November 14, 2022

Comments of the Cybersecurity Coalition
To the Cybersecurity and Infrastructure Security Agency

Re: Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022

Docket Number 2022-19551 (CISA-2002-0010)

The Cybersecurity Coalition (the Coalition) submits the following comments in response to the Cybersecurity and Infrastructure Security Agency's (CISA) Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022.[1] The Coalition appreciates the opportunity to provide input, and we commend CISA for its openness and commitment to working with industry stakeholders to develop balanced and effective incident reporting requirements.

The Coalition is composed of leading companies specializing in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.[2] We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices, information sharing, and voluntary standards throughout the global community. Many Coalition members are in critical infrastructure sectors.

The Coalition is supportive of efforts to secure critical infrastructure and ensure the federal government makes proactive use of incident reports to strengthen security and improve threat awareness. We recommend that CISA's implementation of the Cyber Incident Reporting Act for Critical Infrastructure ("CIRCIA") align with existing reporting requirements, stay grounded in a risk management approach, and reflect the below principles:

- Establish feasible reporting timelines of no less than 72 hours of determination of a significant or material incident for reporting incident information in confidence, while allowing for supplemental reporting as more information becomes known.
- Limit reporting to verified and substantial incidents.

[1] 87 Fed. Reg. 55833 (2022).
[2] The views expressed in this comment reflect the consensus views of the Coalition, and do not necessarily reflect the views of any individual Coalition member. For more information on the Coalition, see www.cybersecuritycoalition.org.

- Limit reporting obligations to the covered entity rather than third parties.
- Harmonize federal cybersecurity incident reporting requirements.
- Ensure confidentiality and nondisclosure of sensitive incident information provided to the government that may cause additional harm to covered entities.
- Balance the urgency to notify with the need to provide accurate information.
- Maintain consistency with international standards and industry best practices for incident reporting and vulnerability handling and disclosure.
- Reporting should complement, not compete with, the incident response procedures of covered entities, and should not create additional risk for covered entities by diverting too many resources from incident response.

The Coalition notes that CIRCIA requires CISA and the National Cybersecurity and Communications Integration Center (NCCIC) to use reports of cyber incidents and ransomware payments for information sharing and analysis.[3] The final rule should provide additional specifics regarding how CISA will use the reports, including the processes CISA will build out to confirm these uses are fulfilled effectively. The purpose of the reporting requirements and overall reporting system should be clear in the final rule. We urge CISA to maintain a feedback loop with industry regarding the efficacy and accessibility of the government's use of reports for cyber incidents and ransomware payments.

Detailed below are the Coalition's responses to specific questions within CISA's request for information.

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).*

I. Continue to prioritize Systemically Important Entities

The definition of "covered entity" must balance the need for robust cyber incident reporting with the need to focus resources, avoid overwhelming incident responders, and avoid generating too many reports of no major significance. Rather than applying incident reporting requirements to all entities within critical infrastructure sectors, we recommend CISA narrow down the scope of "covered entities" to address the most serious risks. Taking a risk management approach will help focus the limited resources of CISA and the NCCIC while reducing the volume of less actionable reports.

CIRCIA defines "covered entity" as an entity within critical infrastructure sectors that also meets a threshold based on the consequences of disruption and the likelihood the entity would be targeted.[4] As CISA considers this threshold, we urge CISA to leverage the National Critical Functions Set and the work underway at the National Risk Management Center and Homeland

[3] Homeland Security Act of 2002, Sec. 2241. See also 6 USC 681a(a).
[4] Homeland Security Act of 2002, Secs. 2240(5), 2242(c). See also 6 USC 681(5), 681b(c)(1).

Security Operations Analysis Center to designate and partner with Systemically Important Entities (SIEs).[5]

"Covered entities" should directly provision a national critical function,[6] but should be a broader group than the Section 9 entities.[7] We further urge CISA to prioritize the designation of Systemically Important Entities (SIEs) that own or operate critical infrastructure systems and assets whose disruption would have a debilitating, systemic, or cascading impact on the nation's critical infrastructure, national security, national economic security, public health, or public safety.[8] SIEs should be considered "covered entities" for purposes of reporting under CIRCIA.

