Consumer Technology Association™

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

July 3, 2024

via Regulations.gov
Todd Klessman
Cybersecurity and Infrastructure Security Agency
1110 N. Glebe Road
Arlington, VA 20598-0630

Re: Cyber Incident Reporting for Critical Infrastructure Notice of Proposed Rulemaking – Docket No. CISA-2022-0010

Mr. Klessman,

Consumer Technology Association (CTA)®[1] appreciates the opportunity to comment on the Cybersecurity and Infrastructure Security Agency (CISA) *Notice of Proposed Rulemaking* (*NPRM*) to implement the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).[2] We share CISA's commitment to ensuring the security of U.S. critical infrastructure. Although the majority of CTA members provide consumer products designed to support non-critical functions, many of CTA's more than 1300 members provide innovative technology products and services that play a role in the critical infrastructure ecosystem.

CTA recognizes the vital role of information sharing—across sectors and between the private sector and government—in spotting trends and addressing ecosystem-wide threats.[3] As the hub for federal cybersecurity risk management, CISA has the potential to enhance this work through CIRCIA implementation. However, doing so will require carefully balancing CISA's imperative to gather information across the broad, diverse set of critical infrastructure owners

[1] As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®—the most powerful tech event in the world.

[2] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644 (Apr. 4, 2024) (*NPRM*).

[3] For example, CTA is working closely with the Federal Communications Commission (FCC) and stakeholders across the IoT ecosystem to build the U.S. Cyber Trust Mark program to give consumers more information about the cybersecurity of the connected products they buy and ensure that those products meet certain standards. *See* Press Release, Laura Ambrosio, CTA, *U.S. Cyber Trust Mark Hits the Mark* (Mar. 14, 2024), https://www.cta.tech/-Resources/Newsroom/Media-Releases/2024/March/U-S-Cyber-Trust-Mark-Hits-the-Mark. CTA has also supported the vital role of coordinated vulnerability disclosure aligned to international standards. *See, e.g.*, David Grossman & Mike Bergman, *Coordinated Disclosure of Cyber Vulnerabilities is a Win for Consumers and Industry*, CTA (2022), https://www.cta.tech/Resources/Articles/2022/Coordinated-Disclosure-of-Cyber-Vulnerabilities-is.

and operators with the need to ensure that collected information is useful and stakeholders can act on that information to drive meaningful security improvements.

As the voice of the consumer technology industry, CTA is concerned that the proposed rules take an overly broad approach to the scope of covered entities and covered cyber incidents, sweeping in consumer-focused technology and companies that, although important for our economy, are not critical infrastructure within the meaning of CIRCIA. As a result, the proposed approach risks undermining both the CIRCIA program and CISA's broader ability to effectively collaborate with the private sector and international partners. CTA urges CISA to narrow the scope of the final rules so that they target the most significant cyber incidents impacting truly critical infrastructure and engender productive partnership across the ecosystem.

To achieve a positive cycle of incident reporting that generates actionable insights, CISA should focus on substantial cyber incidents that pose actual threats to U.S. critical infrastructure, consistent with the risk-based scope Congress imbued in the statute. CISA can materially support partnership in this effort by ensuring the robust entity and information protections included in the statute apply to all entities that report in good faith accordance to the rules, supporting the covered entity experiencing the cyber incident, and by ensuring ongoing engagement as these rules take shape and evolve over time. We elaborate on these points below.

I. Refined Definitions of "Covered Cyber Incident" and "Covered Entity" Will Ensure Limited Resources Address Threats to U.S. Critical Infrastructure

Tailoring the scope of CIRCIA's reporting requirements will make for a more effective program by optimizing resources both within CISA and among reporting entities and encouraging reciprocal policies in international jurisdictions. Conversely, the overly broad scope proposed in the *NPRM* will strain CISA's ability to process and use reported information, divert vital resources within critical infrastructure entities away from operational incident response and preparedness to compliance activities and raise challenges among international partners. While it may be prudent to scope the rules more narrowly in a variety of ways, we recommend four key refinements to target reporting consistent with the focus of the statute.

