U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

November 14, 2022

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Washington, DC 20528

Dear Director Easterly:

Re: Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Docket No. CISA-2022-0010)

The U.S. Chamber of Commerce welcomes the opportunity to comment on the Cybersecurity and Infrastructure Security Agency's (CISA's) request for information (RFI) on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). We appreciate the engagement that CISA has had with the Chamber on this law and the forthcoming rule.[1]

The Chamber especially recognizes CISA's engagement with industry on a number of the programmatic details, such as the definitions and the contents of reports. CISA's recent outreach to the business community has incorporated nearly a dozen public listening sessions—including in Salt Lake City and Kansas City—to receive input on the best approaches to implementing various aspects of the agency's new regulatory authority under CIRCIA.[2]

The Chamber does not attempt to address each question in the RFI, which covers an array of topics that will take more time than the comment period to fully consider and offer a response. Instead, we offer input on key themes and specific issues (e.g., see Appendix I) that tend to be spotlighted by several industry organizations.

---

[1] Cybersecurity and Infrastructure Security Agency (CISA), "Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022," *Federal Register*, September 12, 2022. https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022

[2] CISA, "Cyber Incident Reporting for Critical Infrastructure Act of 2022 Listening Sessions," *Federal Register*, September 12, 2022. See Appendix III.
https://www.federalregister.gov/documents/2022/09/12/2022-19550/cyber-incident-reporting-for-critical-infrastructure-act-of-2022-listening-sessions
https://www.federalregister.gov/documents/2022/10/05/2022-21635/cyber-incident-reporting-for-critical-infrastructure-act-of-2022-washington-dc-listening-session

(B)(1) Definitions, Criteria, and Scope of Regulatory Coverage

(B)(1)(a) The meaning of "covered entity"

- According to CIRCIA, a "covered entity" refers to "an entity in a critical infrastructure sector" that is defined in Presidential Policy Directive 21 (PPD 21)[3] and that also satisfies the definition established by CISA. PPD 21 identifies 16 critical infrastructure sectors and designates associated federal sector risk management agencies (SRMAs).

- CIRCIA further says that the definition of a covered entity will be established by a rule, which must include a clear description of the types of entities that constitute covered entities, based on—

    - The consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety.
    - The likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country.
    - The extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

- CISA should adopt a prioritized, risk-based approach to assess the criticality of the operations and functions of a covered entity. The agency should not rely on the open-ended definition of a covered entity in CIRCIA (section 2240(5)), which notionally includes all entities in the 16 critical infrastructure sectors. Specifically, the definition of covered entities should be tightly construed to include only those entities whose operations and functions pose an immediate, high-level risk with severe and adverse consequences to national security. economic security, or public health and safety.

- The Chamber believes that the scope of covered entities—including a subset of critical infrastructure—could be overly broad from a risk management perspective. For CIRCIA to have a chance at effectiveness, CISA should establish criteria in the rule that creates a narrow list of covered entities within a critical infrastructure sector that, if impacted, would create significant consequences within the U.S. Otherwise, receipt of reports from a large number of entities with different reporting standards could risk creating unintended noise in the system that detracts from protecting critical infrastructure.

---

[3] PPD 21, *Critical Infrastructure Security and Resilience*, February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

(B)(1)(b) The number of entities, either overall or in a specific industry or sector, likely to be "covered entities"

- It is in the interest of both industry and CISA for the agency to take an incremental approach to covering private organizations. A list of covered entities should be limited in reach and risk based. Rather than focus on an elusive number of entities to cover, the Chamber urges CISA to focus on the types of significant cyber incidents that it wants covered critical infrastructure to report. In other words, consideration should be given to placing emphasis on the incident—a significant incident—rather than the entity.

- By following the criteria set forth in CIRCIA, CISA is empowered to create a narrow list of covered entities. CISA should not take on more than it can handle. With an eye toward fostering an effective and collaborative reporting program, the rule should emphasize a focused list of covered entities that is both realistic and achieves policymakers' goals.