CISA should notify entities designated as SIEs of their designation, their reporting requirements, and the resources available to them for preventing and responding to cyber incidents. The relatively manageable number of SIEs (as compared to every entity in a critical infrastructure sector) would make direct outreach from CISA possible, removing confusion regarding whether CIRCIA's cyber incident reporting requirements apply to a particular SIE.

Many entities in critical infrastructure sectors would likely not be designated as SIEs. However, some of those entities may nonetheless be subject to cyber incident reporting requirements under other federal regulations,[9] and reports provided under those regulations may still flow to CISA. CIRCIA requires federal agencies that receive cyber incident reports to provide the reports to CISA,[10] and CIRCIA requires NCCIC to use reports provided by covered entities for information sharing, threat intelligence, and other cyber incident review purposes.[11]

II. Enable entities to meet reporting obligations through other regulations

If a covered entity is required to submit cyber incident reports under other federal regulations, CISA should consider permitting those reports to fulfill the covered entity's initial reporting obligation under CIRCIA. As directed by CIRCIA, CISA should instead enter into agreements with other agencies regarding the sharing of reports of cyber incidents and ransom payments.[12] Such agreements should include enabling CISA to follow up with the reporting entity and request additional information in supplemental reports.

As described below in responses to subsection 3, many entities in critical infrastructure sectors are already subject to incident reporting regulations, or such regulations are expected to soon come into force. Complex, overlapping cyber incident reporting requirements from federal, state,

[5] Testimony of Eric Goldstein before the US House of Representatives, Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection & Innovation, Apr. 6, 2022, pgs. 6-7, https://homeland.house.gov/imo/media/doc/goldstein_testimony_cipi_040622.pdf.
[6] CISA National Critical Functions Set, Apr. 2019, https://www.cisa.gov/national-critical-functions-set.
[7] Executive Order 13636, Improving Critical Infrastructure Cybersecurity, Section 9(a). Section 9 entities are defined as "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."
[8] Cyberspace Solarium Commission, Final Report., Mar. 11, 2020, pg. 138, https://www.cybersolarium.org/reports-and-white-papers.
[9] See responses to subsection 3, below.
[10] CIRCIA, Sec. 104. See also 6 USC 681g(a).
[11] Homeland Security Act of 2002, Sec. 2241(a). See also 6 USC 681a(a).
[12] CIRCIA, Sec. 104(a)(5). See also 6 USC 681g(5).

and international sources risk undermining cybersecurity. Requiring incident responders to file multiple reports with disparate formats and reporting items would risk diverting key resources from incident response and would risk introducing duplication and noise in the federal cyber incident reporting system.

III. Designation based on risk of damage, not size

CIRCIA appropriately requires CISA to consider the potential impact of the entity's disruption, not the size of the entity, in determining whether the entity is a "covered entity." We recommend against exempting smaller critical infrastructure entities based solely on size or revenue. Disruption of an entity with a small number of employees, or small dollar amount of revenue, may nonetheless cause significant consequences.

VI. Third party reporting

CISA should make clear that the obligation to report covered cyber incidents under CIRCIA should rest with covered entities, and that third parties are not responsible for reporting a cyber incident on behalf of the covered entity. However, covered entities should be free to designate a third party to report on behalf of the covered entity.

V. Cybersecurity vulnerability information and tools

The Coalition urges CISA to maintain a distinction between cybersecurity incidents and vulnerabilities. The existence of a vulnerability, or the possession of vulnerability information by adversaries, may create heightened risks but does not otherwise constitute a cybersecurity incident unless those vulnerabilities are exploited and information or systems are compromised.

An organization should not qualify as a "covered entity" solely on the basis of that entity possessing sensitive cybersecurity vulnerability information or penetration testing tools or techniques. Similarly, a cyber incident should not qualify as a "covered incident" solely on the basis of that incident involving unauthorized access to vulnerability information or pentesting tools. Instead, the focus should be on the extent to which the entity provisions a national critical function, and the extent to which the incident impacts the provision of a national critical function.

However, CISA may encourage non-covered entities that experience a cyber incident that involves the loss of vulnerability information or pentesting tools to submit voluntary cyber incident reports.

