October 29, 2024

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane SW
Washington, DC 20598

Re: *Cyber Incident Reporting for Critical Infrastructure Act Implementation*

Dear Director Easterly,

The undersigned associations, whose member companies represent a vast and diverse cross-section of the U.S. critical infrastructure ecosystem, share concerns regarding the Cybersecurity and Infrastructure Security Agency's ("CISA's") Notice of Proposed Rulemaking ("NPRM")[1] to implement the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA").[2] As organizations on the frontlines protecting the nation's critical functions, we support Congress's goals in enacting CIRCIA and share CISA's commitment to enhance ecosystem-wide security in this rulemaking.

First, to support the success of the final rule, we respectfully request that CISA establish an *ex parte* process to facilitate further stakeholder engagement and dialogue to implement CIRCIA. Continued collaboration with industry during a complex rulemaking like this will help strike an appropriate balance between providing CISA with information it needs to execute its responsibilities while allowing cybersecurity teams to focus on critical remediation and response activities.

Second, we offer key recommendations to address widespread concerns from our organizations and others throughout the docket, including several members of Congress. Indeed, in his letter regarding the NPRM, Senate Homeland Security and Governmental Affairs Committee Chairman Gary Peters said CIRCIA "was drafted to ensure that critical infrastructure owners and operators report cyberattacks and ransomware payments to the federal government, allowing our nation's cybersecurity agencies to help them respond to and recover from significant attacks and prevent future breaches."[3] Chairman Peters emphasized the need for regulations that "effectively prioritize efforts to strengthen cybersecurity defenses for critical infrastructure, and that do not overburden critical infrastructure owners and operators and pull our cybersecurity professionals away from their mission to focus on compliance."[4] As

---

[1] CISA, *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements*, Notice of Proposed Rulemaking, 89 Fed. Reg. 23644 (Apr. 4, 2024) ("NPRM").

[2] Consolidated Appropriations Act, Pub. L. No. 117-103, 136 Stat. 49, 1038-59, Div. Y – Cyber Incident Reporting for Critical Infrastructure Act (2022), https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf, codified at 6 U.S.C. § 681b *et. seq.* ("CIRCIA").

[3] Comments of Gary C. Peters (July 3, 2024).

[4] *Id.*

Representative Yvette Clarke previously stated, "our intent was that reporting requirements would be appropriately tailored to limit overreporting and ensure that CIRCIA ultimately yields the security benefits we intended… we did not intend to subject everyone or every incident to reporting."[5] Similarly, House Cybersecurity and Infrastructure Protection Subcommittee Chairman Andrew Garbarino stated, "It is imperative that we get the CIRCIA rule right. CIRCIA should serve as the standard, not another regulation standing in the way of effective cyber defense."[6]

While we recognize CISA's interest that its rule to implement CIRCIA generate sufficient data in a timely manner, we share Chairman Peters' concern that "the effect of this proposed rule would fail to hit this mark."[7] Moreover, the breadth of the proposed rule could jeopardize the productive partnership the critical infrastructure sectors and the U.S. government have built over the last half century. As commenters explain, this is because the proposed rule would induce over-reporting of non-substantial incidents and divert private sector resources away from prevention and deterrence.[8] The statute makes clear that not all cyber incidents should be treated as reportable and not all entities operating in a critical infrastructure sector should be treated as covered entities.[9] As currently proposed, the rule would significantly increase reporting obligations for regulated entities[10] and shift critical infrastructure owners into a compliance mindset. Consequently, these entities would be forced to spend vital time and resources on compliance activities instead of operational prevention, detection, and response efforts to promote resilient American infrastructure.

For these reasons, we recommend that CISA adopt an *ex parte* process to facilitate ongoing and iterative stakeholder engagement to advance our mutual goal that CIRCIA is implemented in a manner consistent with congressional intent.

I. Consistent with the APA, Adopt an *Ex Parte* Process for Ongoing Stakeholder Engagement.

CIRCIA implementation marks a significant shift in CISA's role to support the nation's cybersecurity risk management, and will have a profound impact across every major sector of the

---

[5] *Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking*, HOMELAND.HOUSE.GOV, May 1, 2024, https://homeland.house.gov/hearing/surveying-circia-sector-perspectives-on-the-notice-of-proposedrulemaking/.