- Indeed, a disciplined, risk-oriented approach would advance CISA's goal of moving from traditional public-private partnerships to public-private operational collaboration.[4]

(B)(1)(c) The meaning of "covered cyber incident"

- CIRCIA bill writers did not want CISA to be overwhelmed with a flood of unusable cyber incident data because of overly broad and prescriptive reporting by covered entities.

- To enhance the efficiency of a reporting program, a covered cyber incident should be triggered only when there exists a significant incident with a reasonable likelihood of harm to U.S. economic and national security. A significant cyber incident would demand unity of effort within the government and especially close coordination between the public and private sectors, such as the activities called for under the PPD 41 framework.[5]

---

[4] Testimony of Jen Easterly, CISA director. House Homeland Security Committee hearing on "Evolving the U.S. Approach to Cybersecurity: Raising the Bar Today to Meet the Threats of Tomorrow," November 3, 2021. https://homeland.house.gov/activities/hearings/evolving-the-us-approach-to-cybersecurity-raising-the-bar-today-to-meet-the-threats-of-tomorrow

[5] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

- CISA should thoughtfully set a high threshold for an incident to be considered reportable. Otherwise, the agency risks being inundated with a high volume of low-impact reports, which would be a misuse of public and private organizations' resources. The focus should be on high-impact incidents that would result in an actual disruption or loss to national or economic security, foreign relations, and public safety and health.

- The Chamber believes that covered cyber incidents should be limited to ones that directly disrupt the operation of U.S. critical infrastructure owned and/or operated by a covered entity and would not extend to incidents affecting noncritical or ancillary systems.

- For the reporting program to be effective nationally, incident reporting requirements should be limited to companies' domestic operations. Otherwise, both covered multinational entities and CISA could be burdened with cyber reporting that does not directly affect U.S. economic and national security interests.

- The rule should also be scoped to clearly exclude noncyber threats to infrastructure, such as physical threats from extreme weather, accidental damage, and inadvertent disclosures of personally identifiable information (PII) by covered entities' personnel.

(B)(1)(e) The meaning of "substantial cyber incident"

- The Chamber believes that reporting should be geared toward significant and relevant incidents—the point being that the bar should be set high for the types of incidents that CISA would determine to be reportable.[6]

- Unlike the term "significant cyber incident," the term "substantial" is not defined in the legislation. CIRCIA only says that a "covered cyber incident" refers to a "substantial cyber incident experienced by a covered entity that satisfies the definition and criteria" established by CISA under the rule.

- During the writing of CIRCIA, the Chamber stressed to lawmakers that the word substantial would be unworkable in practice. Substantial is neither defined in law nor policy (e.g., PPD 41). However, both law and policy specifically refer to a significant cyber incident. Substantial is problematic because it could be used by CISA to label almost any cyber incident as covered. Such a lack of definitional discipline would make establishing and implementing a new cyber incident reporting program challenging. In essence, trying to potentially wedge a substantial cyber incident between a cyber incident and a significant cyber incident would be a recipe for confusion and frustration.

[6] https://www.uschamber.com/security/cybersecurity/coalition-letter-cyber-incident-reporting

Definitions of Cyber Incident and Significant Cyber Incident in PPD 41

Cyber incident. An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Significant cyber incident. 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.

Definition of Significant Cyber Incident in CIRCIA

"**(16) SIGNIFICANT CYBER INCIDENT.**—The term 'significant cyber incident' means a cyber incident, or a group of related cyber incidents, that the Secretary determines is 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 people of the United States.[7]

- Reporting a vast number of cyber events of comparatively little importance could easily overwhelm CISA. Businesses should not be reporting insignificant or immaterial cyber activity when reports on harmful incidents are needed most by stakeholders.

- Information that is required to be reported should be credible, verifiable, and actionable and only include information that is necessary for other organizations to take appropriate mitigation actions.

- The compromise of a supply chain alone should not be considered a substantial cyber incident without also causing "an unauthorized access or disruption of business or industrial operations due to loss of service."[8] Additionally, the focus of CIRCIA should be on first-party reporting by covered entities and not their vendors or customers.