> *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.*

CIRCIA provides a fairly detailed description of "covered incident" that focuses on actual, not imminent, jeopardy to information and systems. To this description, we would leverage the National Cyber Incident Scoring System and the National Critical Functions set to add a requirement related to the incident's impact on public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.[13] We assemble this definition of "covered incident" below.

We are skeptical that CISA's implementing rule needs to define the definition of "covered incident" in greater detail than this.[14] Other federal incident reporting rules and proposed rules tend to have more high-level definitions of "covered incident" or "reportable incident" than CIRCIA's description of "covered cyber incident." See our responses at subsection 3 for more details on other incident reporting regulations.

Proposed definition: A "covered cyber incident" is a substantial cyber incident experienced by a covered entity[15] that

(1) The covered entity reasonably believes the incident has, or is likely to, result in
  (a) Demonstrable impact to a national critical function;
  (b) Significant impact to a national critical function; or
  (c) An imminent threat to the provision of a national critical function;[16] and

(2) Actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually jeopardizes, without lawful authority, an information system; and involves[17]
  (a) A substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;
  (b) Disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability, against
    (i) An information system or network; or
    (ii) An operational technology system or process; or
  (c) Unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by,
    (i) a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or by a supply chain compromise."[18]

[13] CISA National Cyber Incident Scoring System, Medium (Yellow), https://www.cisa.gov/uscert/CISA-National-Cyber-Incident-Scoring-System. CISA National Critical Functions Set, Apr. 2019, https://www.cisa.gov/national-critical-functions-set.

[14] CISA may consider issuing additional guidance that demonstrates how to use the National Critical Function Set, National Cyber Incident Scoring System, and other models to help covered entities determine what is a covered incident.

[15] Homeland Security Act of 2002, Sec. 2240(4). See also 6 USC 681(4)

[16] The full set of National Critical Functions may be provided as an annex to the implementing rule.

[17] Homeland Security Act of 2002, Sec. 2209 as amended by Sec. 2240(6). See also 6 USC 659(a)(5) as amended by 6 USC 681(6).

[18] Homeland Security Act of 2002, Sec. 2242(c)(2). See also 6 USC 681b(c)(2).

The terms "cloud service provider," "information system," "managed service provider" and "supply chain compromise" shall have the meanings given those terms in 6 USC 681.

e. The meaning of "substantial cyber incident."

Consistent with our above suggested definition for "covered cyber incident," we suggest that a "substantial cyber incident" is a "cyber incident" that is likely to result in

- Demonstrable impact to a national critical function;
- Significant impact to a national critical function; or
- Imminent threat to the provision of a national critical function.

This proposed definition aligns with high, severe, and emergency priority levels under the National Cyber Incident Scoring System.[19] Rather than placing "substantial cyber incidents" at a lower threshold than "significant cyber incidents," the proposed definition would encompass CIRCIA's definition of "significant cyber incident" under 6 USC 677a(8), which aligns with priority level high under the National Cyber Incident Scoring System.[20]

The Coalition is concerned CIRCIA's definition of "significant cyber incident" may set the threshold too low and result in reporting and action for unverified or non-impactful incidents. We urge CISA and the Secretary to focus resources for significant cyber incident reviews[21] and direct reporting[22] on incidents that align with severe and emergency priority levels under the National Cyber Incident Scoring System.

f. The meaning of "ransom payment" and "ransomware attack," consistent with the definitions provided in section 2240(13) and (14).

CIRCIA's definition of "ransomware attack" makes clear that extortion payments for several types of attacks are to be reported. Without changing this reporting requirement, we urge CISA to distinguish between ransomware, denial of service, and other types of attacks and extortion. This may be done in the report contents (see 2.c below), but also in guidance and other material CISA uses to provide information about ransom payment reporting obligations.

