12/pdf/2022-19550.pdf at 55831.
[5] https://www.fdic.gov/news/board-matters/2021/2021-11-17-notational-fr.pdf at 66429.

II. Reporting mechanics, incident response, and information sharing considerations

As previously noted, the financial services industry has been supportive of the incident reporting provisions of the underlying CIRCIA legislation. We appreciate Congress including specific requirements to harmonize new requirements with existing regulations where possible, such as the timeline for reporting, as well as requirements to coordinate with Sector Risk Management Agencies ("SRMAs") and regulatory authorities to streamline reporting requirements. While we recognize there is value in reporting to CISA alongside our current incident reporting obligations, it is important to ensure government agencies and regulators work together to develop a common reporting form that would be useful for all government entities requiring incident reporting. Otherwise, more time will be spent by first responders in covered entities working with their legal and compliance teams to ensure that each agency's nuanced requirement is met, rather than reporting uniformly and allowing more time to protect critical infrastructure.

Reporting Mechanism – In considering the development of the formal reporting mechanism, we encourage CISA to prioritize accessibility, functionality and simplicity. As previously noted, the Associations believe that reported information should be closely tied to an actionable purpose in furtherance of CISA's mission to protect critical infrastructure. However, the underlying statute requires a potentially onerous set of information to be reported that will likely result in covered entities providing incomplete and decontextualized information, serving to distract both CISA and the victim of the cyber incident.

Therefore, we strongly encourage CISA to create a staggered reporting requirement composed of an initial, high-level notification of the immediately known details of the incident within seventy-two hours containing actionable information for CISA to monitor, and supplemental material updates on an ongoing basis to fulfill the enumerated statutory requirement. This would not preclude CISA from directly engaging with an entity after being notified of a covered cyber incident in order to directly ascertain more details about an ongoing incident, but it would alleviate some of the burden that entities face in balancing a response with initial reporting obligations.

In terms of practical submission, CISA should accept submission through a reasonable range of channels, both electronic and non-electronic, and commensurate with the covered entity's capabilities during an ongoing cyber incident. In the event of a particularly severe cyber incident, the ability to securely transmit required information electronically may be degraded or disabled and covered entities should be able to satisfy initial reporting obligations via other methods of communication. However, this should not preclude CISA from establishing an easily usable and secure online reporting portal and form that can be accessible absent exigent circumstances. Prioritizing accessibility, functionality and simplicity will make it more likely that entities with less-robust response capabilities will still be able to communicate important incident information that may better inform CISA's situational awareness throughout the supply chain and beyond the victim entity regardless of response sophistication.

Supplemental Reporting – Supplemental reports should be voluntarily submitted upon the determination by the covered entity that circumstances surrounding the incident have materially changed. Examples of material changes (i.e., new or different information) would include, but not be limited to: changes to the scope or type (e.g., PII ("personally identifiable information"), MNPI ("material non-public information")) of 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. This is also an opportunity for CISA to consider separate reporting mechanisms and create an initial required reporting mechanism for early warning where the information reported is tightly linked with and supports CISA's response capabilities as well as a channel for ongoing voluntary information sharing of subsequent material

updates regarding a new reportable cyber incident. Finally, we urge CISA to not include a requirement to affirmatively notify it of final remediation of the reported incident. The Associations believe that where CISA is fully engaged with the covered entity in exchanging information and in receipt of supplemental reporting, the dialogue will naturally resolve of its own volition.

Reporting Timelines – We are supportive of the CIRCIA requirement that the reporting timeline commence no earlier than seventy-two hours after determining the occurrence a covered cyber incident. The 72-hour timeline strikes an important balance between allowing an affected entity to implement immediate response measures while ensuring CISA receives timely, useful, and accurate information. The initial stages of an incident response require "all-hands-on-deck" to focus immediately on understanding the incident and implementing mitigation and response measures. Depending on a covered entity's operating footprint in other jurisdictions and the severity of the incident, some are subject to over 100 different global incident reporting requirements with varying and potentially much shorter reporting timelines. Seventy-two hours is a sufficient period to balance the competing priorities of avoiding reports that may be premature and erroneous during the critical early stages of a response with ensuring that information being reported is timely and useful to furthering CISA's mission. In considering the accompanying 24-hour timeline to report ransomware payments, we believe the 24-hour clock should begin only after the transaction has completed, so that there is meaningful transaction data to report and use in interagency response efforts.

