VIA REGULATIONS.GOV

July 1, 2024

Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
ATTN: CISA–2022–0010
2707 Martin Luther King Jr. Ave. SE
Washington, DC 20527

RE: Cyber Incident Reporting for Critical Infrastructure (CIRCIA) Reporting Requirements, Docket Number CISA–2022–0010

Dear Sir or Madam:

The Crypto Council for Innovation ("CCI") appreciates the opportunity to submit comments on the Notice of Proposed Rulemaking on Cyber Incident Reporting for Critical Infrastructure ("CIRCIA") Reporting Requirements ("Proposed Regulations").[1]

CCI is a global alliance of industry leaders in the digital assets space with a mission to communicate the benefits of digital assets and demonstrate their transformational promise. CCI members span the digital asset ecosystem and share the goal of encouraging the responsible global regulation of digital assets to unlock economic potential, improve lives, foster financial inclusion, protect national security, and disrupt illicit activity. CCI believes that achieving these goals requires informed, evidence-based policy decisions realized through collaborative engagement. To that end, CCI provides our comments and recommendations to the Proposed Regulations.

I. Summary

As an initial matter, CCI certainly supports the efforts of the Cybersecurity and Infrastructure Security Agency ("CISA") to mitigate cybersecurity risks to critical U.S. infrastructure and is committed to enhancing cybersecurity in financial services. In fact, CCI's member companies are highly involved in cybersecurity resilience in the crypto industry. We believe that the Proposed Regulations are a step in the right direction, but would recommend that CISA consider delaying publication of the final rule until federal agencies harmonize their reporting and information-sharing standards and requirements to ensure the effectiveness of the

[1] Notice of Proposed Rulemaking, *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements*, published May 6, 2024, 89 Fed. Reg. 37141.

final rule. We make this recommendation because we are particularly concerned that the lack of harmonization with other cyber incident reporting regimes will have deleterious outcomes, such as duplicative and confusing reporting requirements. Whether CISA ultimately decides to delay the rule or not, however, CCI nevertheless recommends that the agency address harmonization issues in its final rule as well as the following: (i) overly burdensome reporting requirements and (ii) data security risks associated with collecting vast swaths of data. Additionally, we would recommend that CISA further explore lessons from the existing efforts of industry to thoughtfully mitigate cyber risks.

II. Detailed Discussion

A. Lack of Harmonization with Existing Reporting Regimes

1. The Proposed Regulations lack harmony with the existing patchwork of federal and state incident reporting requirements, which could lead to confusion and duplicative reporting efforts by covered entities.

Dozens of federal and state cyber incident reporting regimes exist that clash with one another and force covered entities to duplicate their reporting efforts. Specifically, many of the regimes differ with respect to (i) the definition of a reportable cyber incident, (ii) reporting triggers and timelines, and (iii) content requirements. This can lead to confusion for covered entities, and thus, CISA's receipt of lower quality data.

In fact, the Department of Homeland Security ("DHS") itself has acknowledged the need to harmonize the disparate reporting regimes as evidenced by the release of its September 2023 report on the subject.[2] The report identifies 45 unique federal reporting requirements administered by 22 federal agencies. The report further highlights the need for agencies to adopt common definitions (e.g., the meaning of "cyber incident") and standardize reporting timelines. While we appreciate CISA's attempts to proffer standardized cyber incident definitions and reporting requirements through the Proposed Regulations, these efforts, alone, are insufficient. Absent legislation requiring other agencies to adopt CISA's proposed requirements, many covered sectors and entities will continue to face duplicative and unaligned reporting processes.

Within the financial services sector alone, there are eight different federal agencies with requirements for reporting cyber incidents. In addition to obligations to provide suspicious activity reports to FinCEN, some entities may need to report cyber incidents to the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Reserve Board, and/or the Commodity Futures Trading Commission. Moreover, some financial services

[2] *Harmonization of Cyber Incident Reporting to the Federal Government*, Department of Homeland Security (Sep. 23, 2023), https://rb.gy/83316b.

entities may have additional reporting obligations under the Securities and Exchange Commission's new cyber incident disclosure rules.[3] There are also several state reporting regimes. The New York State Department of Financial Services ("NYDFS"), for example, recently updated its cyber incident requirements for all licensed entities, including those conducting virtual currency business activity.[4] Because NYDFS is a state agency, covered entities who are subject to the agency's reporting requirements would not be exempt from CISA reporting requirements under any exception in the Proposed Regulations.