[7] CIRCIA, section 2240(16), 136 STAT. 1040.

Also, by way of comparison, H.R. 5440, the Cyber Incident Reporting for Critical Infrastructure Act of 2021, tied the term "covered cybersecurity incident" to the term "significant cyber incident." https://www.congress.gov/bill/117th-congress/house-bill/5440/text

[8] The wording "an unauthorized access or disruption of business or industrial operations due to loss of service" is taken from CIRCIA section 2242(c)(2)(iii), 136 STAT. 1045.

(B)(2) Report Contents and Submission Procedures

(B)(2)(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

(B)(2)(h) 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

- CISA should ensure that reasonable belief is rooted in a covered cyber incident that actually occurs. Reasonable belief should also be based on the information that is known to the covered entity at the time of the incident. Owing to the fog of incident response, complete certainty that an incident meets the criteria of a covered cyber incident is unrealistic.

- On the one hand, an entity may reasonably conclude that it is highly likely that an incident meets the criteria of a covered cyber incident when it may not have. Some entities may want to amend their initial reporting to indicate that a covered cyber incident did not, in fact, occur. On the other, requiring certainty that an actual incident has occurred is sensible and beneficial. Reporting false positives where it is ultimately determined that there is no covered incident would be wasteful and confusing and would not further our collective cybersecurity goals.

- The rule should maintain a prompt reporting timeline of not less than 72 hours. The 72-hour deadline reflects a flexible standard for notifying CISA about a significant cyber incident. Covered entities need time to investigate an intrusion before making a determination that a covered incident occurred, including reporting it to the government. Covered entities should report an incident after conducting initial mitigation and response efforts. Even relatively minor cyber incidents can absorb hundreds of personnel hours to accurately assess.

- The Chamber holds that the rule should link reporting to confirmed cyber incidents. Businesses need clarity in reporting requirements, which should be targeted to well-defined and verified cyber incidents. Legislative language that the Chamber has considered (e.g., "potential cyber intrusions") would likely be unworkable in practice. Comparatively loose definitions would yield extraneous information that does not improve the situational awareness of CISA and other critical infrastructure organizations.

- Covered cyber incidents need to be attached to clear, objective criteria in any rule that agency and industry stakeholders jointly develop. The 72-hour notification clock should begin when a covered entity has forensically completed an initial assessment of a covered cyber incident.

- Bill writers wanted to ensure "adequate time for investigation and evaluation of an incident to determine whether it is a cyber incident that rises to the level of being a covered cyber incident, all before the 72-hour clock starts."[9]

- From detection to determination, the victim entity needs to decide for itself whether/when it has been impacted by a covered cyber incident. Covered entities need time to follow their own cybersecurity incident and vulnerability response playbooks. In most cases, businesses will not have a complete picture of the (confirmed) cyber incident and its actual or potential effects in the immediate hours following its discovery.

- Covered entities need sufficient time to conduct an investigation, including taking steps to contain and mitigate the compromise of networks and systems and undertake further forensic work to understand the true scope and impact of the incident. These steps, among others, are necessary if early notification and supplemental reporting under CIRCIA will add value to the cybersecurity of industry and the U.S. In a similar way, agencies determine the level of impact of a cyber incident by using incident management processes established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, *Computer Security Incident Handling Guide*.[10]

Reporting a Substantial Cyber Incident
A substantial cyber incident is also significant and confirmable;
it starts the 72-hour reporting clock

- In writing CIRCIA, Congress was clear that the definition of a "substantial cyber incident" should be set at a level to not flood CISA with unnecessary reporting. In other words, comparatively routine occurrences of malicious cyber activity should not be reported.

- A rational definition of "incident" in the cybersecurity context is found in 6 U.S. Code § 659, which defines an incident as an "occurrence"—not merely a hypothetical event—and such an occurrence must "actually or imminently" cause one of the enumerated jeopardies to information or information systems without lawful authority.[11] As a threshold matter, any

[9] Senate Homeland Security and Governmental Affairs Committee paper, "Peters-Portman Cyber Incident Reporting Act Overview," circa September 30, 2021.