First, covered entities should only report when a substantial cyber incident emanates from the part of the entity that is supporting critical infrastructure. The *NPRM* takes an exceptionally broad view of the incidents that must be reported by an equally broad set of covered entities (i.e., any entity in a critical infrastructure sector that exceeds the small business threshold or meets a sector-based criterion).[4] However, myriad consumer products—

[4] *See NPRM*, 89 Fed. Reg. at 23766-67 (defining "covered entity," "covered cyber incident" and "substantial cyber incident"). The *NPRM* proposes to define a "covered entity" as an entity in a critical infrastructure sector that (a) exceeds the small business threshold (set forth in 13 CFR part 121); or (b) meets a sector-based criterion. *See id.* at 23767 (Proposed § 226.2). These criteria, which span all 16 critical infrastructure sectors designated under Presidential Policy Directive 21 (PPD-21), are themselves extremely broad. The definition of "substantial cyber incident" similarly extends beyond the "significant cyber incidents" that CIRCIA is designed to address. *Id.* at 23767.

offered by companies that may perform functions listed in the *NPRM*'s sector-specific criteria—do not support critical functions and if compromised would not impact the core interests Congress designed the statute to address.[5] Indeed, many consumer technology companies include a variety of business components, some of which may support critical infrastructure functions and some of which may serve lower risk functions across the broader commercial marketplace. Although these companies may be considered a covered entity under the proposed definition for the critical infrastructure functions they support in one business component, a "substantial cyber incident" may not pose an actual threat to critical infrastructure if it occurs solely within a non-critical business component. CISA should clarify that entities do not need to report under CIRCIA in such instances.[6] More, the frequency of updates on cyber incidents reported by a covered entity should be left to the discretion of the entity. Due to the constraint of resources, daily updates to CISA will not be feasible for industry to support. Further covered cyber incidents should have a nexus with the PPD-21 definition of critical infrastructure.[7]

Second, covered entities should report only when the cyber incident directly impacts critical infrastructure *in the United States*. Many consumer technology companies serve markets across the world via transactions that have no nexus to the United States. CISA should not require such a company to report under CIRCIA if the incident in question does not directly affect U.S. critical infrastructure. Congress made clear in the statute that CIRCIA is focused on U.S. critical infrastructure for good reason. The United States has a compelling interest in gathering information about major cyber incidents impacting domestic infrastructure. However, an extraterritorial application of these rules could jeopardize national security by encouraging foreign governments to adopt similar requirements that seek sensitive information about U.S. critical infrastructure. It may also conflict with foreign privacy and data protection laws and undermine CISA's ability to collaborate effectively with international counterparts.

---

[5] As the *NPRM* describes, "CIRCIA requires CISA to review covered cyber incidents that are 'likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States' and to 'identify and disseminate ways to prevent or mitigate similar incidents in the future.'" *Id.* at 23651.

[6] This focus would also ensure CISA's approach aligns to existing federal policy (e.g., in implementing EO 13873, the Department of Commerce acknowledged that "ICTS Transactions solely involving personal ICTS hardware devices, such as handsets, do not warrant particular scrutiny.") Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909, 4913 (Jan. 19, 2021). Similarly, much of the automotive sector—which includes after-market consumer devices like radios, lighting, and other products that are segmented from the core function of the vehicle—should not be subject to CIRCIA reporting requirements.

[7] PPD-21 defines the term "critical infrastructure" as having "the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e))," namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. News Release, The White House, *Presidential Policy Directive/PPD-21*, at 12 (Feb. 12, 2013), https://www.cisa.gov/-sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf.

Third, all four prongs of impacts that constitute a substantial cyber incident should be qualified by a "substantial" or "significant" impact. This includes explicitly adding a "substantial" qualifier to prong 3; "A substantial disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services." For prong 4, we recommend CISA add a "substantial" qualifier as well, similar to the language in prongs 1 and 2.

Fourth, the final rule should clarify that entities that do not actually own or operate critical infrastructure—such as trade associations—are not "covered entities" under the CIRCIA rules. Per the statute, the final rule should require reporting related to critical infrastructure whose compromise would result in "demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States."[8] The *NPRM* helpfully notes that some entities that are active participants in different critical infrastructure sectors and communities are not considered part of one or more critical infrastructure sector for the purposes of CIRCIA.[9] CISA should clarify that similarly situated entities—such as trade associations and standards-setting bodies—also fall outside the definition of "in a critical infrastructure sector."