CIRCIA's definition of "ransomware attack" conflates ransomware with and other types of extortion.[23] NIST defines ransomware in NISTIR 8374, as "a type of malware that encrypts an

[19] CISA National Cyber Incident Scoring System, https://www.cisa.gov/uscert/CISA-National-Cyber-Incident-Scoring-System.
[20] Referring to an incident that "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."
[21] Homeland Security Act of 2002, Sec. 2241(a)(6). See also 6 USC 681a(a)(6).
[22] 6 USC 659(j).
[23] Homeland Security Act of 2002, Sec. 2240(4). See also 6 USC 681(14).

organization's data and demands payment as a condition of restoring access to that data."[24] However, CIRCIA's definition of "ransomware attack" includes extortion through the threat of use of malicious code, denial of service and other means.

While these extortion-based attacks are significant security threats, the attacks are distinct from "ransomware" and must be defended against differently. If ransomware payment reports conflate traditional ransomware with denial of service and other extortion, this may undermine CISA's task of providing actionable threat intelligence, trends, and other information for the purpose of defending against such attacks. Similarly, the inconsistent use of terms may confuse private sector stakeholders and lead to wasted resources or gaps in safeguards against extortion-based attacks.

To ensure the use of consistent and accurate terms, we recommend CISA align with NIST definitions of ransomware, denial of service,[25] malware,[26] and other key terms wherever possible.

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

Although CIRCIA's definition of "supply chain compromise" is not inconsistent with the NIST definition of "supply chain attack," we urge CISA to align with the NIST definition as much as possible to provide consistency and avoid confusion.[27]

(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.

CISA should establish a single, secure portal through which covered entities may submit required and voluntary cyber incident reports, as well as reports on ransom payments. This portal should be accessible via mobile devices and out-of-band communication channels in the event normal channels are compromised.

[24] NIST, NISTIR 8374, Cybersecurity Framework Profile for Ransomware Risk Management, Feb. 2022, pg. 1, https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf.
[25] NIST Computer Security Resource Center, Glossary, denial of service (DoS), 2022, https://csrc.nist.gov/glossary/term/denial_of_service.
[26] NIST Computer Security Resource Center, Glossary, malware, 2022 https://csrc.nist.gov/glossary/term/malware.
[27] NIST Computer Security Resource Center, Glossary, supply chain attack, 2022, https://csrc.nist.gov/glossary/term/supply_chain_attack.

The specific information to be included in the reports should include the items listed in section 2242(c)(4), to the extent applicable and available.[28] In addition, the report template should enable the reporting entity to

- Request CISA's assistance;
- List any other government agencies and other organizations (such as incident response providers or news media) that the entity has notified of the cyber incident; and
- Note whether the report was submitted by a third party on behalf of the covered entity, and note the identity of that third party.

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).

The NIST Computer Security Incident Handling Guide notes that "for many organizations, the most challenging part of the incident response process is accurately detecting and assessing possibility incidents — determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem."[29] This is due to the wide variety of incidents, threat indicators, and organizations' incident response capabilities, as well as the high volume of attacks. In addition, threat indicators are not always accurate and the rate of false positives and negatives is not insignificant.

Given this challenge, we urge CISA allow for flexibility in determining when covered entities are expected to have formed a "reasonable belief" that a covered cyber incident has occurred.

c. How covered entities should submit reports on ransom payments, the specific information that should be required to be included in the reports (taking into consideration the requirements in section 2242(c)(5)), any specific format or manner in which information should be submitted (taking into consideration the requirements in section 2242(c)(8)(A)), and any other aspects of the process, manner, form, content, or other items related to ransom payments that would be beneficial for CISA to clarify in the regulations.

CISA should establish a single, secure portal through which covered entities may submit reports on ransom payments, as well as required and voluntary cyber incident reports. This portal should be accessible via mobile devices and out-of-band communication channels in the event normal channels are compromised. As noted in our response to 1.f, the ransom payment report channel should distinguish between the types of extortion-based attacks, rather than collectively referring to them as "ransomware attacks."