[10] Additional federal resources include CISA's *Cybersecurity Incident & Vulnerability Response Playbooks*, November 2021.
https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Office of Management and Budget (OMB) memorandum M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*, November 19, 2019.
https://www.whitehouse.gov/wp-content/uploads/2019/11/M-20-04.pdf

[11] 6 U.S. Code § 659(a)(5) ("[T]he term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an

cyber event that fails to meet this basic definition of "incident" should not be considered a substantial cyber incident.

- To avoid confusion and inconsistent interpretations by policymakers and stakeholders, the term "substantial cyber incident" should address the same areas of concern as a "significant cyber incident," as found in PPD 41. Namely, a covered cyber incident would 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."[12]

- The 72-hour notification clock should begin when a covered entity has forensically completed an initial assessment of a covered cyber incident.

(B)(2)(a) How covered entities should submit reports on covered cyber incidents

(B)(2)(f) How covered entities should submit supplemental reports

(B)(2)(g) The timing for submission of supplemental reports

- For the purposes of writing a rule to implement CIRCIA, the initial report or notification to CISA or a covered entity's sector risk management agency (SRMA) should serve as a high-level alert within 72 hours after a covered entity confirms a significant cyber covered incident.

- CISA should ensure that an entity's resources are deployed toward mitigating the incident and not consumed with granular reporting. CISA should focus on being notified about significant incidents with high-level impacts, such as threats to economic stability, public health and safety, and national security. Covered entities should be incentivized to sound the alarm as quickly as possible without being bogged down in time-consuming reporting.

- Supplemental reporting refers to a more detailed analysis of the incident and its impact, which is submitted to CISA after a covered entity assesses (e.g., conducts a root-cause analysis) and meaningfully mitigates an incident.

- Reporting forms or templates should be harmonized across agencies to reduce duplicative or conflicting requirements, as well as to make reported data increasingly consistent and easy to analyze.

---

information system, or actually or imminently jeopardizes, without lawful authority, an information system").
https://www.law.cornell.edu/uscode/text/6/659

[12] PPD 41, *United States Cyber Incident Coordination*, July 26, 2016.
https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

- The following table provides preliminary feedback on how covered entities should submit reports on covered cyber incidents, how they should submit supplemental reports, and the timing of supplemental reports.

Policy Objective	**Requirements**	
	Timing	**Contents**
Report or notification	A high-level notification to CISA or a covered entity's SRMA within 72 hours after establishing that a significant, or a covered, cyber incident has occurred.	CIRCIA calls for certain information," to the extent applicable and available" on a covered cyber incident, including— • The covered entity's identity and contact information. • An identification and a description of the affected information systems or devices **(qualitative information)**. • A description of the unauthorized access with substantial loss of cybersecurity of the affected information systems or the disruption of business/industrial operations **(qualitative information)**. • The estimated date of the incident. • The impact on the operations of the covered entity **(qualitative information)**. • Where applicable, a description of the vulnerabilities exploited and the security defenses that were in place **(qualitative information)**. • Where applicable, information identifying (e.g., IP addresses, emails) the responsible malicious actor(s).[13]

[13] CIRCIA section 2242(c)(4), 136 STAT. 1045–1046.

Supplemental Report	A more detailed analysis of the covered cyber incident and its impact is submitted to CISA after a covered entity assesses (e.g., conducts a root cause analysis) and meaningfully mitigates the incident within reasonable period of time, but no fewer than 30 days.[14]	Under CIRCIA, a covered entity must "promptly submit" to CISA an update to a previously submitted report if "substantially new or different information" becomes available until the covered entity notifies CISA that the incident has been resolved.[15] Information that a covered entity is likely to include in a supplemental report is— • A root-cause analysis to eliminate or mitigate adversary access to the network. • The vector of attack. • The level of impact (more detailed than the initial notification). • The impacted information, which may include the types of data lost, compromised, or corrupted. • The scope of time and resources needed to recover from the incident. • Adversary signatures; tactics, techniques, and procedures; indicators of compromise; and hashes.

