ITI Promoting Innovation Worldwide

November 14, 2022

Re: ITI Comments Responding to the Cybersecurity and Infrastructure Security Agency's (CISA) Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022

The Information Technology Industry Council appreciates the opportunity to provide feedback responding to the Cybersecurity and Infrastructure Security Agency's (CISA) *Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022.* ITI is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

Cybersecurity and cybersecurity technology are critical to ITI members. Facilitating the protection of our customers (including governments, businesses, and consumers), securing, and protecting the privacy of individuals' data, and making our technology and innovations available to our customers to enable them to improve their businesses are core drivers for our companies. Consequently, ITI has been a leading voice in advocating effective approaches to cybersecurity, both domestically and globally. Cybersecurity is rightly a priority for governments and our industry, and we share the common goal of improving cybersecurity. Further, our members are global companies, doing business in countries around the world. Most service the global market via complex supply chains in which products are developed, made, and assembled in multiple countries around the world, servicing customers that typically span the full range of global industry sectors, such as banking and energy. We thus acutely understand the impact of governments' policies on security innovation and the need for U.S. policies to be compatible with – and drive – global norms, as well as the potential impacts on our customers.

ITI has been deeply engaged in work on cybersecurity incident reporting policy development around the world, including in Australia, Europe, and the United States. As a part of our engagement, we developed and released two sets of policy principles: *Policy Principles for Security Incident Reporting in the U.S.*[1] and *Global Policy Principles for Cybersecurity Incident Reporting*.[2] These documents are intended to help inform and guide policymakers as they consider how to best approach mandatory cyber incident reporting policies and reflect our view of the components that make up a thoughtful approach to incident reporting. We have testified in front of Congress, as well as in front of Australian Parliament on security incident reporting for critical infrastructure and published several additional public-facing pieces that outline our perspectives on incident reporting.

[1] https://www.itic.org/documents/cybersecurity/ITIPolicyPrinciplesonSecurityIncidentReportingFINALJuly2021.pdf
[2] https://www.itic.org/documents/cybersecurity/ITIGlobalPolicyPrinciples-SecurityIncidentReporting.pdf

It is from this global perspective that we encourage CISA, as it develops the rulemaking to implement CIRCIA 2022, to not only examine the existing federal, state, and local incident reporting landscape, but also the international landscape, as there is significant need for alignment across borders. Further, ITI members encourage CISA to emphasize the security objectives of CIRCIA's when developing and implementing the law as it will set a regulatory standard that should inform other federal agencies reporting or disclosure obligations.

At the outset, we also think it important to highlight that in order for the regime to be effective, CISA must triangulate the scope of regulatory coverage, reporting requirements, and processes to ensure that it has the resources, capacity, and capabilities necessary to provide meaningful value to covered entities and the broader cybersecurity community from the information reporting under CIRCIA. To that end, it is vital that CISA articulate its tactical goals and/or plan for actualizing CIRCIA, as only upon understanding what CISA hopes to accomplish with these reports can industry stakeholders provide more specific commentary on key scoping and reporting threshold questions.

1. Section 1: Definitions, Criteria, and Scope of Regulatory Coverage

a. The meaning of "covered entity," consistent with the definition provided in section 2240(5) of the Homeland Security Act of 2002 (as amended), taking into consideration the factors listed in section 2242(c)(1).

At the outset, ITI appreciates Congressional policymakers limiting responsibility for reporting "covered cyber incidents" to owners and operators within the critical infrastructure sectors. Ensuring CIRCIA reports are made by "covered entities" who are the owners and operators of covered entities and not the vendors and third-party service or technology providers protects the supply chain partnerships critical to the cybersecurity ecosystem. As we will discuss in greater detail, a "covered cyber incident" should focus on severe and significant attacks that cause actual disruption or loss. It therefore follows that "covered entities" should be a subset of critical infrastructure owners and operators whose services are most at risk of cyber-attacks that can cause severe and significant actual disruption or loss to national security and essential infrastructure necessary for public health, safety, communications and financial operations.

As CISA begins the process of defining which subset of critical infrastructure entities, as enumerated by PPD-21, are designated as "covered entities" it should consider the following recommendations:

1. Tailor the scope of "covered entities" to ensure CISA has consumable and actionable information. The agency needs to avoid the likelihood of receiving an overwhelming amount of information about a low impact incident that does not satisfy the categories of relevance and risk, or that lacks the ability to provide actionable information because an entity does not have sufficient visibility into an incident.

