IST Institute for SECURITY + TECHNOLOGY

CYBER THREAT ALLIANCE

July 3, 2024

Submitted electronically to https://regulations.gov

To: Jen Easterly, Director and Todd Klessman, CIRCIA Rulemaking Team Lead
Cybersecurity and Infrastructure Security Agency
1110 N. Glebe Road
Arlington, VA 20598-0630

Subject: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements Proposed Rule [Docket No. CISA-2022-0010]

Director Easterly and Mr. Klessman,

The Institute for Security and Technology (IST) and the Cyber Threat Alliance, along with co-signer Chainalysis, submit these comments in response to the Cybersecurity and Infrastructure Security Agency's Notice of Proposed Rulemaking on the Cyber Incident Reporting for Critical Infrastructure Act.

The **Institute for Security and Technology** is a 501(c)(3) think tank that unites technology and policy leaders to create actionable solutions to emerging security challenges. In late 2020, in response to the growing threat posed by the escalating rise in ransomware incidents targeting critical infrastructure, IST convened the Ransomware Task Force (RTF), a multi-stakeholder coalition of 60+ organizations across the public and private sectors who convened in four working groups and examined measures to help better deter, disrupt, prepare, and respond to ransomware. The RTF in April 2021 released a report outlining key actions to tackle the threat of ransomware, organized around four overarching goals. In the three years since, the RTF continues its work to combat ransomware, helping government and industry follow through on its original recommendations. In order to respond to ransomware attacks more effectively, the RTF recommended creating a standard format for incident reporting (Action 4.2.2) and encouraging organizations to report ransomware incidents (Action 4.2.3). The passage of CIRCIA in 2022 marked a significant step towards achieving these objectives. Now, IST draws on the ongoing efforts of the Ransomware Task Force to respond to the Notice of Proposed Rulemaking on CIRCIA.

The **Cyber Threat Alliance** (CTA) is a 501(c)(6) non-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field.

The sponsoring and co-signing organizations support the draft rule. It clearly reflects input from industry, and CISA should proceed with finalizing the rule as soon as possible.

Our recommendations draw from the joint effort by the Cyber Threat Alliance and the Institute for Security and Technology that produced the Cyber Incident Reporting Framework (CIRF), which was submitted to CISA as part of the initial RFP for implementing this legislation and rulemaking.[1] In our comments below we continue to draw from that effort, which multiple technology- and cybersecurity-focused organizations co-sponsored.

Since submitting the CIRF in response to the RFI, our interactions with critical infrastructure companies have reinforced a key concept: to maintain support for this reporting requirement, CISA will need to demonstrate its value to critical infrastructure companies. In our view, CISA can demonstrate its value through three primary use cases: support to the reporting organization, near-term threat intelligence sharing to similarly situated companies to enable better defensive action, and long-term trend analysis to support policy decisions and private sector investments. CISA should position itself to successfully implement all three use cases.

Therefore, we recommend that CISA focus on ensuring that the data collected helps CISA's critical infrastructure protection mission, including analyzing the data it collects from participating organizations and distributing key lessons learned to the broader cybersecurity community. IST and CTA's joint comments include recommendations that seek to make the information collected easier for CISA to intake and analyze.

As noted in the CIRF, the sponsors and co-signers of these comments affirm that it is reasonable to exclude small- and medium-sized enterprises (SMEs) from being required to report under this rule. However, this decision does have potential drawbacks: a lack of data about attacks against these enterprises may lead to a failure to understand and address threats to SMEs. We recommend that CISA engage with the small- and medium-sized enterprise community through alternative means to gather information about cyber threats to critical infrastructure supported by SMEs.

Incident Reporting Harmonization:

- **Harmonization at international, federal, state, local, and tribal levels:** We greatly appreciate the NPRM's acknowledgement that harmonization is critical, and the effort made by CISA in seeking to use the common template reached through the DHS-led interagency process focused on incident reporting. As noted by the ONCD report released in June 2024, "The lack of harmonization and reciprocity harms cybersecurity outcomes…[and] compliance spending [can sometimes draw] resources from cybersecurity programs."[2] The ONCD report also highlights that there are "inconsistent

[1] "Cyber Incident Reporting Framework," Institute for Security and Technology and Cyber Threat Alliance, November 2022, https://securityandtechnology.org/virtual-library/reports/cyber-incident-reporting-framework/.