- CISA should center its reporting requirements to solicit actionable, useful information from covered entities. CIRCIA section 2242(c)(4) requires covered entities to disclose much qualitative information about a reportable incident, such as a description of the function of an affected information system, the details surrounding the unauthorized access to a network, and the corresponding impacts. This information is often not easy to immediately obtain, and it can be highly sensitive.

[14] According to the OMB, agencies must supplement their 7-day notification to Congress about a major incident with another report no later than 30 days after the agency discovers a major incident. See OMB memorandum M-20-04, p. 7.

[15] CIRCIA section 2242(a)(3), 136 STAT. 1043.

- Since the available information about a (covered) cyber incident would be evolving, and sufficient time is required to assess whether an attack was successful, reporting such information within the prescribed timeline (72 hours) is unlikely to help CISA in its review and analysis. Instead, CISA should want to acquire basic and targeted information that can be immediately reviewed and, following the decision that a covered cyber incident happened, a more detailed report can be shared with appropriate parties while minimizing disruption to incident response efforts.

- As CISA undertakes its rulemaking process to implement the statutory requirements in CIRCIA, the Chamber believes that the agency should not try to depart from existing practices. CISA's form *Sharing Cyber Event Information: Observe, Act, Report* captures 10 elements that stakeholders should share about cyber-related events:

    - Incident date and time.
    - Incident location.
    - Type of observed activity **(qualitative information)**.
    - Detailed narrative of the event **(qualitative information)**.
    - Number of people or systems affected.
    - Company/organization name.
    - Point of contact details.
    - Severity of event **(qualitative information)**.
    - Critical infrastructure sector if known.
    - Anyone else you informed.[16]

- CISA's comparatively simple cyber incident reporting form focuses on gathering the essentials—an organization's contact information and basic details, a description of the incident, and the nature of the incident's impact.[17] CISA should keep the required contents of a report submitted in the first 72 hours as simple as possible, particularly regarding information that is qualitative in nature.

(B)(2)(i) Guidelines or procedures regarding the use of third-party submitters

- Under CIRCIA, there is no requirement for third-party reporting, but rather an allowance for third parties to report at the request of a covered entity. A main thrust behind the optional third-party reporting is to help covered small and midsize businesses, among other covered entities. Such entities may not have the resources or capabilities to comply with the requirements in a timely manner. CIRCIA allows them to leverage the expertise of incident response firms and others to report on their behalf.

---

[16] https://www.cisa.gov/sites/default/files/publications/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf

[17] https://www.cisa.gov/report

- According to the underlying statute, the duty to report (section 2242(d)(3)) is the responsibility of the covered entity. This section does not mandate any reporting requirements for third-party entities that are not considered covered entities as defined by CIRCIA.

- The only requirement (section 2242(d)(4)) is that a third party that makes a ransomware payment on behalf of a covered entity must advise the covered entity of the obligation to report the ransomware payment under section 2242(a)(2).

(B)(2)(j) Covered entity information preservation requirements

- The Chamber defers to sector-based organizations to recommend how information should be preserved based on existing laws, regulations, and guidance.

(3) Other Incident Reporting Requirements and Security Vulnerability Information Sharing

(B)(3)(a) Other existing or proposed federal or state regulations, directives, or similar policies that require reporting of cyber incidents or ransom payments

- The list of international, federal, and state cyber incident reporting requirements in this area is immense. CISA should work with sector-based organizations to compile key regulations, directives, and similar policies to identify them as candidates for harmonization.

(B)(3)(b) What federal departments, agencies, commissions, or other federal entities receive reports of cyber incidents or ransom payments

- The Chamber defers to sector-based organizations to provide the listing requested here.

(B)(3)(f) Criteria or guidance CISA should use to determine if a report provided to another federal entity constitutes "substantially similar reported information"

- The Chamber was pleased to host DHS officials on October 6 to discuss the Cyber Incident Reporting Council (CIRC). The CIRC has spent considerable time looking at best practices and opportunities to better align definitions of reportable incidents, the thresholds for reporting, and the content of reports. These are areas of focus that the Chamber and DHS/CISA should continue to discuss.