2. Scoping Should Be Consistent with a National Criticality Assessment. CISA should develop criteria based on criticality assessment to national and economic security when entities are performing national critical functions. For example, the IT and Communications sectors have developed criticality assessments to identify the most critical ICT out of the national critical functions. Such an approach should be encouraged to narrow down when entities are truly carrying out national critical functions that matter to national security, such as satellite communications, versus commercial use cases. If a system is not reasonably tied to a critical function at the national level, then it should not be covered.

3. Ensure transparency when delineating covered entities. While the process that CISA undertakes to assess national risk and identify those entities that should be covered by the requirements of CIRCIA, it will be equally important to ensure "covered entities" are made aware of their status. CISA should identify "covered entities" by name, communicate those entities' covered status, and identify a point-of-contact within the "covered entity" to solidify lines of communication and triage any questions from the "covered entity."

4. Exclude third-parties from the scope of "covered entity". The statutory emphasis that a "covered entity" is the "owner or operator of the information system" (see *e.g.,* Sec. 103) is significant. As the recommended action to CISA's Cybersecurity Performance Goal 5.6 states, "third-parties with demonstrated expertise in (IT and/or OT) cybersecurity regulation validate the effectiveness and coverage of an organization's cybersecurity defenses."[3] Critical infrastructure "owners and operators" need to rely on and trust their technology vendors and service providers. As such, third-parties/third-party vendors should be excluded from the scope of covered entities. Reporting should fall only on the impacted entity itself.

5. Ensure the adoption of common terminology. As the National Infrastructure Advisory Council concluded in 2017, "today's fragmentation of federal cybersecurity capabilities, authorities, missions, roles and oversight is inefficient and precarious. A bold new approach is needed." This finding was part of the rationale for establishing the National Risk Management center to enable cross-sector systematic risk analysis and planning. The NRMC has developed the National Critical Functions (NCF) List[4] to identify and facilitate the assessment of critical infrastructure interdependencies. CISA should establish the NCF as a common lexicon that the interagency can leverage to further its understanding of supply chain risk activities and programs.

6. Finalize ongoing critical infrastructure programs. CISA should continue with its process to designate primary systemically important entities (PSIEs), or otherwise undertake a

[3] https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf
[4] https://www.cisa.gov/national-critical-functions-set

similar process to determine the most critical entities within each critical infrastructure sector in support of President Biden's recent letter to Congress on the Nation's Critical Infrastructure.[5] This will help the agency to narrow the entities that are covered to those that are the *most* critical, which in turn will help manage the volume of reports it receives. If CISA launches a new process in support of the review process outlined in Biden's letter, we encourage it to de-duplicate that process with the ongoing PSIEs effort.

7. Create an exception for entities that are already subject to similar reporting requirements or will be subject to similar reporting requirements in other sectors. Once CISA has undertaken an assessment of entities within the PPD-21 construct that it believes should be "covered entities," to enhance reporting efficiency, reduce regulatory burden, and maximize CISA's limited resources, it should exempt those entities within critical infrastructure sectors that already have or will have similar reporting requirements. Rather, CISA should enter into memoranda of understanding with other critical infrastructure sectors with incident reporting requirements to ensure CISA builds a common operating picture of the most significant and severe cyber incidents. CISA should begin a dialogue with other Sector Risk Management Agencies (SRMAs) now to bake regulatory harmonization into the CIRCIA process at that outset, rather than bolting it on afterwards.

8. Scope "covered entity" to ensure that it covers only U.S.-based subsidiaries of multinational companies. Many companies operate internationally and have headquarters outside of the United States. Given the focus of this rulemaking is on critical infrastructure in the U.S., CISA should ensure that the rule clearly states that a "covered entity" means only a U.S.-based subsidiary that experiences a "covered cyber incident," as opposed to the entire multinational organization.

9. Scope "covered entity" to ensure that it covers only a company's offerings that constitute critical infrastructure. Many companies operate a variety of services and offerings, some of which may reasonably be considered critical infrastructure and some of which may not. The regulation should be scoped so that such companies can be clear about which aspects of their operations are covered and which are not.