[28] Homeland Security Act of 2002, sec. 2242(c)(4). See also 6 USC 681b(c)(4).
[29] NIST SP 800-61r2, Computer Security Incident Handling Guide, Aug. 2012, pg. 26, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

The specific information to be included in the reports should include the items listed in section 2242(c)(5), to the extent applicable and available.[30] In addition, the report template should enable the reporting entity to

- Request CISA's assistance;
- List any other government agencies and other organizations (such as incident response providers or news media) that the entity has notified of the ransom payment; and
- Note whether the report was submitted by a third party on behalf of the covered entity, and note the identity of that third party.

e. When should the time for the 24-hour deadline for reporting ransom payments begin (i.e., when a ransom payment is considered to have been "made").

The ransom payment is made when the funds or items of value are transmitted to the extorting party. This may occur after an agreement to pay is made and before the ransomware encryption key is released.

f. 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.

Supplemental reports should use the same portal and format as the initial report. This helps streamline reporting and provides CISA with more consistently structured data.

The point at which a cyber incident is mitigated and resolved will vary depending on the incident. The NIST Computer Security Incident Handling Guide notes that an incident may not be fully resolved upon containment of the attacker, and that eradication and recovery actions are system-specific and "may take months" before completion.[31] Consistent with this guidance, we urge CISA to provide the reporting entity flexibility regarding when they determine an incident has been resolved.

g. 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).

We recommend that CISA impose a deadline of not less than 72 hours after the covered entity determines that it possesses substantial new or different information regarding the incident reported in the initial report. This timeline provides the reporting entity with time to confirm

[30] Homeland Security Act of 2002, Sec. 2242(c)(5). See also 6 USC 681b(c)(5).
[31] NIST SP 800-61r2, pgs. 36-37, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

such information, coordinate with its internal stakeholders, and draft the supplemental report – while managing the incident response. Covered entities should be permitted to voluntarily submit supplemental reports before that deadline as appropriate. Because responding to cyber incidents is a dynamic process, CISA should recognize that reporting substantial new or different information is not out of the norm, and covered entities should not be deterred from reporting new information that contradicts earlier reports.

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" when establishing deadlines and criteria for supplemental reports.

Too much supplemental reporting would interfere with incident response and would not likely provide CISA with accurate, actionable, or complete information. CISA should consider setting a deadline for supplemental reporting requirements that is not less than 72 hours after the covered entity determines it possesses substantial new or different information regarding the incident reported in the initial report.

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

Submitted reports should note the use of a third-party submitter and identify that third party. The identity of the third party may be useful to CISA for post-incident collaboration with the covered entity. The use of a third-party submitter should not otherwise subject the covered entity to additional reporting requirements.

k. To clarify or supplement the examples provided in section 2242(d)(1), what constitutes a third-party entity who may submit a covered cyber incident report or ransom payment report on behalf of a covered entity.

We suggest what constitutes an appropriate third party is that a valid contractual relationship exists between the third party and the covered entity, and that this relationship provides for submission of cyber incident reports or ransom payment reports. While a variety of third parties may appropriately submit a report, requiring a formal relationship helps avoid reports from unauthorized parties, and confusion regarding responsibility for the report.

l. How a third party can meet its responsibility to advise an impacted covered entity of its ransom payment reporting responsibilities under section 2242(d)(4).

The third party and covered entity should have flexibility to specify the form this advice must take. However, we believe this advice should be in writing and note the date.

(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.*

Numerous federal, state, and international regulations or proposed regulations require organizations in critical infrastructure sectors to submit cyber incident reports.[32] We urge CISA to review available resources that compile and compare these requirements.[33] Although these regulations include some similarities, they also present different reporting deadlines, reporting criteria, triggering event, purpose for the report, and confidentiality rules.

Areas of overlap with CIRCIA include covered entities and incidents. Private sector critical infrastructure entities that are subject to US incident reporting requirements and proposed requirements include publicly traded companies, federal contractors, electric utilities and bulk electric system operators, pipeline owners and operators, and an array of financial institutions (non-banking, banking, and credit unions).[34] In addition, CISA should consider the impact of international cyber incident reporting requirements, such as the European Union's (EU) proposed revision to the Network and Information Security (NIS) Directive, which will cover critical infrastructure -like sectors operating in the EU. Although the trigger for reporting differs between these regulations, there is a high likelihood that "covered cyber incidents" under CIRCIA must also be reported under these other regimes.