- Many defense industrial base (DIB) contractors, for example, report cyber incidents through the Defense Industrial Base (DIB) Cybersecurity Portal (as required by DFARS

252.204-7012),[18] which would meet the "substantially similar" requirement, thus eliminating the need to report cyber incidents twice. CISA should consider DIB Cybersecurity Portal reporting as sufficient to meet the needs of CIRCIA. It would align with how a large segment of government contractors already do business and have processes in place to comply with similar reporting cyber incidents.[19]

- CISA should make it easy for covered entities to report covered cyber incidents to the government by having a common pathway in which to report cyber incidents. Adhering to multiple reporting timelines, details, and portals is costly and draws contractors' focus away from the real priority—investigating, containing, and remediating cyber incidents.

(B)(3)(g) What constitutes a "substantially similar time frame" for submission of a report to another federal entity

- The Chamber believes that reporting time frames ranging from 24 hours to 72 hours should default to 72 hours. Otherwise, there needs to be a connection between the urgency of the reporting and the government's readiness to disrupt or degrade the actions of malicious actors.

(B)(3)(h) Principles governing the timing and manner in which information relating to security vulnerabilities may be shared

- To reduce the risk of exploitation by malicious actors, information concerning vulnerabilities should be kept in strict confidence during the coordinated vulnerability disclosure (CVD) and handling process until mitigations are publicly available. These practices are embodied in binding operational directives issued by CISA and international standards for CVD, as well as endorsed by Congress.[20]

---

[18] https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting

[19] https://dibnet.dod.mil

[20] CISA, "New Federal Government Cybersecurity Incident and Vulnerability Response Playbooks," November 16, 2021.
https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability

See the IoT Cybersecurity Improvement Act of 2020 (P.L. 116-207).
https://www.congress.gov/bill/116th-congress/house-bill/1668

Any requirements related to patching should be developed in a manner consistent with industry best practices and international standards (e.g., ISO/IEC 30111, 29147) for coordinated vulnerability handling and disclosure and CISA's Binding Operational Directive 22-01, requiring non-Department of Defense executive branch agencies to prioritize the remediation of known exploited vulnerabilities based on risk.
https://www.cisa.gov/binding-operational-directive-22-01

(4) Additional Policies, Procedures, and Requirements

(B)(4)(b) Information on protections for reporting entities under section 2245

- CIRCIA's safeguards and restrictions on government use of data closely align with the Cybersecurity Information Sharing Act of 2015 (CISA 2015), including liability protections.[21] Here are some key safeguards in CIRCIA that the rule should follow:

    - Prohibit federal and state governments from using submitted data to regulate reporting entities.
    - Treat reported information as commercial, financial, and proprietary.
    - Exempt reported information from federal and state disclosure laws.
    - Preserve trade secret protections and any related privileges or protections.
    - Waive governmental rules related to ex parte communications.

- CISA should only share reported information with other federal agencies with responsibilities over incident response or law enforcement investigations.

(B)(4)(c) Any other policies, procedures, or requirements

- The RFI does not appear to address what CISA will do with reported information to provide indicators and warnings to covered entities and other industry stakeholders. Cybersecurity information sharing must be bidirectional. Information reported to government needs to be promptly aggregated, anonymized, analyzed, and shared with industry to foster the mitigation and/or prevention of future cyber incidents.

- A persistent shortcoming experienced by businesses across many sectors is a lack of timely and effective action or feedback on cyber reports from government. We need a reporting program that leads to businesses telling the Chamber that they are receiving actionable data and assistance from CISA, law enforcement, and other agencies to enhance industry groups' security postures.