[6] Comments of Andrew Garbarino (May 1, 2024).

[7] Peters Comments at 1.

[8] *See, e.g.*, American Medical Association Comments at 2; Crypto Council for Innovation at 4-5; Consumer Technology Association (CTA) Comments at 2; CTIA Comments at 9-13; Edison Electric Institute (EEI) Comments at 4; Epic Systems Corporation Comments at 3; Financial Sector Trades (ABA, BPI, IIB, SIFMA) Comments at 2; Kaiser Permanente Comments at 1-2; Massachusetts Health Data Consortium Comments at 2; National Federation of Independent Business (NFIB) Comments at 2; NCTA – The Internet and Television Association (NCTA) Comments at 4; Ohio Credit Union League Comments at 2; OrbitFab Comments at 1; USTelecom Comments at 2; Virginia Hospital & Healthcare Association (VHHA) Comments at 2, 4-5; Win-Tech Comments at 1.

[9] 6 U.S.C. § 681b(c)(1)–(2).

[10] *See, e.g.*, CTIA Comments at 9-13 (July 3, 2024).

economy. We commend CISA for its ongoing efforts to safeguard the nation's critical infrastructure. However, given the complexities and far-reaching implications of CIRCIA, we believe that additional stakeholder input is essential to ensure CISA's implementing regulation achieves its intended objectives without unintended consequences. As Chairman Peters noted, "cybersecurity, and particularly cyber incident reporting, is a complex and ever-evolving area. Writing rules for cybersecurity requires hard work and strong collaboration."[11] With this in mind, as stakeholders representing numerous sectors, we urge CISA to adopt an *ex parte* process for ongoing engagement – both to tailor these rules at the outset and refine them as we gain experience with CIRCIA reporting and adapt to cyber landscape shifts over time.[12] Adopting such a process would also be consistent with Chairman Peters' recommendation that CISA "carefully consider public comments from the cybersecurity community, critical infrastructure sectors, and other valuable partners, and re-scope parts of the proposed rule to address these comments."[13]

Iterative *ex parte* processes like this are routine in many rulemaking proceedings and particularly valuable in foundational, complex rulemakings like CIRCIA. Representatives Thompson, Clarke, and Swalwell acknowledged this in their CIRCIA comment letter saying, "proper implementation of CIRCIA requires a full understanding of the many technical issues involved in a rule of this significance and complexity, and consultation with impacted entities will be essential to determining how the rule will affect critical infrastructure.[14]

Stakeholders have deep and longstanding experience engaging with other agencies whose *ex parte* processes support the requirements of the Administrative Procedure Act (APA) and these processes can serve as models for CISA.[15] CISA might also consider establishing an engagement model that leverages various Sector Coordinating Councils where industry representatives commonly collaborate with government partners on a broad range of policy topics related to critical infrastructure security and resilience. Developing a strong public record that allows affected entities to dynamically engage with CISA leaders and staff is imperative for the success of the proceeding; it will engender more effective rules now, and into the future.

---

[11] Peters Comments at 1.

[12] *See, e.g.*, Business Roundtable (BRT) Comments at 3-4; CTA Comments at 5, CTIA Comments at 39-40; NCTA Comments at 8, 34; USTelecom Comments at 17-18; VHHA at 4. *See also* Aerospace Industries Association Comments at 2, 6 (recommending the Cybersecurity Forum for Independent and Executive Branch Regulators be opened to critical infrastructure sector representatives for similar reasons). *See also, e.g.,* Red Wind Casino Comments, The Cherokee Nation Comments, Tribal-ISAC Comments, Morongo Band of Mission Indians Comments, Sycuan Band of the Kumeyaay Nation Comments, Yocha Dehe Wintun Nation Comments (disagreeing with CISA's determination that tribal consultation is not warranted in this proceeding and urging either exemption from the rules or formal consultation). These comments underscore that additional and ongoing opportunities for engagement with CISA on CIRCIA implementation are necessary.