Areas of conflict include the reporting trigger, deadline for reporting, and the confidentiality of the reports. CIRCIA's definition of "cyber incident" excludes incidents that do not actually jeopardize information and systems,[35] but some other regulations require reporting for attempted attacks.[36] While CIRCIA requires reports within 72 hours of the determination of a reportable incident, other federal regulations and proposed regulations have a wide range of deadlines. For example, a US-based publicly traded electric utility may need to file an initial report to NERC within one hour,[37] a report to CISA within 72 hours, a report to SEC within 4 days,[38] a follow-up report to NERC within seven days,[39] a quarterly status update to SEC,[40] and potential supplemental reports to CISA.

While most regulations (including CIRCIA) treat cyber incident reports as confidential, the rules proposed by SEC and FTC would make such reports publicly available, potentially creating new

[32] Note that there we are excluding notification requirements for breaches of personal information.
[33] See, e.g.,R Street Institute, Federal Cyber Incident and Breach Reporting, Jul. 28, 2022, https://www.rstreet.org/wp-content/uploads/2022/07/federal-cyber-incident-breach-reporting-072822-1.pd. See also, Rapid7, Cyber Incident Reporting Requirements, Aug. 8, 2022, https://www.rapid7.com/globalassets/_pdfs/Rapid7-Incident-Reporting-Regulation-Summary-Chart-080822.pdf.
[34] *Id*.
[35] Homeland Security Act of 2002, Sec. 2240(6)(B). See also 6 USC 681(6)(B).
[36] See, e.g., NERC CIP 008-6, R4.
[37] NERC CIP 008-6, R4.2.
[38] 87 Fed. Reg. 16595.
[39] NERC CIP 008-6, R4.3.
[40] 87 Fed. Reg. 16596.

cybersecurity risks.[41] The SEC's purpose for requiring a cyber incident report is to provide investors with information to make investment decisions, but this is not aligned with the cybersecurity purposes for incident reporting identified under CIRCIA.[42] The Coalition has expressed concern to the SEC that requiring public disclosure of unmitigated incidents as a default will expose organizations to additional risk.[43]

We again urge CISA to work with its agency partners and the private sector to harmonize cyber incident reporting requirements.

> *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.*

The Coalition urges CISA to distinguish between vulnerabilities and incidents. The existence of a vulnerability does not mean that an incident has occurred that places information or systems in jeopardy of unauthorized access or disruption. However, if a vulnerability is exploited, this may lead to the occurrence of such an incident. CISA should not require disclosure of vulnerabilities in the absence of a covered cybersecurity incident or a significant cybersecurity incident.

If CISA requires the disclosure of a vulnerability for which there is no mitigation yet available, CISA should limit sharing that vulnerability. CISA should avoid, whenever possible, publicly disclosing vulnerability details prior to mitigation or a patch for the vulnerability. Industry standards and best practices for vulnerability disclosure and incident response – such as ISO/IEC 29147 and 30111 and the CERT Guide to CVD – encourage organizations to limit the pre-mitigation disclosure of vulnerabilities to necessary parties.[44] However, there are exceptional circumstances under which public disclosure of unmitigated vulnerabilities may be necessary. Typically this occurs after failure to mitigate (such as due to inability to engage the affected organization), or when users should take defensive measures before mitigation because ongoing exploitation of the vulnerability "in the wild" is actively harming users.

(4) Additional Policies, Procedures, and Requirements

> *c. Any other policies, procedures, or requirements that it would benefit the regulated community for CISA to address in the proposed rule.*

I. Harmonization.

---

[41] See Comments of Rapid7 to SEC on Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Aug. 29, 2022, https://www.sec.gov/comments/s7-09-22/s70922-20137661-308069.pdf.
[42] Homeland Security Act of 2002, Sec. 2245(a). See also 6 USC 681e(a).
[43] See Comments of the Cybersecurity Coalition to SEC on Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, May 9, 2002, https://www.cybersecuritycoalition.org/filings/comments-on-sec-proposed-rule-regarding-cybersecurity-risk-management-strategy-governance-and-incident-disclosure-file-s7-09-22.
[44] CERT, Guide to Coordinated Vulnerability Disclosure, 5.7 Disclosure Timing, Sep. 16, 2019, https://vuls.cert.org/confluence/display/CVD/5.7+Disclosure+Timing#id-5.7DisclosureTiming-ReleasingPartialInf.