- Critical infrastructure entities with mature cybersecurity programs receive comparatively limited government support or actionable information to contest foreign malicious cyber activity. Notable exceptions include law enforcement. Public-private partnerships, such as the information sharing and analysis centers and the new Joint Cyber Defense Collaborative at CISA, should be leveraged in more purposeful ways to degrade foreign adversaries' abilities to interfere with America's critical infrastructure.[22]

---

[21] https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance

[22] https://www.uschamber.com/security/cybersecurity/coalition-letter-on-cyber-amendment-to-h-r-7900-the-fy23-national-defense-authorization-act

- Many critical infrastructure owners and operators regularly seek opportunities for deeper operational collaboration—especially ones involving the intelligence community and national security agencies, which are permitted under U.S. law to knock our strategic adversaries off balance before they can exploit American businesses and government institutions. CISA does not undertake such operations (see Appendix II).

- Organizations should not be required to report customer information or other potential PII. There should be a requirement in the rule to ensure that victim names reported to CISA are not shared outside the agency. These privacy and security safeguards for nonactionable information are consistent with the protections granted to reporting entities and reported information under CISA 2015.

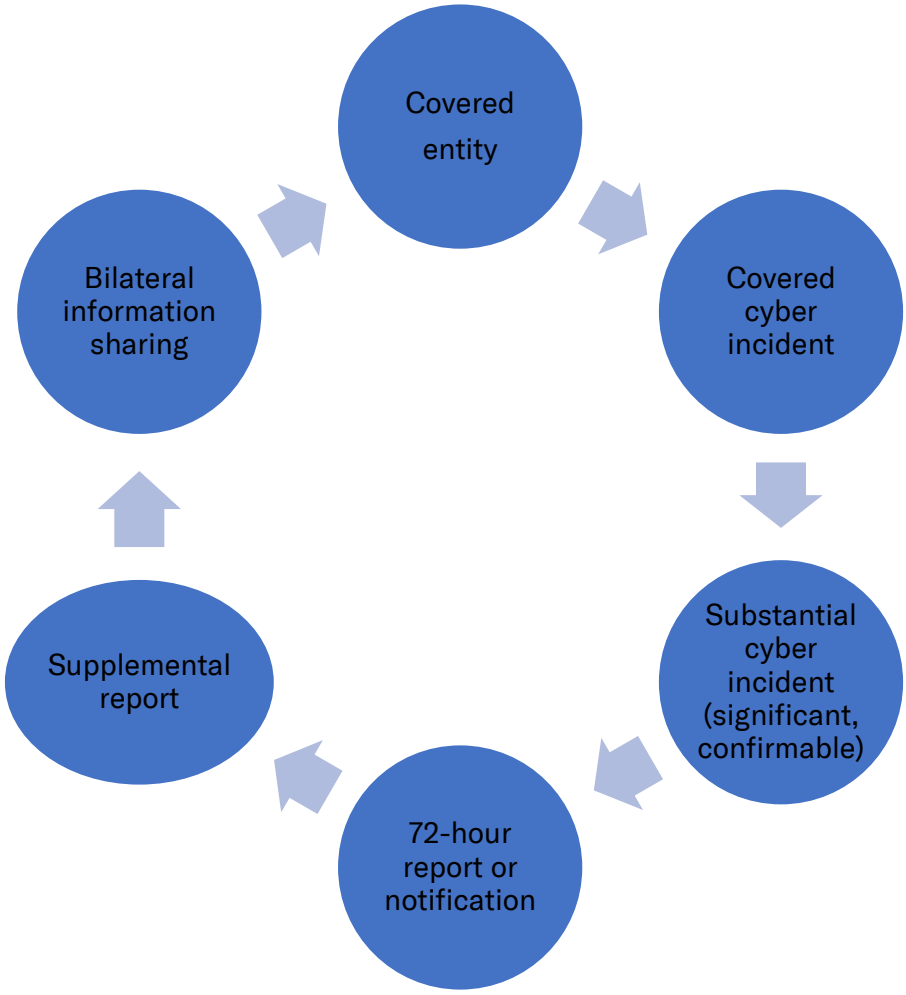
***

Thank you for the opportunity to provide CISA with comments on the proposed rule. If you have any questions or need more information, please do not hesitate to contact Matthew Eggers (meggers@uschamber.com).

