BR Business Roundtable

1000 Maine Avenue, NW, STE 500
Washington, DC 20024
202.872.1260
brt.org

November 14, 2022

Mr. Todd Klessman
Cyber Incident Reporting for Critical Infrastructure Act of 2022
Rulemaking Team Lead
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, DC 20528-0380

Re: Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022

Dear Mr. Klessman,

This letter is submitted on behalf of Business Roundtable, an organization of chief executive officers of America's largest companies. Business Roundtable member companies employ over 20 million people and spend and invest over $7 trillion a year, helping sustain and grow tens of thousands of communities and millions of small- and medium-sized businesses.

We appreciate the opportunity to comment on the Request for Information ("RFI") on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") issued by the Cybersecurity and Infrastructure Security Agency ("CISA") on September 12, 2022.[1] Passed by Congress as Division Y of the Consolidated Appropriations Act of 2022 and signed into law by President Biden on March 15, 2022, CIRCIA creates two significant new requirements for critical infrastructure entities: first, to report certain cybersecurity incidents to CISA within 72 hours and second, to report ransomware payments to CISA within 24 hours. Both requirements are subject to rulemaking by CISA before becoming effective.

Business Roundtable appreciates CISA's initial approach to this rulemaking process. CISA is right to approach this significant rulemaking with a collaborative, thoughtful and careful approach. Business Roundtable consequently welcomes CISA's decision to solicit feedback through this RFI as well as through the listening sessions that CISA has undertaken in recent months. In these comments, we highlight three priorities for CISA to consider as it works to implement this important statute.

[1] Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022, 87 Fed. Reg. 55833 (Sept. 12, 2022).

I. Appropriately Scope "Covered Entities" and "Covered Cyber Incident"

CIRCIA's ransom payment and cyber incident reporting requirements apply to organizations that are considered "covered entities." In addition, Congress tied the statute's cyber incident reporting requirement to the occurrence of a "covered cyber incident." Properly scoping these two terms will be critical to accomplishing Congress' intent to create an effective incident reporting mechanism that will strengthen the security of our nation's critical infrastructure.

Scope "Covered Entities" Appropriately: A "covered entity" under CIRCIA is "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the criteria established" by the forthcoming rulemaking.[2] In other words, Congress tasked CISA with selecting the subset of critical infrastructure entities that should be subject to the forthcoming rule. CISA should follow three principles as it establishes these criteria.

- First, CISA should take a risk-based approach tailored to the cyber threats to our nation's critical infrastructure and prioritized to properly allocate its own available resources. During the COVID-19 pandemic, for example, CISA issued guidance that included a wide range of personnel within the scope of "Essential Critical Infrastructure Workers."[3] Attempting to cover an equally broad set of entities in this context is likely to result in uncertainty about the entities that are subject to the rule, submission of reports that do not advance congressional intent and undue burden on private sector entities. Instead, CISA should take a risk-based approach, as reflected in the factors dictated by Congress, which can be summarized as the criticality of the entity, the likelihood of attack, and the potential operational consequences from an attack.[4]

- Second, CISA should limit the scope of covered entities to owners and operators (i.e., the primary operators) of relevant U.S. critical infrastructure. We believe this interpretation of "entity in a critical infrastructure sector" reflects congressional intent. For example, Congress rightly rejected proposals that would have required reporting by cybersecurity companies or other third-party vendors to critical infrastructure entities. In the case of third-party vendors, for example, they often will not have visibility into incidents at the same level of detail as the actual customer and would not be able to distinguish what is a "substantial cyber incident." CISA should reflect these decisions and operational limitations in its definition of an entity "in a critical infrastructure sector" while allowing members of the ecosystem to maintain appropriate contractual arrangements for reporting.

---

[2] *See* 6 U.S.C. § 681(5).
[3] *See* Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency, Advisory Memorandum on Ensuring Essential Critical Infrastructure Workers' Ability to Work During the COVID-19 Response v.4.1 (Aug. 10, 2021).
[4] *See* 6 U.S.C. § 681b(c)(1).