[13] Peters Comments at 2.

[14] Comments of Bennie G. Thompson, Yvette D. Clarke, and Eric M. Swalwell (Jul. 3, 2024).

[15] *See, e.g.*, CTIA comments at 39, citing 47 C.F.R. § 1.1200 (FCC *ex parte* rules); U.S. Department of Transportation, Memorandum for Secretarial Officers and Heads of Operating Administrators: Guidance on Communication with Parties outside of the Federal Executive Branch (Ex Parte Communications) (Apr. 19, 2022), https://www.transportation.gov/sites/dot.gov/files/2022-04/Guidance-on-Communication-with-Parties-outside-ofthe-Federal-Executive-Branch-%28Ex-Parte-Communications%29.pdf.

House Homeland Security Committee leaders echoed the importance of this engagement when articulating a similar concern "that limiting feedback to written comments received in advance of the published deadline will be insufficient for CISA to fully engage with stakeholders.[16]

With that being the case, soliciting additional input through *ex parte* discussions with industry can provide CISA with a nuanced understanding of how proposed regulations may impact the real-world operations of critical infrastructure. This would be especially beneficial as CISA seeks to strike a balance between regulatory requirements and the practical realities of maintaining uninterrupted services across sectors underpinning the nation's economy and security. Moreover, a robust public comment process is indispensable to protecting CIRCIA rules from legal challenges, especially in light of the Supreme Court's decision in *Loper Bright Enterprises v. Raimondo.* In particular, without a more robust *ex parte* and stakeholder feedback process, the agency increases its risk of not arriving at the "single best meaning" of CIRCIA.[17]

Simply put, the public record to date is insufficient, and a single round of comments in response to CISA's NPRM will not allow the agency to effectively capture and leverage stakeholder feedback.

Absent increased industry engagement, CISA's proposed regulation may inadvertently impose requirements that hinder rather than help our sectors maintain security and operational efficiency. For instance, overly broad reporting requirements could lead to an overwhelming volume of data submissions, thereby diluting the focus on truly significant incidents.

II. Narrow the Scope of CIRCIA Reporting to Enable a Positive Cycle of Information Sharing and Actionable Insights.

Stakeholders share optimism that a targeted CIRCIA program will enhance information sharing and incident awareness, ultimately raising the collective cyber posture of U.S. critical infrastructure. As recent CISA Executive Assistant Director Eric Goldstein described, a successful CIRCIA program will create a positive cycle of information sharing between the private sector and government "to drive investment in building more effective products and deploying more effective enterprise controls that are responsive to the threats we are seeing such that our adversaries need to burn a previously unknown vulnerability or a novel exploit for every single intrusion."[18] However, to achieve this outcome, it is critical that CISA refine the definitions proposed in the NPRM to more effectively target reporting to substantial cyber incidents impacting U.S. *critical* infrastructure – not all infrastructure.[19] At minimum, this means:

---

[16] Thompson, Clarke, and Swalwell Comments at 9.

[17] *See Loper Bright Enterprises v. Raimondo*, 144 S. Ct. 2244, 2266 (2024).

[18] *See* CSIS event "Cyber Incident Reporting in the Communications Sector" at 8:06.

[19] *See* Peters Comments at 1 (cautioning that "[t]he proposed rule is overbroad and needs additional clarity in the definitions for covered incident, covered entity, and others…").

- **Adopting a definition of "*covered cyber incident*" that captures incidents directly impacting the operational capabilities of the critical infrastructure entity, as determined by the owners and operators, and only where such operational capabilities fall within congressional intent.** Specifically, CISA should limit the definition to incidents that directly impact the portion of the covered entity that provides a service or function that makes the entity covered (i.e., the part that supports critical infrastructure); exclude incidents that do not involve U.S. infrastructure; establish a higher substantiality threshold; and narrow the trigger for reporting supply chain incidents.[20]

