November 9, 2022

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 Payments Leadership Association[1] (PLC) appreciates the opportunity to comment on 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. As a CEO-led organization, the PLC is committed to expanding global commerce and driving inclusive growth by encouraging public policies that protect consumers, foster inclusion, and promote innovation and competition in payments.

Protecting America's payments system is more important than ever as information and communications technology play an increasingly critical role in our broader economy and society, including in our financials, energy, health care, and education systems. High-profile cyber attacks have highlighted the need to harden our nation's cyber defenses and ensure that the public and private sectors are working together to strengthen our nation's cybersecurity. As this issue has risen in importance, the federal government has increased private sector data sharing requirements, but there are opportunities for this process to be improved, including enhancing the government's own data sharing apparatus with the private sector. The current asynchronized flow of data, paired with a lack of security clearance for private sector cyber experts, creates a challenging environment for companies trying to prevent ever-evolving cyber threats. Policy makers should prioritize further investment to enhance public-private collaboration and information-sharing, streamline the security clearance process for private sector cybersecurity experts, clarify and simplify cybersecurity reporting guidance and agency requirements, and build coordinated and effective cyber response plans. These efforts will ensure digital networks, including payments networks, have the proper tools at their disposal to prevent future cyber risks.

The definition of covered entity should ensure that critical infrastructure sectors are uniformly held to the same set of reporting standards and focus on the materiality of the incident over the characteristics of the covered entity

As we have seen with recent events, a serious cyber incident need not originate from the largest or most dominant market participants. If compromised, virtually any entity – from a retailer to entities

[1] American Express, Discover, FIS, Fiserv, Mastercard and Visa

within each of the sixteen critical infrastructure sectors identified by Presidential Policy Directive 21 ("PPD-21") – could present a potential threat to U.S. national security, economic stability, or public health and safety. Payments companies (and the financial institutions we work with) continue to expand the use of new and emerging technology to strengthen the resilience of operations. As the threat landscape continues to evolve and PLC members continue to invest in the security and resilience of 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 a firm outside the PPD-21 designation provides non-critical services to a PPD-21 -designated entity and becomes a novel vector for a threat actor to perpetrate a significant 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. This could also include service providers with a material technology relationship to the critical infrastructure entity (cloud service providers, data aggregators, etc.). CISA should also clarify how the resulting covered entity designation distinguishes if at all from other similar terms, both existing and proposed.

The definition of covered cyber incident should align to the NIST definition which is widely used and will support efforts to align to existing cyber incident reporting requirements and frameworks

We encourage CISA to develop definitions that adhere to the NIST framework. As cyber threats evolve, so will efforts to combat threats. 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.

In addition to basing the definition on existing NIST terminology, we encourage CISA to focus on incidents where there is actual harm to the confidentiality, integrity, or availability of an information system or information in a system that is owned and operated by a U.S. entity. This accomplishes the purpose of ensuring that CISA is alerted to significant 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 information.

The definition of substantial cyber incident should include only incidents of a particularly elevated severity.

While a harmonized NIST-based definition is useful to describe a covered cyber incident, it is critical that the definition of a substantial cyber incident align to the statutory intent of this reporting standard and be sufficiently elevated and tailored to ensure that cyber incidents reported to CISA are severe and threatening to U.S. critical infrastructure, not mere technology outages or inconvenient service interruptions. It is equally important to ensure that the covered entity is responsible for

evaluating and determining the materiality relative to the specific facts and circumstances present at the time of the event.

We encourage CISA to consider additional existing language found in the Computer-Security Incident Notification rule[2] to develop its severity characteristics and adopt parts of its definition of a "notification incident" to create a more harmonized definition of a "substantial cyber incident." Using this as a model, CISA should define a substantial cyber incident as one that a covered entity believes in good faith 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 level of materiality will ensure that only the most critical and threatening incidents deserving of CISA's attention are reported for immediate action. Doing so will also contribute significantly to harmonization across various incident notification and reporting requirements the financial services sector, bringing much-needed efficiencies to the reporting process.

Reporting Mechanism – In considering the development of the formal reporting mechanism, we encourage CISA to prioritize accessibility, functionality and simplicity. 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 event. In the event of a particularly severe cyber incident, the ability to securely transmit required incident 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 online reporting portal and form that can be accessible absent exigent circumstances. Prioritizing accessibility, functionality and simplicity will also 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.

"Reasonably Believe" – We recommend that "reasonably believe" (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 covered cyber incident. Speed is critical, especially for an agency in CISA's position seeking to analyze, coordinate, and react to a potential significant cyber event. 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 significant 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.

Reporting Timelines – We are supportive of the CIRCIA requirement that the reporting timeline commence no earlier than 72 hours after determining the occurrence of 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

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

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 covered entities are subject to over 100 different global incident reporting requirements with disparate reporting timelines as soon as six hours or even "without delay." Seventy-two hours is a sufficient period to balance the competing priorities of avoiding distractions from critical work in the early stages of a response and resulting in reports that are premature and likely erroneous and ensuring that information being reported is timely and useful to further 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 there is meaningful transaction data to report and utilize in interagency response efforts.

Supplemental Reporting – Supplemental reports should be submitted upon the determination by the covered entity that circumstances surrounding the incident have changed materially. 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, MNPI) 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.

Harmonization - The payments 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**.** 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 burden on covered entities by advancing common standards for incident reporting.

Substantially Similar Reported Information and Timeframe – CISA should determine that a report provided to another federal entity for the purposes of reporting a cyber event constitutes "substantially similar reported information" if the material essence of the incident is reflected in the information contained within the report to the other federal entity and deem the entity in compliance with CISA's forthcoming rule. However, this should not preclude CISA from engaging directly with the affected covered entity to obtain additional details.

Interagency Utility and Coordination – CISA should maintain or establish interagency channels, especially with Sector Risk Management Agencies (SRMAs) and federal law enforcement, both to avoid redundant reporting and ensure 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" on the back end with other government assets and resources, recognizing patterns and coordinated threat actor activity to respond faster and more effectively to protect critical infrastructure. Including a way for information to be easily shared at the

interagency level while 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, and we urge CISA to provide covered entities with assurances as to its own data security practices and clarity around plans for sharing information with other agencies.

Thank you for the opportunity to provide comments for your consideration. We would be pleased to elaborate on or discuss further any of the comments we have provided.