CIRCIA directs the Secretary of Homeland Security to lead an intergovernmental Cyber Incident Reporting Council to coordinate, deconflict, and harmonize federal incident reporting requirements.[45] We urge CISA and the Department of Homeland Security to establish this council as soon as possible and to ensure the cyber incident reporting requirements and processes from the implementation of CIRCIA are harmonized with the incident reporting requirements of other agencies.

II. Separating critical and non-critical systems.

Many covered entities may have systems and information that are related to a national critical function, as well as those that are *not* related to a national critical function. CIRCIA is unclear regarding what is the obligation of the covered entity to report an incident that affects a system or information that is not related to a national critical function. Consistent with focusing incident reporting on serious risks to critical infrastructure, the Coalition urges CISA to clarify that cyber incident reporting is not required for incidents that affect systems which are not related to a national critical function.

III. Significant incident review and strategic partnership and for long term security.

Cyber incident reporting is reactive by nature, coming in the aftermath of a cyber incident. There is a substantial risk that a more holistic approach to long term security is overlooked in the cycle of incidents, mitigation, and compliance. The Cybersecurity Coalition urges CISA to work with industry to develop categories of information and analyses that may aid significant reduction of common threats and vulnerabilities over time. These analyses could be part of the review of the details surrounding significant cyber incidents, as required by CIRCIA.[46] However, it is essential that this information and other follow-up questions remain subject to the same confidentiality and liability protections as initial reports under CIRCIA, including exemption from FOIA.[47]

These tasks may require special technical expertise and resources, and we do not recommend that it be incorporated into requirements to report covered cyber incidents at this time. Rather, we envision CISA collaborating with SIEs and sharing information on a voluntary and confidential basis for the purpose of facilitating a fundamentally more resilient digital ecosystem.

Categories of information and analysis that may help advance this objective include:

- Root cause analyses - Performing root cause analysis of vulnerabilities can aid understanding of the software architecture that causes vulnerabilities to be present despite repeated patching to prevent similar types of exploits.

- Patch adoption and rollout - Patching vulnerabilities is an essential security practice. However, limited industry-wide metrics are available for security patch adoption, frequency of patching, prevalence of automated security updates, and the manner in which patches are presented to end users. Greater transparency regarding these activities

[45] Homeland Security Act of 2002, Sec. 2246. See also 6 USC 681f(a), 681g(b).
[46] Homeland Security Act of 2002, Sec. 2241(a)(6). See also 6 USC 681a(a)(6).
[47] Homeland Security Act of 2002, Sec. 2245. 6 USC 681e.

would enable stakeholders to better determine the most effective practices, and the extent to which platforms and users are improving their patching practices.

- Coordinated vulnerability disclosure - While all organizations should have a means to receive and respond to unsolicited vulnerabilities disclosures, it is unclear how many organizations have established vulnerability disclosure policies. It is less clear the extent to which such vulnerability disclosure policies are backed by internal vulnerability management programs with adequate resources and mature processes that can carry a vulnerability disclosure through to technical analysis and mitigation in alignment with international best practices and standards.[48] Without such resources and processes, vulnerability disclosure policies have reduced effectiveness.

- Adoption of NIST Cybersecurity Framework - The NIST Cybersecurity Framework for Critical Infrastructure is a highly regarded tool for cyber risk management. However, there are limited metrics regarding how many critical infrastructure organizations use the Framework to manage cyber risk. Knowing when and how the Framework is used across industry can help identify incentives or barriers to Framework adoption.

* * *

The Coalition hopes that its input will be helpful to CISA as it implements CIRCIA, harmonizes cyber incident reporting requirements, and leverages cyber incident reports into actionable information that strengthens cybersecurity. Should you have any questions, or if we can assist in any other way, please contact Harley Geiger at HLGeiger@Venable.com.

Respectfully submitted,

The Cybersecurity Coalition

[48] See, e.g., ISO/IEC 29147 and 30111.