Sincerely,

Matthew J. Eggers
Vice President
Cyber, Space, and National Security Policy Division
U.S. Chamber of Commerce

Appendix I



- A **covered entity** refers to a limited number of U.S. critical infrastructure entities.
- A **covered cyber incident** refers to a "substantial cyber incident" experienced by a covered entity.
- A **substantial cyber incident** is also a demonstrable "significant cyber incident."
- The **72-hour notification clock** begins when a covered entity has forensically confirmed an initial assessment of a covered cyber incident.
- A **supplemental report** refers to a covered entity promptly submitting to CISA an update to a prior report until the incident has been resolved.
- **Bilateral information sharing** refers to treating reporting as a means to bidirectional sharing and public-private operational collaboration.

Appendix II

Bilateral information sharing should be timely and actionable. Government agencies should disrupt foreign attackers.

Appendix III

Matthew J. Eggers
Vice President, Cybersecurity Policy
Cyber, Space, and National Security Policy Division
U.S. Chamber of Commerce

Remarks Prepared for Delivery

Cybersecurity and Infrastructure Security Agency Listening Session
Request for Information (RFI) on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
October 19, 2022

I'm Matthew Eggers, vice president for cybersecurity policy in the Cyber, Space, and National Security Policy Division at the U.S. Chamber of Commerce. The Chamber is pleased to have the opportunity to make some initial comments on a few points related to the RFI. We plan to submit written comments next month.

First, the meaning of "covered entity"

- According to CIRCIA, a "covered entity" refers to "an entity in a critical infrastructure sector" defined in PPD 21.

- The Chamber believes that the scope of covered entities—which is likely to feature a subset of critical infrastructure—could still be too broad from a risk management perspective.

- For CIRCIA to be effective, CISA should establish criteria in the rule that creates a narrow list of covered entities that if impacted could create significant consequences within the U.S.

Second, the number of entities

- Rather than focus on an elusive number of entities to cover, the Chamber urges CISA to focus on the types of significant cyber incidents that it wants covered entities to report.

- In other words, consideration should be given to placing emphasis on the incident—a significant incident—rather than the entity.

Third, the meaning of "covered cyber incident"

- The authors of CIRCIA did not want CISA to be overwhelmed with a flood of unusable cyber incident data because of overly broad and prescriptive reporting by covered entities.

- To enhance reporting efficiency, a covered cyber incident should be triggered only when there is a reasonable likelihood of a significant incident or harm to U.S. economic and national security.

- The Chamber believes that covered cyber incidents should be limited to incidents that directly disrupt the operation of U.S. infrastructure owned or operated by a covered entity.

Fourth, the meaning of "substantial cyber incident"

- The Chamber believes that reporting should be geared toward significant and relevant incidents—the point being that the bar should be set high for the types of incidents that CISA would determine to be reportable.

- Unlike the term "significant cyber incident," the word "substantial" is not defined in the legislation.

- The Chamber stressed to lawmakers that the word substantial would be unworkable in practice.

- Substantial is problematic because it could be used by CISA to label almost any cyber incident as covered.

Fifth, "reasonable belief" and the 72-hour reporting deadline for covered cyber incidents

- The rule should maintain a prompt reporting timeline of not less than 72 hours.

- The 72-hour deadline reflects a flexible standard for notifying CISA about significant cyber incidents.

- The rule should tie reporting to confirmed cyber incidents. Businesses need clarity in reporting requirements, which should be targeted to well-defined and confirmed cyber incidents.

Sixth, regarding additional policies, procedures, and so forth

- The RFI does not appear to address what CISA will do with reported information to provide indicators and warnings to covered entities and other industry stakeholders.

- CISA needs to treat reporting as a means to bidirectional sharing and collaboration, including helping law enforcement identify and prosecute bad actors.

- Cybersecurity information sharing needs to be bidirectional and safeguarded, consistent with the Cybersecurity Information Sharing Act of 2015.

- Information reported to government needs to be promptly aggregated, anonymized, analyzed, and shared with industry to foster the mitigation and/or prevention of future cyber incidents.

The Chamber appreciates being with CISA this morning to offer some preliminary views. We invite CISA to discuss our feedback with us as it develops a final rule that safeguards industry and is effective for businesses and the agency.