[2] Office of the National Cyber Director, "Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information," June 2024,

or duplicative requirements across international and state regulatory regimes." In addition to the work to harmonize at the federal level, we encourage use of common templates at state, local, tribal, and territorial level as well–efforts that CISA can encourage, even though they fall beyond its immediate purview.

- **A maximalist approach to harmonization and deconfliction**: Given that many cybersecurity incidents have cross-border elements, we encourage CISA to take a maximalist approach to harmonizing and deconflicting requirements between jurisdictions across the globe. While we understand that the CIRCIA legislation requires specific elements in the implementing regulations, when possible we encourage maximum flexibility with U.S. regulation in order to harmonize across jurisdictions in partner nations. We particularly recommend harmonization with the provisions of the EU-NIS-2 directive, as that directive will likely drive reporting requirements outside of the EU. We are heartened that DG Connect and ONCD are working on this issue.[3] This coordination has potential to provide enormous value to cybersecurity authorities and sector risk management agencies globally, as it will allow for the low-friction transfer of key information regarding cybersecurity incidents of concern, while also reducing the burden placed on entities that have been the victims of cyber crimes.

Incident Reporting Format:

- **The importance of streamlined incident reporting**: Given that CISA will likely be collecting substantial amounts of information from a wide variety of entities, including but not limited to entities with limited cybersecurity capacity and low levels of maturity, CISA should make reporting as easy as possible for entities to complete. Additionally, CISA will have limited resources to intake, analyze, anonymize, and disseminate this information. Therefore, information should be collected in the most streamlined manner possible.

- **Standardized reporting formats**: Given our experience with threat intelligence sharing among many different cybersecurity organizations, we strongly recommend that CISA reduce the number of free-form reporting fields as much as possible. Instead, we suggest using drop-down menus that then generate different fields based on the answers. Unless the form constrains the choices available to reporting entities, the reports CISA receives will contain too much variation for CISA to make use of them or to analyze them at scale.

- **Dynamic reporting**: We recommend that CISA build a dynamic reporting portal, as discussed in the NPRM (IV.E.ii). We recognize that other methods need to be available

https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf.

[3] Department of Homeland Security "DHS and DG CONNECT Announce Initiative Comparing Cyber Incident Reporting to Better Align Transatlantic Approaches," press release, March 20, 2024, https://www.dhs.gov/news/2024/03/20/dhs-and-dg-connect-announce-initiative-comparing-cyber-incident-reporting-better.

for organizations that are unable to access the portal due to disruptions caused by the significant cyber incident in question (IV.E.i.1). However, we strongly suggest that CISA highlight the web portal as the preferred method of reporting. A dynamic portal has several key benefits, including allowing covered entities to update information about the incident as they collect more evidence and conduct additional analysis. A portal with time stamps and version histories can capture updates and help collect metrics for time and frequency of inputs between updates.

  - Under CIRCIA, a covered entity "must submit a Covered Cyber Incident Report to CISA no later than 72 hours after the covered entity reasonably believes the covered cyber incident has occurred" [§226.5.a]. Since many entities will have limited knowledge regarding the incident in the first 72 hours, a dynamic portal will make it easier for organizations to update information as it is uncovered. Dynamic reporting can also help incentivize supplemental reporting, which are supposed to be submitted "promptly" [§226.3.d.1] as "substantial new or different information becomes available" [§226.3.d.1.i] or if a ransom is paid by the organization or on the organization's behalf [§226.3.d.1.ii]. Recommendations included timelines ranging from 12 hours to one year after the incident occurs [III.F.vii]. Because CIRCIA requires supplemental reporting until the incident is concluded, a dynamic portal can make reporting easier to complete. Dynamic reporting can also be more quickly distilled, analyzed, and shared outward to covered entities to improve defenses and mitigate effects of cyber incidents.