- **Narrowing the definition of "*covered entity*" to assets with the ability to affect the secure and reliable operation of U.S. critical infrastructure and delivery of critical services.** Specifically, CISA should clarify that "covered entities" (i) only include U.S.-based subsidiaries of multinational companies (i.e., foreign subsidiaries/affiliates are out of scope); (ii) only include a company's offerings that constitute "critical infrastructure" (perhaps as informed by PPD-41 or a National Criticality Assessment); and (iii) only include "active participants" in a critical infrastructure sector (e.g., not trade associations, standards bodies, or other organizations that may be considered part of the sector but do not directly support critical infrastructure).[21] CISA should ensure that "covered entities" understand their designation and identify points-of-contact for CISA within each.[22]

- **Clarifying that a "*reasonable belief*" about the substantiality of a cyber incident is a fact-specific and context-specific matter.** Specifically, CISA should clarify that while many entities may be able to establish a reasonable belief that a reportable substantial cyber incident has occurred within hours, not days, for some entities these assessments may take longer (e.g., depending on the complexity of the incident, involvement of third parties, and other factors).[23] CISA's assumption that this can be done in all cases within hours will only encourage companies to over-report insubstantial incidents. Accordingly, a covered entity's formation of a reasonable belief should be presumed to be in good faith absent evidence of "unreasonable delay".

---

[20] *See, e.g.,* Alliance for Automotive Innovation (Auto Innovators) Comments at 4; American Chemistry Council (ACC) Comments at 3; American Council of Life Insurers Comments at 3; BRT Comments at 7; Coalition, Inc. Comments at 2; CTA Comments at 3-4; CTIA Comments at 14-20; Information Technology Industry Council (ITI) Comments at 5-7; Depository Trust & Clearing Corporation Comments at 4; EEI Comments at 13-18; Ernst & Young Comments at 3; Food and Agriculture-Information Sharing and Analysis Center Comments at 2-3; Georgia Tech Research Institute Comments at 1-2; Henry Ford Health at 2; National Defense Information Sharing & Analysis Center Comments at 2; VHHA Comments at 3-4; Virginia Department of Transportation Comments at 1.

[21] *See, e.g.*, ACC Comments at 3-5; Auto Innovators Comments at 2-3; CTA Comments at 2-5; CTIA Comments at 26-29; Cybersecurity Coalition Comments at 2-3; Fairview Health Services (Fairview) Comments at 2-3; ITI Comments at 3-5; Microsoft Comments at 2-3; Premier Comments at 1, 3-4; National Association of Manufacturer (NAM) Comments at 3-4; The Healthcare Trust Institute Comments at 2-3; U.S Chamber of Commerce Comments at 8-9.

[22] *See* ITI Comments at 5; HackerOne Comments at 2.

[23] *See, e.g.*, Core Electric Cooperative (CORE) Comments at 3, 5; CTIA Comments at 20-21, EEI Comments at 6-7, 27-29; ITI Comments at 8-9; Joint Comments of Institute for Security and Technology and the Cyber Threat Alliance at 4; USTelecom Comments at 8; VHHA Comments at 5.

Our suggestions are consistent with Congressional intent. As Chairman Peters explained, "The proposed rule is overbroad and needs additional clarity in the definitions for covered incident, covered entity, and others."[24] CISA must "be able to properly ingest, triage, and analyze the reported information and use the data to improve cybersecurity recommendations and support critical infrastructure."[25] Finally, narrowing the scope of the CIRCIA reporting requirements—in line with record support and congressional intent—will be important to ensure that the rules can pass muster under *Loper Bright.*[26]

III. Proactively Harmonize CIRCIA Implementation with Existing Regulatory Requirements to Optimize Operational Response.

Recognizing the myriad reporting requirements facing most entities subject to CIRCIA, we agree with Chairman Peters that "CISA should proactively and earnestly communicate on the status of formulating the information sharing agreements with other federal agencies to ensure that these mechanisms are in place before the final rule is issued and validate that these agreements will be effective mechanisms for improving cybersecurity and supporting the owners and operators of critical infrastructure."[27] In response to the NPRM, commenters universally underscored the need for harmonization amid dozens of overlapping reporting requirements at the state, federal, and international levels. The current landscape of overlapping and sometimes conflicting regulations poses significant challenges to our sectors, creating inefficiencies and potential compliance risks.

