1212 New York Ave. NW
Suite 900
Washington, D.C. 20005
202-525-5717

Free Markets. Real Solutions.
www.rstreet.org

November 14, 2022

Cybersecurity and Infrastructure Security Agency (CISA)
1110 N. Glebe Road
Arlington, VA 22201

Re: Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022
Document ID (CISA-2022-0010) |Federal Register Number 2022-19551
Submitted Electronically

I. INTRODUCTION

The R Street Institute (R Street) is a nonprofit, nonpartisan public policy research organization headquartered in Washington, D.C. Our mission is to engage in policy research and outreach to promote free markets and limited, effective government. R Street's Cybersecurity and Emerging Threats team focuses on the national security implications of individual, business and government cyber risk.

In the past year, we have paid close attention to cybersecurity incident reporting requirements stemming from multiple federal agencies and pending regulations from the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). This summer, we submitted a response to the Securities and Exchange Commission (SEC), noting several areas that are also relevant to this Request for Information (RFI).[1] This comment focuses specifically on the definition of "substantial cyber incident," its materiality, the 72-hour reporting requirement and report submission requirements.

In addition, we analyzed federally mandated cybersecurity incident reporting and data breach notification requirements and noted two dozen regulations and statutes with varying degrees of reporting requirements.[2] The analysis did not include the approximately 36 state-enacted cybersecurity

[1] Mary Brooks and Brandon Pugh, "Comments on Proposed Rulemaking by the Securities and Exchange Commission on 'Governing Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,'" R Street Institute, May 5, 2022. https://www.rstreet.org/2022/05/05/comments-on-proposed-rulemaking-by-the-securities-and-exchange-commission-on-governing-cybersecurity-risk-management-strategy-governance-and-incident-disclosure.

[2] Mary Brooks and Sofia Lesmes, "Cybersecurity Incident and Breach Reporting Requirements," R Street Institute, June 23, 2022. https://www.rstreet.org/2022/06/23/cybersecurity-incident-and-breach-reporting-requirements; Sofia Lesmes and Mary Brooks, "By the Numbers: Parsing Cybersecurity Incident and Breach Reporting Requirements," R Street Institute, Sept. 1, 2022. https://www.rstreet.org/2022/09/01/by-the-numbers-parsing-cybersecurity-incident-and-breach-reporting-requirements.

laws; the 50 state data breach notification laws; the EU's Global Data Protection Regulation; the updated Network and Information Society (NIS) Directive, NIS2; and other global incident reporting laws from India, Singapore, Australia and more.[3]

We broadly support mandatory cybersecurity incident and risk management reporting that is reasonable, balances industry concerns and provides usable data to industry and critical infrastructure (CI) entities.[4] The number of disparate reporting requirements at the state, federal and international levels poses an operational burden and risk of non-compliance on small, medium and large entities (from large corporations to municipalities).

To help inform CISA's development of the proposed CIRCIA rulemaking, this formal response highlights several considerations and recommendations around the use of CISA's harmonization effort under CIRCIA, including the reduction of information-sharing burdens and areas of confusion and broader awareness for CI entities. The need to harmonize incident reporting requirements at the federal level can alleviate duplicative reporting requirements currently in existence and support effective interoperable information-sharing with federal government rulemakings on incident reporting.

The cybersecurity information-sharing and reporting landscape is confusing and noisy as new cyber incident reporting rulemakings are proposed. There has to be a balance in which CI entities and businesses can provide accurate and timely threat information without burdening their operations. This submission will go over key considerations and provide recommendations to assist in CISA's effort to harmonize incident reporting requirements and reduce burdens for industry and CI entities.

II. CONSIDERATIONS

Cyber incident reporting is a complicated web in which there is more than one federal agency with cyber incident reporting regulations, and CI entities have to report to multiple agencies with varying reporting thresholds and timelines. With CIRCIA, CISA has an opportunity to clarify the best method to identify

[3] "Cybersecurity Legislation 2021," National Conference of State Legislatures, July 1, 2022. https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2021.aspx; "Security Breach Notification Laws," National Conference of State Legislatures, Jan. 17, 2022. https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx; Cheryl Saniuk-Heinig, "State Data Breach Notification Chart," International Association of Privacy Professionals (IAPP), March 2021. https://iapp.org/resources/article/state-data-breach-notification-chart; Ben Wolford, "What is GDPR, the EU's new data protection law?" GDPR.EU. https://gdpr.eu/what-is-gdpr; Ana Hadnes Bruder et al., "NIS2 Directive New Cybersecurity Rules Expected in the EU," Oct. 6, 2022. https://www.mayerbrown.com/en/perspectives-events/publications/2022/10/nis2-directive-new-cybersecurity-rules-expected-in-the-eu.