II. To Promote Candor and Operational Response, CISA Must Ensure Robust Protections for Reporting Entities and the Information They Share

In the context of cyber threat information sharing, the United States has long recognized the importance of strong legal and practical protections for both the sensitive information reported and the reporting entities themselves.[10] Congress wisely included such protections in CIRCIA.[11] Skirting these protections would undermine the positive cycle of information sharing CISA aims to achieve. CISA should clarify in the rules and remain vigilant in ensuring that covered entities who report in good faith accordance with the CIRCIA rules are entitled to all protections under the statute. For example, the rules should specify that information shared by CISA with another government entity may not be used as the basis for initiating an enforcement inquiry, investigation, or in prosecuting an enforcement action, including but not limited to actions against a covered entity's executives and employees. Further, the Request for Information and subpoena themselves that may follow an entity failing to report should receive the same protections as the submitted information is accorded in the proposed rules.

---

[8] *See* Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, Div. Y, 136 Stat. 49, 1038-59 (2022) (codified at 6 U.S.C. § 681b et. seq. (CIRCIA), § 2240(16)).

[9] *NPRM*, 89 Fed. Reg. at 23678 (such entities include advertising firms, law firms, political parties, graphic design firms, think tanks, and public interest groups).

[10] *See, e.g.*, Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, 129 Stat. 2242, 2936 (codified at 6 U.S.C. § 1501 et. seq.).

[11] CIRCIA § 2245 (limiting the types of activities for which the federal government may use reported information; ensuring confidentiality, privacy and civil liberties, and digital security; prohibiting use of reported information in regulatory actions; and protecting reporting entities and information from undue disclosure via Freedom of Information Act requests or waivers of privilege, trade secret protection, etc.).

III. Prioritize Steps to Harmonize CIRCIA With Other Incident Reporting Requirements

CTA appreciates CIRCIA's attempt to streamline and harmonize different federal cyber incident reporting requirements and CISA's attempt to harmonize requirements by introducing the concept of CIRCIA agreements. We would urge CISA to finalize CIRCIA agreements to eliminate duplicative reporting requirements before the final rules take effect. For example, CSPs that have FedRAMP authorized services must report incidents in a shorter timeframe and the health sector has specific reporting rules in the event of a cybersecurity breach under the Health Insurance Portability and Accountability Act.

Additionally, CISA should consider streamlining the initial reporting requirements to make them more consistent with the elements laid out by Congress, which could help harmonize CIRCIA with other existing requirements. The many additional details required for a cyber incident report, as proposed in the *NPRM*, could be onerous and make it difficult to identify other reporting requirements with "substantially similar information" required as CIRCIA.

IV. Provide More Details on How Information Will Be Shared and Protected

While the *NPRM* lays out instances when CISA will share information with other government agencies, we encourage CISA to provide more details on when and how the information will be shared. This is particularly important when sharing reports that may include victim information that must be safeguarded.[12] We recommend that CISA share its plans for how to safeguard the information contained in CIRCIA reports, and how other government agencies with whom CISA shares the reports will do the same. Finally, we believe that CISA should limit the retention period of the information contained in the reports as a further measure to safeguard the information and minimize the risk that the information will be accessed by unauthorized actors.

V. Given the Unprecedented Nature of CIRCIA, Further Opportunities for Dialogue With Industry Are Crucial to Facilitate Better Partnership and More Effective Rules

CIRCIA implementation marks a significant shift in the role CISA plays in support of the nation's cybersecurity risk management, which will have a profound impact on the technology marketplace based on the broad scope of the *NPRM*. To get this right, and foster a positive feedback loop of information sharing, CISA needs more open and robust dialogue with stakeholders than can be afforded by two comment cycles and ad hoc listening sessions. Other agencies have established models CISA can easily adopt.[13] Building a strong public record that allows effected entities to dynamically engage with CISA staff will support more effective rules now, and as the CIRCIA rules necessarily evolve over time.

[12] CISA should also adopt a clear process for requesting and approving confidential treatment of sensitive information shared in these reports to incentivize candor and protect reporting entities.

[13] For example, the FCC has addressed this through its permit-but-disclose/*ex parte* process. *See, e.g.*, 47 C.F.R. § 1.1206.

*****

CTA shares CISA's commitment to enhancing the security of U.S. critical infrastructure through targeted reporting to generate insightful threat analysis and drive strategic cyber investments. However, proposals in the *NPRM* will hinder this effort in an overly broad compliance regime that could harm the innovative consumer technology industry. Instead, CISA should narrow the scope of covered entities and covered cyber incidents under the *NPRM* and support ongoing partnership through robust protections and an ongoing stakeholder engagement. CTA welcomes further discussion with CISA on these important topics.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ J. David Grossman*
J. David Grossman
Vice President, Policy & Regulatory Affairs

/s/ Mike Bergman
Mike Bergman
Vice President, Technology & Standards