- Third, CISA should ensure that an entity is only treated as a "covered entity" to the extent that it owns or operates relevant critical infrastructure. For example, consider a conglomerate that consists of businesses that own or operate critical infrastructure and other businesses that do not. That entire conglomerate should not be treated as a "covered entity" for purposes of the forthcoming rule. Neither should an entity be treated as a "covered entity" if it has contracted to perform certain operations but is not the primary operator of relevant critical infrastructure. Rather only those constituent businesses that own or are the primary operator for relevant critical infrastructure should be "covered entities" and only to the extent that they own or operate critical infrastructure.

Scope "Covered Cyber Incident" Appropriately: A "covered cyber incident" under CIRCIA is "a *substantial* cyber incident experienced by a covered entity that satisfies the definition and criteria" established by CISA in the forthcoming rule.[5] While CISA may further narrow the scope of incidents subject to reporting under CIRCIA, Congress intended only a subset of cyber incidents to be reportable under CIRCIA. Congress explained the minimum features of such "substantial cyber incidents" in CIRCIA, as well as the factors CISA should consider in defining such incidents, including the sophistication or novelty of the tactics used, the number of individuals directly or indirectly affected and potential impacts on industrial control systems.[6] CISA should adhere to this limitation in the definition and criteria it implements by rule. In particular, CISA should tie this concept of "substantial" cyber incidents to the purpose of the statute: to help protect U.S. critical infrastructure. Incidents that do not affect U.S. critical infrastructure should not be reportable under CIRCIA, even if they are substantial. For example, reporting should not be required for a data breach that affects a company's employees, an incident in which a hacker steals trade secrets relating to a product that is not used in critical infrastructure or an incident that only affects systems outside the United States.

Scoping these key terms in this manner will accomplish the statutory purpose of robust sharing of incident and ransom payment information without unduly distracting response teams or disrupting effective existing cybersecurity practices. We note also that CISA will retain rulemaking authority under CIRCIA.[7] CISA should plan to use that authority in the future as necessary—including as risks change, rather than seeking to cover every entity or incident arguably subject to CIRCIA in the first instance.

---

[5] *See* 6 U.S.C. § 681(4) (emphasis added).
[6] *See* 6 U.S.C. § 681b(c)(2).
[7] *See* 6 U.S.C. § 681b(b)(3).

II. Pursue A Workable Approach to Reporting Requirements That Appropriately Prioritizes Incident Response

Incident response teams play a critical role in containing and reducing the harm caused by cyber incidents. These teams may well be stretched to the limit by significant cyber incidents. Every hour of the team's time can make a difference in the heat of such incidents—and particularly within the first 72-hour period. While we agree with the goals of incident reporting, it is critical that incident response teams are allowed to focus on responding effectively to cyber incidents and are not unduly distracted by unnecessary short-term reporting requirements. CISA accordingly must ensure that the requirements imposed by the forthcoming rule are practical and workable in the context of the response to a substantial cyber incident. For example, the trigger for the 72-hour period should reflect the practical realities of an incident, including the limited information that may be available to a response team as it makes the determinations that may be required under any forthcoming rule.

Focus incident reporting on high-value information. CIRCIA describes the intended contents of required incident reports.[8] We would encourage CISA not to expand upon those elements. We also would ask CISA to ensure that each required element may be satisfied by the key, high-value information necessary to understand the basic features of a substantial cyber incident. CISA should not ask victim companies to provide unnecessary detail that would substantially increase the time necessary to prepare the report without providing significant additional value. For example, covered entities should not be required to disclose the specific fields of "personal information" that may have been at risk.