[4] Ayan Islam, "CISA hears from business, pipeline groups on considerations for upcoming reporting regime," R Street Institute, Oct. 20, 2022. https://www.rstreet.org/2022/10/20/insidecybersecurity-com; Mary Brooks and Sofia Lesmes, "Last Call at the 'Star Wars Bar': Harmonizing Incident and Breach Reporting Requirements," R Street Institute, July 5, 2022. https://www.rstreet.org/2022/07/05/last-call-at-the-star-wars-bar-harmonizing-incident-and-breach-reporting-requirements.

and pursue cyber incident reporting harmonization with federal regulators. We will focus on two areas in which CISA can help reduce operational burdens and the risk of missing threat information.

1. ***Critical Infrastructure Entities Have Multiple Reporting Obligations Between State, Federal and Other Nations' Governments.***

Critical infrastructure entities, ranging from municipalities to global corporations, are subject to three or four federal reporting requirements as a result of the business-related thresholds of each CI sector. And some entities may have multiple reporting obligations depending on which CI sector(s) they touch, which states they may have a business nexus to as a result of the data they possess and whether that data implicates EU or other foreign citizens' data.

To give an example, a health care entity may be required to report to both the Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) if a cybersecurity incident results in a loss of personal health records and the entity is covered under the Health Insurance Portability and Accountability Act of 1996 (HIPPA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). Similarly, a pharmaceutical company with research labs and an outsourced manufacturing facility could potentially have multiple reporting requirements to HHS; the Department of Homeland Security, due to the chemical manufacturing piece; and the FTC if patient clinical trial records are impacted in an incident with multiple dependencies.

To further compound the problem, entities will have to conduct internal reviews to determine which components of their business fall under certain CI sectors for federal cyber incident reporting, the nexus in cyber incident reporting thresholds for each state, and global reporting requirements (particularly in the EU). One could argue that this problem is limited to global organizations; however, the same thinking is applicable to small, municipal entities that may not have sufficient resources to conduct this assessment and that rely on a managed security service provider—if they even have the means to hire one.

The opportunity to streamline reporting and clarify who should receive reports can substantially assist industry and CI entities that have multiple reporting obligations. Streamlining also reduces the potential for liability exposure for smaller entities that make an honest mistake in reporting to one place and not another.

2. ***Not All Entities Know Where to Report Cyber Incidents or Assume They Will Be Shared Broadly.***

A key question that is of utmost importance regarding the future effectiveness of CIRCIA's incident reporting rules: **Do entities know where to submit cyber incident reports?** Currently, CISA has an incident reporting form that appears to be buried in handouts and not listed under the "Resources" column on CISA's homepage, on its Information Sharing webpage under the Cybersecurity section, or prominently shown elsewhere. To access CISA's "Incident Reporting System," users must search to find precise links.[5] Additionally, the incident reporting form has certain "required" fields that may be difficult to complete if a form submitter fails to realize that the federal incident notification guidelines are the "how to" instructions for completing the incident reporting form. To add to this, industry and CI entities have separate forms to complete for cyber incident reporting, which can create additional confusion on what information was shared where, with whom and whether it was shared at all, as each agency has a different submission form.

Additionally, depending on the entity and its awareness of all the federal cybersecurity roles and responsibilities, there are many occasions in which information is submitted to one agency with the assumption that it would be shared with other agencies. For example, an entity may report to a federal regulator with the assumption that the information will land at CISA and/or with the Federal Bureau of Investigation (FBI). Moreover, some may think that the FBI offers cybersecurity incident response services and not realize it is one of CISA's free cybersecurity offerings. Rather, the FBI is meant to investigate certain types of cyber crimes. The cybersecurity landscape is confusing with the unclear federal role and opaque responsibilities when it comes to service offerings, incident reporting requirements and who is a lead or partner for cyber incident response and information-sharing engagements. This issue increases the risk—which could be mitigated at the source or across sectors—of missing critical threat information.