10. Exclude manufacturers of consumer products from the scope of "covered entity." Manufacturers of consumer equipment such as cellphones, laptops, printers, routers or other consumer ICT products or consumer-facing software should not be considered covered entities under CIRCIA's reporting obligations. This is primarily to protect against the perception that CISA is encroaching on the average American's privacy and focusing on the IT/OT that supports the subset of the most critical infrastructure entities.

[5] See letter here: https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/07/letter-from-the-president-to-select-congressional-leadership-on-the-nations-critical-infrastructure/

c. *The meaning of "covered cyber incident," consistent with the definition provided in section 2240(4), taking into account the requirements, considerations, and exclusions in section 2242(c)(2)(A), (B), and (C), respectively. Additionally, the extent to which the definition of "covered cyber incident" under CIRCIA is similar to or different from the definition used to describe cyber incidents that must be reported under other existing federal regulatory programs.*

CISA should also consider the federal government's ability to leverage information on "covered cyber incidents" to improve the security and resilience of both the impacted entity and the nation as a whole. We emphasize the benefits of a collective federal response to "covered cyber incidents," as CISA states in the RFI text, "for the express purpose of disrupting threat actors who caused the incident" and "providing technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery." From the perspective of resource maximization, the goal of "bring[ing] malicious actors to justice" should be a secondary priority. Given the potential high-volume of incidents that could be reported under CIRCIA, information sharing and operational collaboration with federal law enforcement and the intelligence community, will have the greatest impact on improving the security and resilience of U.S. critical infrastructure. To ensure greater effective use of limited resources and advanced the RFI's stated objective, CISA should embrace the following principles when developing a definition of "covered cyber incident."

1. Limit reporting to severe and significant attacks that cause actual disruption or loss and include specific parameters. Maintain the key distinction between unexploited vulnerabilities and cyber incidents consistent with CIRCIA reference to international standards (ISO/IEC 29147, 30111).
2. Focus, as much as is practicable, on the impacts of an incident or the cybersecurity consequences of an incident.
3. Emphasize incidents that likely have impacts to cross-sector dependencies or ubiquitously used platforms, services, or products.
4. Calibrate reporting requirements to meet analytical process realities and response capacity.
5. Set a de minimis threshold when considering the functional or information impacts of an incident.
6. Limit "covered cyber incident" to cyber events that occur on U.S.-based networks to exclude networks or systems outside of the jurisdiction of the United States.

We also offer below several other recommendations, which we think will help CISA as it seeks to further define a "covered cyber incident:"

- CISA should leverage the National Cyber Incident Scoring System (NCISS)[6] and the Cyber Incident Severity Schema[7] to develop an objective and repeatable analytical framework to determine the occurrence of a covered cybersecurity incident.

- CISA should seek, to the greatest extent practicable, to enter into memoranda of understanding or other binding agreements with other federal regulators to standardize the terminology around what is, and how to analyze "covered cyber incidents."

- CISA should also consider developing or leveraging an existing an incident reporting matrix, which may help to conceptualize the severity of incidents. As mentioned above, the threshold for what constitutes a "covered cyber incident" should be mapped to specific criteria and specific incident severity levels related to identifiable harms, such as to public health and safety, or operational disruption.[8] An incident categorization model or matrix[9] can represent the severity of an incident more accurately, which will in turn help with determining the threshold for a "covered cyber incident." In developing an incident reporting matrix, we encourage CISA to consider both quantitative and qualitative criteria to determine severity. *Quantitative criteria* could include things like financial loss, impact on customers/employees, or impact on financial markets. *Qualitative criteria* could include things like impact on information systems or services, severe reputational damage to the company, actual breaches of legal or regulatory requirements, data loss caused by the incident, risk posed to the financial health and stability of the covered entity, geographical spread, type/sensitivity of data lost (e.g., PII, trade secrets, etc.)

e. The meaning of "substantial cyber incident."

Consistent with the above, we encourage CISA to view a "substantial cyber incident" through the lens of actual significant harm or material disruption.

h. The meaning of "supply chain compromise," consistent with the definition in section 2240(17).