We urge CISA to prioritize harmonization by, for example, leveraging the Cyber Incident Reporting Council; harmonizing with the Federal Acquisition Regulation Council and other government agencies and entities to achieve consistent and reasonable requirements; approaching its evaluations of "substantially similar" with flexibility to maximize the number of CIRCIA Agreements reached; and creating a "Common Form" for federal incident reporting and providing this form as a voluntary option for covered entities to use CISA as a single point of entry for federally-mandated cyber incident reports.[28] The more CISA can help streamline reporting requirements for covered entities, the more effective those entities can be in operational response. A harmonized approach, developed through close collaboration with relevant stakeholders, would not only streamline compliance but also enhance the overall cybersecurity of our nation.

---

[24] *See* Peters Comments at 1.

[25] *Id.*

[26] *See* Loper Bright at 2268 ("Courts interpret statutes, no matter the context, based on the traditional tools of statutory construction . . . .").

[28] *See, e.g.*, American Hospital Association Comments at 2; Auto Innovators Comments at 4; BSA Comments at 2; BRT Comments at 1-3; CORE Comments at 3-4; CTA Comments at 5; CTIA Comments at 32-38; Cybersecurity Coalition Comments at 4; ITI Comments at 2-3; Joint Letter from ABA, APPA, BPI, EEI, NRECA, NTCA, SIFMA, USTelecom at 2; NCTA Comments at 7-8, 25-31; Edison Electric Institute Comments at 37-38; Fiserv Comments at 5-6; Illinois Credit Union League Comments at 2; OrbitFab Comments at 2; Sure Secure Solutions (Sure Secure) Comments at 2; The Clearing House Payments Company Comments at 3-4; USTelecom Comments at 10-11; Win-Tech Comments at 2.

IV. Strengthen Safeguards for Information and Protections Against Liability to Support Cyberattack Victims and Foster Candor in Reporting.

Congress included vital protections in CIRCIA to ensure the rules support our collective mission to enhance the security of U.S. critical infrastructure without overburdening or diverting the work of our cybersecurity professionals or revictimizing entities subject to cyberattacks. To promote candor and foster the virtuous cycle of information sharing prerequisite to CIRCIA's success, CISA must ensure these protections are robust in the letter of the rules and steadfastly uphold them throughout the life of the program.[29] For example, CISA should:

- Confirm explicitly how it will maintain the confidentiality of the report data and safeguard data, records, reports, and other information it receives;

- Specify that information from CIRCIA reports 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 actions against a covered entity's executives and employees); and

- Protect from public disclosure the same protections to information generated in response to a Request for Information or subpoena.

CISA stands at the beginning of an ecosystem-shifting moment in the evolution of the nation's incident awareness and risk management. Our hope is these recommendations help ensure a sound foundation for implementing this regulation and achieve CIRCIA's purpose to enhance the situational awareness of cybersecurity threats across critical infrastructure. The undersigned associations appreciate CISA's work to implement these rules and welcome deeper engagement on these topics in the months ahead.

Sincerely,

ACA Connects – America's Communications Association
Airlines for America
Airports Council International – North America
American Gas Association
American Public Power Association
American Water Works Association
Association of American Railroads
CTIA
Edison Electric Institute
Healthcare Information and Management Systems Society

[29] *See, e.g.*, Auto Innovators at 3; BRT Comments at 11-14; BSA Comments at 8-9; CTA Comments at 4-5; CTIA Comments at 38-39; ITI Comments at 7-11; National Rural Water Association Comments at 3; NFIB Comments at 4; NCTA Comments at 8, 31-34; USTelecom Comments at 14-16.

Information Technology Industry Council
Internet Security Alliance
National Association of Broadcasters
National Association of Wholesaler-Distributors
National Electrical Manufacturers Association
National Rural Electric Cooperative Association
NCTA – The Internet & Television Association
NTCA –The Rural Broadband Association
Telecommunications Industry Association
U.S. Chamber of Commerce
USTelecom – The Broadband Association