There is also an assumption that submitting a report to the regulator and a sector-specific Information Sharing and Analysis Center (ISAC) or Information Sharing and Analysis Organization (ISAO) will mean that other federal agencies will receive the report too. While some agencies have preexisting interagency information-sharing agreements in place, it is not always evident who has those agreements in place to share the entity's cyber incident information and whether it is clear for submitting entities how the information will be shared and protected, what liability protections are in place for submission and for what the information will be used. As CISA reviews the various reporting mechanism, there are a few questions for consideration when assessing information-sharing channels:

- Do all of the Sector Risk Management Agencies (SRMAs) have interagency informational-sharing agreements between their Security Operation Centers and CISA Central?[6]
- What cyber incident information is currently required from regulated entities? And can the regulators share the information with CISA?
- Are critical infrastructure sector entities aware of the differences in reporting to CISA Central, the FBI's CyWatch, the Internet Crime Complaint Center, the Department of Defense Cyber

[5] "Report," Cybersecurity & Infrastructure Security Agency, last accessed Nov. 8, 2022. https://www.cisa.gov/report; "CISA Incident Reporting System," Cybersecurity & Infrastructure Security Agency, last accessed Nov. 8, 2022. https://us-cert.cisa.gov/forms/report.

[6] "CISA Central," Cybersecurity & Infrastructure Security Agency, last accessed Nov. 8, 2022. https://www.cisa.gov/central.

Crime Center, the National Cyber Investigative Joint Task Force, sector-specific ISACs/ISAOS and the respective regulatory agency or agencies?[7]
- Is regional cyber incident reporting reaching the right teams for follow-up and coordination at the headquarter and/or regional level?

Conducting a review of CISA's current reporting form and the information shared among federal agencies and with CI entities can limit confusion, increase information-sharing, improve the effectiveness of CIRCIA's incident reporting requirements and inform bi-directional engagement with industry.

III. RECOMMENDATIONS

1. *Analyze federal incident reporting regulations for harmonization opportunities.*

Under Section 106 of CIRCIA, the Cyber Incident Reporting Council (Council) is required to submit a report on the "harmonization of reporting regulations." It is reassuring that Congress mandated this report because it forces a comprehensive look at the number of duplicative federal cyber incident reporting requirements on covered entities and requires proposals to streamline and reduce duplicative incident reporting. As part of the Council's analysis, R Street offers these two documents to support the development of the report:

- "Cybersecurity Incident and Breach Reporting Requirements"[8]
- "By the Numbers: Parsing Cybersecurity Incident and Breach Reporting Requirements" [9]

It is imperative that the Council completes the report soon to inform the development of CISA's CIRCIA advanced proposed rulemaking and leverage recommendations received from incident reporting harmonization discussions with SRMA and key CI sector partners.

2. *Conduct engagement sessions with industry and CI entities to develop improved incident reporting solutions (including incremental reporting to begin with "reasonable belief" of a cyber incident to material content and determining what constitutes a covered cyber incident).*

[7] The Department of Defense Cyber Crime Center, "DC3 Mission Overview," Department of Defense, last accessed Nov. 8, 2022. https://www.dc3.mil; "The Cyber Threat," Federal Bureau of Investigation, last accessed Nov. 8, 2022. https://www.fbi.gov/investigate/cyber.

[8] Mary Brooks and Sofia Lesmes, "Cybersecurity Incident and Breach Reporting Requirements," R Street Institute, June 23, 2022. https://www.rstreet.org/2022/06/23/cybersecurity-incident-and-breach-reporting-requirements.

[9] Sofia Lesmes and Mary Brooks, "By the Numbers: Parsing Cybersecurity Incident and Breach Reporting Requirements," R Street Institute, Sept. 1, 2022. https://www.rstreet.org/2022/09/01/by-the-numbers-parsing-cybersecurity-incident-and-breach-reporting-requirements.

It is important that CISA takes a closer look at the reporting methods that it and other federal agencies currently use for CI sector reporting requirements and considers how much information is already being received from regulatory agencies.