We generally believe that the statutory definition of "supply chain compromise" in Section 2240(17) is sufficient. Our only additional suggestion would be to ensure the final regulation

[6] https://www.cisa.gov/uscert/CISA-National-Cyber-Incident-Scoring-System

[7] https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf

[8] Currently, the US approach to categorizing cyber incidents in the National Cyber Incident Response Plan defines a "Significant Cyber Incident" as a cyber incident that is (or group of related cyber incidents that together are) likely to result in 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 American people.

[9] Similar approaches have been proposed by CISA and are already adopted by the UK and Australia.

annotates consistency with NIST CNSSI 4009-2015, which defines "supply chain attack" as "attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle." Our contention is that the statutory language and NIST definition are not in conflict, but as previously stated a goal of the CIRCIA regulatory process should be consistency in cyber terminology. It may also be worth considering how to align the definition with the MITRE definition of supply chain compromise, which is somewhat broader.[10]

2. Section 2: Report Contents and Submission Procedures

a. *How covered entities should submit reports on covered cyber incidents, the specific information that should be required to be included in the reports (taking into consideration the requirements in section 2242(c)(4)), any specific format or manner in which information should be submitted (taking into consideration the requirements in section 2242(c)(8)(A)), any specific information that should be included in reports to facilitate appropriate sharing of reports among federal partners, and any other aspects of the process, manner, form, content, or other items related to covered cyber incident reporting that would be beneficial for CISA to clarify in the regulations.*

How covered entities should submit reports. CISA should explore creating a streamlined, secure/encrypted interface by which covered entities can submit incident reports. It would be helpful for this interface to be web-based and to contain a standardized set of fields that entities need to respond to. Ideally, such a template would align with existing frameworks with broad adoption, like MITRE ATT&CK or VERIS. This was a recommendation that we explored further in our Global Incident Reporting Policy Principles. In our view, this approach is preferable to CISA receiving a plethora of emails from impacted entities. However, it would also be helpful for CISA to consider other avenues for reporting so in case the web interface goes down, there is other ways for covered entities to submit reports. We encourage CISA to allow the secure, web-based form to be printed/saved following the submission, and provide an email or telephone number that can be used.

Specific information that should be required to be included in reports. We believe that the requirements set forth in Section 2242(c)(4) are largely sufficient for an initial incident report. We appreciate that several of the information categories proposed in CIRCIA are delineated as "where appropriate," since such information may not be available in every instance. It may also be helpful for CISA to consider a few additional categories of information, including:

- Whether the entity requires specific support from DHS/CISA
- How DHS/CISA can best support the impacted entity
- Whether the incident has been reported to CERT, CSIRT, FBI, Sector-Specific Agencies, Local Authorities, or International Entities

[10] See MITRE definition here: https://collaborate.mitre.org/attackics/index.php/Technique/T0862

Covered entities should also **have the option to voluntarily report additional types of information on cybersecurity incidents**. This can help to address emerging trends or otherwise preempt attacks.

b. What constitutes "reasonable belief" that a covered cyber incident has occurred, which would initiate the time for the 72-hour deadline for reporting covered cyber incidents under section 2242(a)(1).

In our view, "reasonable belief" should be understood to mean a confirmed cybersecurity incident. Security event investigations should have progressed to a point that indicators of actual loss or harm to covered entities have been identified. Entities should not be made to report on "potential" cybersecurity incidents, on incidents that have not yet been confirmed, or on incidents that have not resulted in actual loss or harm.

c. How covered entities should submit supplemental reports, what specific information should be included in supplemental reports, any specific format or manner in which supplemental report information should be submitted, the criteria by which a covered entity determines "that the covered cyber incident at issue has concluded and has been fully mitigated and resolved," and any other aspects of the process, manner, form, content, or other items related to supplemental reports that would be beneficial for CISA to clarify in the regulations.

It is our view that supplemental reports should be submitted in the same format as initial reports, using the same streamlined interface recommended previously. Supplemental reports should be submitted when new and different information becomes available. For example, oftentimes early on in an investigation, impact may not be known. Or, throughout the course of the investigation of the incident, the impacted entity's initial assessment of the impact may change. In those cases, it would be reasonable for that entity to submit a supplemental report.

d. The timing for submission of supplemental reports and what constitutes "substantial new or different information," taking into account the considerations in section 2242(c)(7)(B) and (C) and e. what CISA should consider when "balanc[ing] the need for situational awareness with the ability of the covered entity to conduct cyber incident response and investigations" when establishing deadlines and criteria for supplemental reports.