Adopt a practical approach to updates. CIRCIA requires victim companies to file "Supplemental Reports" about a substantial cyber incident if "substantial new or different information becomes available."[9] CISA should implement this requirement in a manner that avoids requiring companies to make numerous successive reports that distract them from the task of remediation. CISA also should not require, as a general matter, the submission of an incident completion report. Rather, such reports should be optional, allowing companies to choose whether to clearly identify the end of any supplemental reporting obligation.[10]

Take a practical approach to data retention. CIRCIA provides that a covered entity that submits an incident report or ransom payment report must "preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established" by the forthcoming rule.[11] CISA should take a practical approach to this requirement, giving flexibility

---

[8] *See* 6 U.S.C. § 681b(c)(4).
[9] *See* 6 U.S.C. § 681b(a)(3).
[10] *See id.* (describing conditional obligation to submit supplemental reports until the covered entity notifies CISA that the covered cyber incident has "concluded and has been fully mitigated and remediated).
[11] *See* 6 U.S.C. § 681b(a)(4).

to covered entities so that they do not find themselves wrestling with data retention challenges (e.g., for out-of-band communication channels used during an incident) during an incident.

Ensure multiple avenues of reporting incidents. CISA should provide multiple avenues of reporting incidents, including a secure, web-based form (that includes the ability to print/save the report following submission) or email given the short time frame and potential for the covered entity to be limited in its ability to submit the report through a single means.

III. Contribute To an Effective and Coordinated National Cybersecurity Strategy

Mandatory incident reporting to CISA will play a valuable role in our nation's overall approach to critical infrastructure cybersecurity if effectively implemented. But reporting under CIRCIA will be only one element of the cybersecurity strategy for U.S. critical infrastructure. CISA should implement CIRCIA with this in mind, making sure that the implemented regulations contribute to overall U.S. cybersecurity. CISA can take three key steps to help achieve that goal.

Harmonize and Rationalize Incident Reporting to the Federal Government. CIRCIA tasks the Homeland Security Secretary with leading a new Intergovernmental Cyber Incident Reporting Council that will "coordinate, deconflict, and harmonize Federal incident reporting requirements."[12] In addition, CIRCIA requires any federal agency—including independent agencies—to provide incident reports it receives to CISA within 24 hours.[13] CIRCIA thus reflects a clear judgment by Congress that CISA is the proper ultimate custodian of information about cyber incidents affecting critical infrastructure. CISA should implement CIRCIA and work with its federal partners outside the rulemaking to solidify this position. In particular, CISA should confirm that reporting equivalent information to a federal partner (or CISA itself) under another federal regime renders any additional reporting under CIRCIA unnecessary. It also should collaborate with federal partners to the extent that those partners work to remove incident reporting requirements that are rendered unnecessary by CIRCIA. Finally, CISA should ensure that it distributes necessary information to appropriate federal partners promptly and discourages those partners from requesting covered entities to submit additional incident information through separate channels.

Support Voluntary Information Sharing. Required incident reporting remains only one piece of effective public-private cyber information sharing. Voluntary information sharing will remain a critical tool for understanding cyber threats to critical infrastructure and the nation more broadly. CISA should ensure that it does not implement CIRCIA in a way that would discourage

[12] 6 U.S.C. § 681f.
[13] 6 U.S.C. § 681g.

voluntary information sharing.[14] For example, CISA should avoid making incident reporting so burdensome as to discourage other forms of information sharing.

Support Ongoing Collaboration. Critical infrastructure cybersecurity requires effective collaboration between the public and private sectors. CISA should facilitate that robust collaboration by ensuring that CIRCIA implementation preserves a productive and cooperative relationship between CISA and covered entities. CISA should also ensure that timely, actionable information on cybersecurity threats is shared back to the private sector. Too often, information shared on such threats is too vague for companies to be able to respond proactively. CISA has the opportunity to greatly increase sharing and collaboration between the public and private sectors by providing more specific information on threats.

Conclusion

Business Roundtable appreciates the opportunity to provide our input during this process. We would be happy to discuss these comments or any other matters you believe would be helpful. Please contact Will Anderson, Vice President, Technology & Innovation Policy, at Business Roundtable, at wanderson@brt.org or (202) 496-3259.

[14] This includes information sharing pursuant to the Cybersecurity Information Sharing Act of 2015, as well as voluntary information sharing under CIRCIA itself, *see* 6 U.S.C. § 681c.