  - CISA should also be clear that the federal government will not penalize entities that provide initial information that is incorrect, so long as that information is corrected in a timely manner and so long as the entities did not provide the initial information with malicious or negligent intent. The guidance should note that CISA welcomes additional information that clarifies, modifies, or changes information to reflect better understanding of the incident.

- **Categorizing types of incidents**: We recommend that CISA provide a standardized list of incident types in its reporting formats. Different incident types require distinct information fields. By standardizing the types of incidents reported through CIRCIA, CISA can streamline information processing and reduce unnecessary work clarifying and categorizing incidents on the backend. The CIRF provides a list of specific forms of incidents, specifying key information fields necessary for each type of event. This list breaks down incidents into 10 types: business email compromise; ransomware or other extortion; data theft; financial theft (e.g., banking trojans); service theft; denial of service / availability attack; disruptive or destructive attack; data manipulation or integrity loss; branding / reputation attack; and unauthorized access to mission critical information or systems (e.g., OT, SCADA, or ICS systems). The form could also allow the option to select "unknown at this time" in cases where the incident type is unknown, which could then allow for further information to be provided after the initial report. Again, if CISA does not constrain the choices available, it will have to expend substantial resources making the data comparable.

- **Technical details**: We encourage CISA to separate out technical details into a distinct reporting layer to ease the burden of reporting on organizations. The CIRF framework provides clear suggestions about how to distill technical details. As mentioned above, a dynamic reporting portal can make this kind of separation easier to organize and manage.

- **Security of the portal and the information gathered:** Given that the information gathered by this process will include substantial and critical data about vulnerabilities and discovery of malicious activity, CISA must ensure that data collected is well-secured and cannot be hacked, including by sophisticated hacking groups. To complete its reports on aggregated data, CISA will want to retain the data and define its processes for secure data storage and the duration of data retention. CISA will also need to define policies for eventual destruction of data to ensure its availability for research purposes and compliance with regulatory requirements.

- **Penalties for unauthorized disclosure:** To reassure reporting entities that their data will be kept confidential, CISA could consider including specific penalties for government personnel that make unauthorized disclosures of information contained in the reports.

Definition of Substantial Cyber Incident:

- **Confidentiality provision**: We recommend that CISA consider clarifying the definition of a substantial cyber incident related to loss of confidentiality by including specific forms of information that should be prioritized. The draft definition states that a substantial cyber incident includes an event where an actor gains “unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein” through a third party data hosting provider or supply chain compromise (§226.1). CTA and IST believe this definition should be refined to provide more concrete guidance for organizations as they determine how to implement CIRCIA reporting. The CIRF provides a useful definition that CISA should consider. It classifies a substantial cyber incident related to loss of confidentiality as “Material loss of, compromise in, unauthorized access to, or denial of access to: sensitive non-public data, personally identifiable information, intellectual property, or trade secrets; revenue, income, or assets; business operations or system functionality; or, brand or corporate reputation.”

- **Social media**: We recommend CISA clarify whether social media accounts can be a potential source of a substantial cyber incident. The current definition [§226.1] does not mention social media. Social media is only identified as a possible beneficial avenue for spreading awareness of incidents and CISA resources [V.A.v]. Given the potential for misinformation to spread through social media, we recommend that CISA incorporate incidents affecting these entities into the current definition of a substantial cyber incident.

Incident Reporting Timeline

- **Deadlines**: To ensure comprehensive reporting, we recommend that CISA specify some deadlines in the supplemental reporting process, such as requiring entities to provide a corrected report within 48 hours if further investigation indicates that their initial report was substantially incorrect or incomplete. Such a requirement would ensure that CISA receives the most up-to-date and complete information to alert organizations that could be facing similar vulnerabilities and allow CISA to effectively coordinate responses and provide assistance to victims.

IST and CTA are available to CISA as it works to complete implementation of the Rule. Should you have questions about our response, or if we can assist in any other way, please contact Taylor Grossman at Taylor@securityandtechnology.org.