CISA should remain flexible as to when supplemental reports can be submitted. That being said, such reports should not be required sooner than 60-90 days after the initial incident notification. Following this, additional supplemental reports could be provided if and when new information is discovered.

In considering supplemental reporting, we also encourage CISA to create a mechanism by which entities may be able to deescalate an initial incident report should they further investigate and

conclude that the incident is not actually substantial, and therefore, does not constitute a "covered cyber incident."

f. Guidelines or procedures regarding the use of third-party submitters, consistent with section 2242(d).

Should third-party submitters be used, we encourage CISA to consider creating some sort of mechanism by which third-party submitters can register and be verified. CISA should also consider the potential for self-interested parties or business competition to submit reports on or involving competitors and craft guardrails to avoid such misuse of the provision. This could be achieved through explicitly barring third-party reports from anonymous sources.

3. Section 3: Other Incident Reporting Requirements and Security Vulnerability Information Sharing

a. Other existing or proposed federal or state regulations, directives, or similar policies that require reporting of cyber incidents or ransom payments, and any areas of actual, likely, or potential overlap, duplication, or conflict between those regulations, directives, or policies and CIRCIA's reporting requirements & b. what federal departments, agencies, commissions, or other federal entities receive reports of cyber incidents or ransom payments from critical infrastructure owners and operators.

Our member companies are subject to multiple incident reporting requirements at the state and federal level in the U.S., as well as numerous global regulations. In particular, we point CISA to our recently released memo, which highlights key incident reporting policy proposals around the world.[11] Many are still under development, but the incident reporting obligations in the EU's NIS2, the new proposal for EU Cyber Resilience Act, as well as in Australia's *Security Legislation Amendment (Critical Infrastructure) Bill 2021* have been finalized. With that in mind, we encourage CISA to not only evaluate the U.S. incident reporting landscape but also the international landscape.

Below, we have outlined several key provisions in both pieces of legislation that CISA should be aware of. Inclusion of these provisions does not indicate our support for a similar approach, but merely that CISA may want to consider these regulations in addition to those in the United States to foster interoperability to the extent possible and appropriate. In fact, as a general matter, we have encouraged other nations considering incident reporting obligations to look to CIRCIA as a starting point.

[11] Cybersecurity Incident Reporting Memo, available here: https://www.itic.org/news-events/news-releases/iti-releases-2022-2023-global-cybersecurity-incident-reporting-policy-index

Europe - NIS2[12]

Scope: Essential and important entities as defined in Annex I and II and meet or exceed the threshold for medium-sized enterprises within Recommendation 2003/361.

Threshold & Timeline: It is worth considering how the threshold for reporting is defined in NIS2, which requires a report for any incident having a significant impact on the provision of the services. NIS2 requires that an essential or important entity provide an "early warning" report of an event within 24 hours after becoming aware of the incident, to be followed up with a more formal incident notification 72 hours after becoming aware of the same incident. It also requires entities to submit a final report no later than one month after the incident notification is made.

- **Definition of significant impact:** (a) the incident has caused or is capable of causing severe operational disruption of the service or financial losses for the entity concerned; (b) the incident has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material losses.[13]

Definition of incident: Any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.[14]

Contents of report: In the "early warning" report, entities must only specify whether the incident is presumed to be caused by unlawful or malicious actors. The follow-up incident notification must include additional detail, updating any information provided in the "early warning" report, and offering an initial assessment of the incident, its severity and impact, and any indicators of compromise. The final report should be even more fulsome, including a detailed description of the incident, its severity, and impact; the type of threat or root cause that led to the incident; applied and ongoing mitigating measures; and where applicable, any cross-border impacts of the incident.[15]

ITI has offered specific thoughts on the NIS2 Directive throughout its development and encourage CISA to review our perspectives on the legislation.[16]

[12] See NIS2 Political Agreement here: https://data.consilium.europa.eu/doc/document/ST-10356-2022-INIT/en/pdf
[13] Ibid, Article 20(3).
[14] Ibid, Article 4.
[15] Ibid, Article 20(4).
[16] See ITI recommendations here: https://www.itic.org/documents/europe/ITINIS2TrilogueNegRecommendedTextFINAL.pdf; ITI's initial position here: https://www.itic.org/documents/europe/ITINIS2ProposalComments18032021%282%29%5B1%5D.pdf;