2. The reporting exemptions for entities that must already report to agencies with CIRCIA Agreements do not adequately address harmonization issues.

Under the Proposed Regulations, a covered entity with cyber incident reporting obligations to another federal agency may be exempt from CIRCIA requirements so long as (i) the agency has a "CIRCIA Agreement" in place with CISA and (ii) the contents and timing of the other agency's reporting requirements are "substantially similar" to CIRCIA's. However, CISA does not explicitly define what "substantially similar" means, and instead merely offers certain facts and circumstances for the covered entity to consider. Thus, even in instances where a covered entity must report to another agency with a CIRCIA Agreement, the covered entity must still analyze whether the competing requirements are substantially similar. This leaves CISA with broad discretion to deny exemptions to entities that must already report to other federal agencies.

CCI Recommendation:

CCI respectfully recommends that CISA should focus on harmonization efforts first and foremost before actually implementing a final rule. In doing so, CISA must take into account other federal reporting requirements, as well as state, local, and foreign[5] cyber incident reporting requirements. CISA should work directly with all federal agencies that require cyber incident reporting to standardize definitions, timelines, and processes, and to identify how to address any necessary exceptions to the overarching requirements due to individual agencies' critical needs.

Through these collaborative efforts, CISA should also assess the best technological infrastructure and practices for cyber incident reporting across agencies. CISA should minimize the burden on the private sector to report the same information through several channels, and

[3] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release Nos. 33-11216; 34-97989 (Jul. 26, 2023) [88 FR 51896 (Aug. 4, 2023)], https://rb.gy/71xsl9.
[4] Press Release, *Governor Hochul Announces Updates to New York's Nation-Leading Cybersecurity Regulations as Part of Sweeping Effort to Protect Businesses and Consumers from Cyber Threats* (Nov. 1, 2023), https://rb.gy/aqmbui.
[5] *See e.g.*, European Union Cyber Resilience Act (2024), available at: https://t.ly/LQsHq.

instead, expect federal agencies to communicate key information amongst themselves. Not only is this a more efficient method of data sharing, but also it frees up covered entities to focus on responding to cyber incidents rather than expending critical resources to prepare and submit duplicative reports.

B. Overly Burdensome Reporting Requirements

1. Successful implementation of CIRCIA will prove difficult since the Proposed Regulations would require a highly detailed and resource-intensive level of reporting.

In order to comply with the data sharing requirements under the Proposed Regulations, covered entities will have to expend significant technological and workforce resources to retain and track the proposed data elements. This is because the Proposed Regulations call for an exceedingly detailed narrative on each cyber incident in addition to granting CISA discretion to submit follow-up requests on any additional items it deems pertinent. In fact, the requirements under the Proposed Regulations extend beyond those originally contemplated under CIRICIA.

To elaborate, CIRCIA calls for the following information to be reported: (i) identity of the covered entity, (ii) relevant contact information, (iii) third party authorization for third party entities that submitted a report on behalf of the covered entity, (iv) a description of the covered incident itself, (v) pertinent security vulnerabilities and controls that were in place, and (vi) any known information about the identity of the perpetrator. The Proposed Regulations would further expand upon CIRCIA's original requirements by adding the following: (i) information on mitigation and response activities, including the covered entity's assessment of the effectiveness of these activities and (ii) any other relevant data or information.

Although the proposed field to optionally include other relevant data may be appropriate, seeking "information on mitigation and response activities, including the covered entity's assessment of the effectiveness of these activities" will likely require significant additional work and detract from a covered entity's response efforts during a critical period. A covered entity may not even be able to provide such an assessment within the required period of time—not because the entity does not wish to, but because 72 hours may not be sufficient time to provide the substantive analysis that CISA requires. Accordingly, this provision could tie-up covered entities' resources and reduce their front-line capacity to address immediate damage and prevent risks to other institutions in the wake of a cyber incident.

Finally, the Proposed Regulations' supplemental reporting requirements may also prove unduly burdensome. CISA interprets "substantial new or different information" as anything responsive to a required data field in a CIRCIA report. Thus, an impacted entity will likely have

to provide numerous supplemental reports during a single incident response. As previously mentioned, such reporting requirements could unintentionally pose operational risks by diverting resources away from the cyber incident itself that could result in financial harm to the entity or its consumers.

2. Not only will information collection under the Proposed Regulations prove to be burdensome for covered entities, but it will also be difficult for CISA itself to manage the receipt of reported information.