Improving Coordination and Response - The financial services industry currently reports to many federal departments, agencies and independent regulators that receive cyber incident or ransom payment reports from critical infrastructure. There is significant overlap between reporting timelines and materiality thresholds, which if not coordinated, can both distract from or degrade ongoing incident response.[6] We appreciate the approach taken in the underlying CIRCIA law to acknowledge this by establishing the Cyber Incident Reporting Council ("CIRC") to coordinate, deconflict and harmonize existing and future federal cyber incident reporting requirements. We recommend that CISA review and where permitted, adopt the findings of the Council's ongoing work to meaningfully improve cybersecurity and reduce the shared burden by advancing common standards for incident reporting. We also encourage CISA to coordinate with other authorities, including international peers, to converge on a common reporting format such as the kind described in the Financial Stability Board's ("FSB") recent consultative document, *Achieving Greater Convergence in Cyber Incident Reporting*. Within this document, the FSB notes that in reviewing the state of global reporting regimes, there is "…a high degree of commonality in the information requirements for cyber incident reports."[7] The FSB recommends that authorities explore the opportunity for further convergence through the development of a common reporting format (as referenced in the consultation, a format for incident reporting exchange, or "FIRE") that "could greatly enhance incident reporting practices on a global basis, address operational challenges and foster better communication."[8]

Interagency Utility and Coordination – CISA should establish or maintain interagency channels, especially with SRMAs such as the financial sector's Treasury Department and federal law enforcement, both to avoid redundant reporting and to ensure that relevant information is shared or otherwise made available in a timely manner. A core element of CISA's value-add to the cyber incident response ecosystem should be the ability to quickly and confidently "connect the dots" with other government assets and resources, recognize patterns and coordinated threat actor activity to respond faster and more effectively to protect critical infrastructure. Including ways to share information easily at the interagency level while

[6] https://bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/
[7] https://www.fsb.org/wp-content/uploads/P171022.pdf at 24.
[8] Id.

maintaining protections against disclosure and misuse as outlined in CIRCIA would help immensely with duplicative reporting and incident response on the part of affected covered entities. Incident reports submitted to CISA may contain highly sensitive or proprietary information. Therefore, we urge CISA to provide covered entities with assurances as to its own data security practices and clarity around its plans for sharing information with other agencies. To that end, as Memorandums of Understanding ("MOUs") and other mechanisms are developed between agencies it is critical that any interagency information sharing be conducted in an anonymized manner so that covered entities can feel assured in the confidentiality of the disclosed information.

Operational Burden – CISA requests detailed information about the quantifiable time and costs associated with compiling and reporting on a cyber incident, as well as associated costs related to incident data retention. Due to the wide variability in requirements across the incident reporting requirement landscape, as well as the varying nature of cyber incidents, there is not readily available or meaningful data to share on a sectoral basis. However, we would like to highlight the many professionals, enterprise-wide and potentially multi-jurisdictionally, who are engaged in response and remediation during a major cyber incident in tasks that likely outside of their normal routine. During such an incident, there would be engagement from cyber and technology to recover and remediate the event; legal and compliance to advise on notification obligations and the preservation of information; regulatory relations to examine and act on obligations at both the federal and local level; corporate communications to engage with media where the impact is publicly known, legislative affairs to keep congressional representatives apprised of developments; and corporate governance to ensure timely notification to shareholders, when appropriate, and others required to update key executives and board members responsible for corporate governance. In each incident occurrence, resources devoted to complying with additional or disparate reporting requirements are resources that could be devoted to focusing on incident response and recovery.

Substantially Similar Reported Information and Timeframe – With regard to the initial covered incident reporting requirement being developed, we support the CIRCIA language that carves out covered entities required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe where CISA and the Federal agency have an agreement in place to satisfy CIRCIA reporting requirements. We urge CISA to identify where these agreements already exist and where they need to be formed, to reduce the shared reporting burden and to streamline the flow of information from entities already engaged in incident response.

Reasonable Belief – We recommend that "reasonable belief" as referenced in CIRCIA be interpreted to mean that the covered entity has determined *in good faith* that the incident has reached the threshold of a substantial cyber incident. Speed is critical, especially for an agency in CISA's position seeking to analyze, coordinate, and react to augment response efforts. But it is equally critical that covered entities do not feel pressured to determine incident severity instantly and precisely while they are defending their systems and trying to understand impact. Covered entities experiencing a substantial cyber incident are targets and victims, and a "good faith" component will allow firms to meet their reporting obligations with the confidence that their initial evaluation is not subject to second-guessing or subsequent punitive actions.

Liability Protection – We appreciate the evident commitment to confidentiality and information security throughout CISA's public industry engagements and within the underlying RFI. As the victims of a cyber incident, reporting entities must feel confident to proactively report in a confidential manner without fear of penalty or reputational harm in order for CISA's mission to be realized. Liability protections should incentivize proactive reporting and transparency and strengthen sound cyber risk management practices. We urge CISA to keep in mind that covered entities reporting under the forthcoming rule are victims of a cyber incident and incident reporting should not be designed to penalize or publicly shame them.

If you have any questions or would like to discuss these responses further, please reach out to Brian Anderson at brian.anderson@bpi.com, John Carlson at jcarlson@aba.com, Michelle Meertens at mmertens@iib.org, or Thomas Wagner at twagner@sifma.org.

Respectfully submitted,

Brian R. Anderson
Senior Vice President, Technology Regulation
Bank Policy Institute

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

Briget Polichene
Chief Executive Officer
Institute of International Bankers

Thomas M Wagner

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