Australia - Security Legislation Amendment (Critical Infrastructure) Bill 2021[17]

Scope: The CI Bill of 2021 expanded the scope of covered entities to 11, with the notable inclusion of data storage or processing asset, which we highlighted our concerns with in our comments and a multi-association letter to the Australian Government, as well as in our testimony before the Australian Parliament.[18] Other critical assets include telecommunications, broadcasting, domain name systems, banking, superannuation, insurance, financial market infrastructure, water, electricity, gas, energy market operators, liquid fuel, hospital, education, food and grocery, port, freight infrastructure, freight services, public transport, aviation, and defence industry.

Threshold & Timeline: Also notable is the fact that the impacts of incidents are defined in two ways – significant and relevant – with incidents having a significant impact being reported within 12 hours, and incidents having a relevant impact being reported within 72 hours.

- **Definition of significant impact:** The legislation defines a significant impact as an impact on the availability of the asset "if and only if: (a) both the asset is used in connection with the provision of essential goods and services; and the incident has *materially* disrupted the availability of those essential goods and services, and (b) any of the circumstances specified in the rules exist in relation to the incident."[19]

Definition of cybersecurity incident: "One or more acts, events or circumstances involving any of the following: unauthorized access or modification to computer data or to a computer program; unauthorized impairment of electronic communication to or from a computer or the availability, reliability, security or operation of a computer, computer data, or a computer program."[20]

United States

SEC Proposed Rule on Cybersecurity Risk Management, Strategy, and Governance[21]

In the U.S., the Securities and Exchange Commission Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (RIN 3235-AM89; File Number S7-09-22) has raised particular concern. While we support SEC's intent to improve investors' awareness of material cybersecurity incidents and believe that in many instances offering information about cybersecurity incidents and governance procedures can help to improve transparency, we also have concerns with the way the proposed rule is currently written,

[17] See Part 3A of Security Legislation Amendment (Critical Infrastructure) Bill 2021 here: https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6657_aspassed/toc_pdf/20182b01.pdf;fileType=application%2Fpdf

[18] See ITI comments here: https://www.aph.gov.au/DocumentStore.ashx?id=04c36c84-3067-4ffb-bec2-53c780079a02&subId=701444 and multi-association letter here: https://www.itic.org/documents/asia-pacific/LtrAUGovCIBill_ITI_10.13.21.pdf. See opening statement here: https://www.aph.gov.au/DocumentStore.ashx?id=c0a572da-ec83-4e8c-9b78-529e4e0fdc95&subId=701444

[19] Ibid, Part 1, Article 30BEA.

[20] Ibid, Part 1, Article 12M.

[21] See SEC Proposed rule here: https://www.sec.gov/rules/proposed/2022/33-11038.pdf

including the fact that it could lead to disclosure of unmitigated vulnerabilities and that it may precede and thus overlap with the CISA rulemaking to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA 2022). As a result, ITI has urged the SEC to delay implementation of the proposed rule to provide the SEC and stakeholders the opportunity to work through these challenges and allow the SEC the time to coordinate with the Cybersecurity and Infrastructure Security Agency (CISA) to deconflict the proposed rule with the forthcoming regulations to implement CIRCIA 2022. Such reporting (of unmitigated vulnerabilities) is further inconsistent with international standards and industry best practices for vulnerability handling and disclosure, endorsed in CIRCIA, federal law (e.g., the IoT Cybersecurity Improvement Act), and CISA BOD 20-01.

That being said, this is not the only potential incident reporting requirement that exists. There are at least 25 other federal cybersecurity incident reporting requirements, and even more at the state/local level. We highlight several below that it would be useful for CISA to consider:

DFARS Clause 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting

Scope: This DFARs clause requires contractors for the Department of Defense to report cyber incidents against "covered defense information" and/or "covered contractor information systems."

Threshold & Timeline: Covered contractors must report an incident when it "affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical."[22] Such incidents must be reported to the DoD within 72 hours of discovery.

Definition of cyber incident: A cyber incident is defined as "actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein."