CISA can likely reach multiple incident reporting solutions, including improvements to its incident reporting form, if it hosts a series of workshops to both survey and receive recommendations from CI sector entities and its providers. Similar to the CIRCIA RFI listening sessions, CISA can leverage its Sector Coordinating Councils, relationships with ISACs/ISAOs/associations and Joint Cyber Defense Collaborative partners to survey what information-sharing mechanisms work well, are interoperable and could potentially be modified or revived.[10]

There is likely not a one-size-fits-all model. For example, the Transportation Security Administration (TSA) has an information-sharing agreement with CISA Central and promises entities that any information shared with either agency will meet the reporting requirement and will be shared between TSA and CISA, respectively.[11] Aviation entities, therefore, can report a cyber incident to the Aviation-ISAC and TSA or CISA, knowing that if they inadvertently missed one agency, the other will be looped in. This is only one example, and there may be other methods available for consideration.

Furthermore, agreement on which incident reporting form template is needed can help an entity with initial reporting and subsequent follow-up by providing additional details such as Techniques, Tactics and Procedures (TTPs) and/or Indicators of Compromise (IOC). This level of detail on the materiality of the event becomes evident after several weeks of forensic investigations and is typically not available in the first 72 hours or even the first seven days after an incident occurs. Also, the reporting thresholds for covered entities tend to vary based on the sector's threat landscape, and each sector has its own definition of what it considers a "covered cyber incident."

Because cyber threat information varies in each sector, it would benefit CISA and SRMAs to engage with industry and CI entities to analyze the types of information already provided and to determine what constitutes a "covered cyber incident." This will mitigate the likelihood of a definition that will become burdensome for industry and CI entities.

3. Educate CI stakeholders and interagency partners.

Educating stakeholders through interagency meetings, public-partnership workshops, webinars, guidance and handouts ensures that all types of outreach methods are covered and clear information

[10] "Cyber Incident Reporting for Critical Infrastructure Act Of 2022 (CIRCIA)," Cybersecurity & Infrastructure Security Agency, last accessed Nov. 9, 2022. https://www.cisa.gov/circia; "Critical Infrastructure Sector Partnerships," Cybersecurity & Infrastructure Security Agency, last accessed Nov. 9, 2022. https://www.cisa.gov/critical-infrastructure-sector-partnerships; "Joint Cyber Defense Collaborative," Cybersecurity & Infrastructure Security Agency, last accessed Nov. 9, 2022. https://www.cisa.gov/jcdc.

[11] "Security Directive Pipeline-2021-02C," pages 3-4, Transportation Security Administration, last accessed Nov. 9, 2022. https://www.tsa.gov/sites/default/files/tsa_sd_pipeline-2021-02-july-21_2022.pdf.

can be easily shared. More broadly, there are many rules already in existence, and if CI entities are unaware or do not understand, the effectiveness of the incident reporting requirement will be limited.

Any entity directly or indirectly affected by the upcoming CIRCIA incident reporting regulations has an important role in shaping the rulemaking and should both partake in and request opportunities to provide constructive feedback. As such, CISA should host a workshop prior to the advanced notice for proposed rulemaking and notice for proposed rulemaking windows to ensure that affected entities have multiple chances to contribute and to convey how the information they receive will be used. Unfortunately, the issue of submitting information and not receiving information in return has been one of the main barriers to voluntary reporting to CISA. Industry and CI entities will need assurances on how the information they provide will be used, secured and shared back with them and anonymized with others.

IV. CONCLUSION

In conclusion, the R Street Cybersecurity team supports CISA's efforts to improve cybersecurity information-sharing and reduce cybersecurity risk across a sector or set of sectors using cybersecurity incident and risk management reporting requirements that are reasonable, balance industry concerns and provide usable data back to industry and CI entities. As CISA continues to engage with CI entities and the public, we urge CISA to consider harmonizing incident reporting requirements at the federal level to alleviate duplicative reporting requirements and support effective interoperable information-sharing with federal government rulemakings on incident reporting. We appreciate the opportunity to comment and remain a resource to you and others.

Respectfully submitted,
The R Street Cybersecurity Team

POC: Ayan Islam
Associate Policy Director, Cybersecurity and Emerging Threats
aislam@rstreet.org
R Street Institute
1212 New York Ave. NW
Suite 900
Washington, D.C. 20005