BR Business Roundtable

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

June 15, 2026

Nichole Clagett
CIRCIA Deputy Associate Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, DC 20528-0380

Re: Docket No. CISA–2022–0010
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Rulemaking; Town Halls

Dear Ms. Clagett,

These supplemental comments are submitted on behalf of Business Roundtable, an association of more than 200 chief executive officers (CEOs) of America's leading companies, representing every sector of the U.S. economy. Business Roundtable CEOs lead U.S.-based companies that support one in four American jobs and almost a quarter of U.S. GDP. Through CEO-led policy committees, Business Roundtable members develop and advocate directly for policies to promote a thriving U.S. economy and expanded opportunity for all Americans.

Business Roundtable appreciates the opportunity to provide additional input on refining the scope and burden of CIRCIA as issued in the Federal Register on February 13, 2026. As emphasized in our July 3, 2024 comment letter, Business Roundtable believes CIRCIA should be implemented in a manner that strengthens national cybersecurity while avoiding unnecessary redundancy, subjectivity and compliance burdens that divert resources from incident response. Below, we address specific topics of interest enumerated in the Cybersecurity and Infrastructure Security Agency's (CISA) Notice on Town Hall Meetings on CIRCIA to better align CIRCIA's rulemaking with its statutory purpose.

I. Scope of Covered Entities and Applicability Criteria

A. Size-Based Criterion

As stated in our previous filings, Business Roundtable is concerned that using a size-based criterion to determine which entities are within the scope of the rulemaking would unnecessarily increase the number of covered entities without meaningfully improving cybersecurity outcomes. An entity's annual revenue or employee count are neither reliable nor consistent proxies for systemic risk to national critical functions. Implementing thresholds for covered entities using these metrics would risk including entities whose disruption would not

have a debilitating impact on national security, economic security, or public health and safety, while potentially missing smaller entities whose operations are systemically important. Therefore, Business Roundtable recommends that CISA either adopt "Alternative B" from its April 2024 Proposed Rule, which would eliminate the size-based threshold completely, or substantially narrow the threshold to ensure that it is clearly tied to demonstrable systemic risk.

B. Sector-Based Criteria and Alternative Approaches

Similar to our concerns regarding a size-based criterion, Business Roundtable is concerned that using certain sector-based criteria could unnecessarily increase the number of covered entities without meaningfully improving cybersecurity outcomes. Broadly relying on existing Sector-Specific Plans (SSPs) to determine the scope of covered entities would be unwise given the plans were not developed for this purpose and have not been updated in several years.

To more closely align the rule to the statutory mandate, CISA should work with the relevant Sector Risk Management Agencies (SRMAs) and private sector partners to develop targeted, sector-based criteria that focus on, and reflect the operational realities of, entities whose disruption would have severe consequences. To ensure appropriate scoping, CISA should specifically focus on entities that own or operate assets or services that directly and primarily provision a National Critical Function (NCF). CISA should also clarify that an entity's ancillary involvement in a critical infrastructure sector or presence in a corporate family conducting business in a critical infrastructure sector is insufficient to render an entity "in" that sector. Likewise, incidents affecting a covered entity's non-critical business units that have no material operational overlap should not constitute covered cybersecurity incidents.

Similarly, any criteria applicable to Managed Service Providers (MSPs) or Cloud Service Providers (CSPs) should be tied to demonstrable impact on covered entities' critical operations. The use of open-source software, standing alone, should not create a separate reporting trigger, as the presence of open-source components does not inherently elevate systemic risk. CISA should also clarify that service providers are not required to submit duplicative reports regarding impacts to customer systems. Likewise, CISA should state that each covered entity remains independently responsible for determining whether it must file a report based on the impact to its own information systems and operations.

II. Definition and Examples of Substantial Cyber Incidents

Business Roundtable recommends that CISA anchor the definition of "substantial cyber incidents" to those incidents that have a demonstrable impact on national security, economic security, public health and safety, or critical infrastructure operations. Leveraging CISA's National Cyber Incident Scoring System (NCISS) would provide a more objective and repeatable framework for severity determinations and reduce subjectivity across sectors.

Business Roundtable also urges CISA to state that non-exploited vulnerabilities are not reportable and that good-faith security research and inadvertent employee errors without malicious intent are excluded. Routine, low-level cyber events that do not present systemic risk should not qualify as substantial cyber incidents.

III. Improvements to the Content of Reports

Business Roundtable urges CISA to streamline required report content to focus on information necessary to enhance federal visibility into systemic cyber risk. Many of the detailed data elements proposed in the previous NPRM exceed all other existing incident reporting requirements and are difficult to ascertain within 72 hours, contributing to fragmentation and potentially diverting resources from incident containment and remediation.

Supplemental reporting should be triggered by material developments rather than any "new or different information." The deadline for supplemental reports should be no sooner than 72 hours following discovery of a significant update. This approach would better balance operational realities with CISA's information-sharing objectives.

IV. Requests for Information (RFIs) and Subpoenas

CISA should clarify that only CISA employees designated by the Director have authority to issue RFIs. Liability for inaccurate statements should apply only where a covered entity knowingly provides false information, not where information was reasonably believed to be accurate at the time of submission.

Confidentiality, liability and evidentiary protections should not be stripped from information submitted in response to a subpoena in circumstances involving good faith disagreements over reportability. Removing these protections would discourage transparency and undermine CIRCIA's purpose.

V. Harmonization and Reduction of Duplication

Harmonizing CIRCIA reporting requirements with other federal and state, local, tribal, and territorial regimes remains essential. Without meaningful harmonization, covered entities will continue to face duplicative and potentially conflicting obligations during active incident response, potentially distracting from remediation efforts and worsening outcomes.

To address this, Business Roundtable urges CISA to develop a secure reporting portal capable of distributing submissions to appropriate agencies, standardize definitions of key terms across federal agencies, and recognize substantially similar reports without requiring formal CIRCIA agreements as a precondition. Covered entities should also have the option to use CIRCIA reports to satisfy other reporting obligations where appropriate, while maintaining the ability

to submit separate reports as appropriate, depending on the nature of the incident and the relevant regulator. Absent these mechanisms, the final rule will impose significant compliance burdens without commensurate cybersecurity benefit.

VI. Confidentiality, Data Protection and Preservation

Data preservation requirements should be narrowed to records directly relevant to the covered cyber incident. Broad, two-year retention requirements for expansive datasets create cost and security risks without clear benefit.

CISA should also clarify the scope of anonymization prior to sharing reports, identify which agencies will have access to submitted information, and designate CIRCIA reports as commercial, financial, and proprietary information by default. Given the sensitivity of the information collected, CISA must employ robust cybersecurity safeguards and regularly assess their effectiveness.

Conclusion

Business Roundtable members are committed to strengthening the nation's cybersecurity posture and to working collaboratively with CISA. A carefully tailored, risk-based and harmonized final rule will best advance CIRCIA's statutory objectives while enabling companies to focus on preventing and responding to cyber threats.

Business Roundtable appreciates your consideration of these comments and the additional opportunity for stakeholder feedback. For any questions, please contact Amy Shuart, Vice President of Technology & Innovation, Business Roundtable, at ashuart@brt.org or (202) 496-3290.