CISA estimates that more than 316,000 companies will be considered covered entities under the final rule and that CISA will receive roughly 15,000 cyber incident reports annually. However, the NPRM's Preliminary Regulatory Impact Analysis acknowledges the "high degree of uncertainty" around the expected number of reports.[6] Given the unprecedented number of entities that will be covered and the likelihood for overreporting as many firms seek to avoid compliance violations when the requirement obligations are nascent, CISA is likely to receive far more than the 15,000 annual incident reports it currently projects. Thus, CISA will likely have to expend considerable resources administering this regime. However, the Proposed Regulations are not clear as to how CISA intends to manage these new responsibilities. Specifically, it is unclear how CISA will manage such a large volume of information, share reported information with other federal agencies, and provide timely and useful alerts on cyber incidents to the public.

CCI Recommendation:

CISA should streamline reporting requirements as much as possible and not seek data beyond what CIRCIA specifies, except for adding an *optional* space for entities to offer "additional relevant information." CISA should also consider adding a materiality threshold determination of the cyber incident before triggering the 72-hour time period.

Before implementing the final rules, CISA should ensure that it has the capacity to manage its proposed reporting regime. In the final rules, CISA should further explain this capacity as well as how it plans to share reported information with other federal agencies.

C. Data Security Concerns

As discussed, CISA will have to collect and maintain large volumes of data in order to successfully deploy its proposed reporting regime. Collecting such a significant amount of data increases risks to maintaining privacy and security since such repositories could serve as honeypots for bad actors. Moreover, data sharing among federal agencies further increases the

[6] Risk Impact Analysis, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Proposed Rule, 89 Fed. Reg. 23644 (April 4, 2024), https://rb.gy/osgjjk.

risk that sensitive information will get into the wrong hands, especially when cybersecurity standards and practices are uneven throughout the government.

CCI Recommendation:

CISA should put measures in place to ensure that sensitive cyber incident information reported by the private sector is protected from inadvertent disclosure. The first step in doing so would be to work with other federal agencies to ensure they have fully implemented Executive Order 14028 and that Zero Trust Architecture is established internally throughout the US government.[7] The US Government Accountability Office in April 2024 recommended that CISA undertake additional actions to fully complete the executive order's requirements.[8] Additionally, CISA should ensure that safeguarding data from inadvertent disclosure includes protections of the Freedom of Information Act and applicable privileges.

III. Opportunities for Public-Private Partnerships

CCI appreciates CISA's willingness to engage with the private sector as the agency attempts to effectively implement CIRCIA. As CISA finalizes these rules, we encourage the agency to consider how industry-government partnerships can further support its goals. Like traditional financial institutions, members of the digital asset industry have already been working to improve information-sharing to address cyber incidents, including through the Security Alliance[9] and the Crypto-ISAC.[10] Such efforts are likely to improve the speed and substance of cyber incident reporting around digital assets. CISA may find benefit in learning from the methodologies and best practices of industry-led efforts before enacting new federal reporting requirements.

IV. Conclusion

We believe that CIRCIA will play a vital role in mitigating malicious cyber attacks, but we urge CISA to revise the proposed rule in the aforementioned areas to ensure that its requirements (i) align with those of other federal agencies; (ii) adequately support CISA's goals of promoting efficient information sharing; and (iii) do not unintentionally create additional data security and privacy risks. We further encourage CISA to partner with the private sector in order to gain lessons from industry to help achieve CIRCIA's goal of establishing an effective cyber incident reporting regime.

---

[7] White House Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021), https://rb.gy/c72g1d.
[8] *Cybersecurity: Implementation of Executive Order Requirements is Essential to Address Key Actions*, Government Accountability Office (Apr. 18, 2024), https://rb.gy/1ppgo9.
[9] Press Release, *Security Alliance (SEAL) Launches Free, Crypto-Native ISAC* (Apr. 18, 2024), https://rb.gy/r3px0l.
[10] Ian Allison, *Crypto Gets Another 'Neighborhood Watch' to Guard Against Hacks*, CoinDesk (May 6, 2024), https://rb.gy/6cuczz.

CCI is committed to working with CISA and other federal agencies for the security of U.S. cyber infrastructure. We look forward to hearing from CISA on this matter.

***

Respectfully submitted,

Sheila Warren
Chief Executive Officer
Crypto Council for Innovation

Ji Hun Kim
Chief Legal & Policy Officer
Crypto Council for Innovation

Yaya J. Fanusie
Director of Policy for AML & Cyber Risk
Crypto Council for Innovation