DFARS Clause 252.239-7010: Cloud Computing Services[23]
Scope: This DFARs clause requires contractors who provide cloud computing services to the DoD or who use cloud-computing services to report "all cyber incidents that are related to the cloud computing service provided" to the DoD.

Threshold & Timeline: The threshold is fairly broad, indicating that "all cyber incidents *related* to the cloud computing service" be reported. The timeline for reporting is also unclear from the text.

[22] See DFARS Clause here: https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
[23] See DFARS Clause here: https://www.law.cornell.edu/cfr/text/48/252.239-7010

Definition of cyber incident: The definition of cyber incident is the same as the one outlined above.

FAR 2021-017 – Cyber Threat and Incident Reporting Information Sharing (*in progress)*[24]

The Federal Acquisition Regulations are being updated pursuant to the *Executive Order on Improving the Nation's Cybersecurity* to include provisions on incident reporting and threat sharing. All ICT service providers who enter into a contract with federal civilian executive branch agencies must report cybersecurity compromises to those agencies and to CISA.

The text of the rule is still forthcoming, so timeline and threshold remain undetermined at this time. It is also unclear how cybersecurity incident will be defined. However, it will be crucial for CISA to leverage the Cyber Incident Reporting Council to streamline requirements for critical infrastructure owners and operators with the requirements placed on federal contractors, as in some cases, these entities may overlap.

Computer Security Incident Notification Requirements for Banking Organizations and their Bank Service Providers[25]
Scope: The rule covers banking organizations and banking service providers.

Threshold and Timeline: The rule requires covered organizations to report a "notification incident" no later than 36 hours after it has been determined that an incident has occurred. This threshold in particular may offer CISA insight into how to scope "covered cyber incidents" as it differentiates a "computer-security incident" from a "notification incident" (which, in our read, is a more severe incident).

- *Computer-security incident* is defined as "an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores or transmits."
- *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 ability to carry out banking operations…business lines that upon failure would result in a material loss of revenue, profit or franchise value."

The above list is not exhaustive but is instead illustrative of just a few of the incident reporting policies that exist at the federal level. Other research groups have developed robust catalogues of reporting requirements at the federal level that may be useful for CISA to review throughout the course of the rulemaking.[26]

[24] See open case here: https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=9000-AO34
[25] 12 CFR Part 53 Office of the Comptroller of the Currency. Effective April 1, 2022
[26] See, for example, *R Street Institute's* Cyber Incident Reporting Catalogue here: https://www.rstreet.org/wp-content/uploads/2022/07/federal-cyber-incident-breach-reporting-072822-1.pdf.

Above all else, we encourage CISA to leverage the Cyber Incident Reporting Council created under CIRCIA to further identify, track, and analyze the contents of each of the incident reporting policies in order to facilitate regulatory streamlining.

> *h. Principles governing the timing and manner in which information relating to security vulnerabilities may be shared, including any common industry best practices and United States or international standards.*

Vulnerabilities are distinct from incidents. If exploited, in certain cases, vulnerabilities may constitute an incident, but generally that is not the case. The goal of vulnerability handling processes is to limit the potential harm to end users by developing mitigations and releasing them to prevent exploitation. Common industry standards and best practices for coordinated vulnerability disclosure include ISO/IEC 29147 and 30111. These standards appropriately limit and protect information disclosed to entities essential to the CVD process, prior to public disclosure, and are endorsed by Congress and CISA alike (see the IoT Cybersecurity Improvement Act, CIRCIA and DHS CISA BOD 20-01).

> *j. Covered entity information preservation requirements, such as the types of data to be preserved, how covered entities should be required to preserve information, how long information must be preserved, allowable uses of information preserved by covered entities, and any specific processes or procedures governing covered entity information preservation.*

We raise for CISA's consideration the fact that when a company is finished remediating an incident, they do not often retain said information unless they are subject to a legal hold. It is extremely costly to retain information. We caution against imposing overly burdensome information preservation requirements that would put a company or organization in a situation where they have to choose between preserving a firewall appliance and maintaining a large number of server images on the off chance that the information *may* be needed at some undetermined point in the future. We also encourage CISA to lay down additional data privacy safeguards to ensure that the sensitive information reported by the entities is protected. A list of agencies who will receive access to this information should be shared.