July 3, 2024

Jennie M. Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
1110 N. Glebe Rd.
Arlington, VA 20598

RE: Docket No. CISA-2022-0010, Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

Dear Director Easterly:

Associated Builders and Contractors hereby submits the following comments to the Cybersecurity and Infrastructure Security Agency in response to the above-referenced notice of proposed rulemaking published in the Federal Register on April 4, 2024, at 89 Federal Register 23644.

About Associated Builders and Contractors

ABC is a national construction industry trade association representing more than 23,000 member companies. ABC and its 67 chapters help members develop people, win work and deliver that work safely, ethically and profitably for the betterment of the communities in which ABC and its members work.

ABC's membership represents all specialties within the U.S. construction industry and is comprised primarily of general contractors and subcontractors that perform work in the industrial and commercial sectors for government and private sector customers.[1]

The vast majority of ABC's contractor members are also small businesses. This is consistent with the U.S. Census Bureau and U.S. Small Business Administration's Office of Advocacy's findings that the construction industry has one of the highest concentrations of small businesses (82% of all construction firms have fewer than 10 employees)[2] and industry workforce employment (nearly 81% of the construction

[1] For example, see ABC's 34nd Excellence in Construction Awards program from 2024: https://www.abc.org/Portals/1/2024/EIC/34th%20EIC%20program.pdf?ver=mzYgfDwm9eScx_LNSAZXAQ%3d%3d.
[2] U.S. Census Bureau 2021 County Business Patterns: https://data.census.gov/table?q=CBP2021.CB2100CBP&tid=CBP2021.CB2100CBP&hidePreview=true and https://www.census.gov/programs-surveys/cbp/data/tables.html.

industry is employed by small businesses).[3] In fact, construction companies that employ fewer than 100 construction professionals comprise 99% of construction firms in the United States and account for 69% of all construction industry employment.[4]

In addition to small business member contractors that build private and public works projects, ABC also has large member general contractors and subcontractors that perform construction services for private sector customers and federal, state and local governments procuring construction contracts subject to respective government acquisition policies and regulations.

ABC's diverse membership is bound by a shared commitment to the merit shop philosophy in the construction industry. The philosophy is based on the principles of nondiscrimination due to labor affiliation and the awarding of construction contracts through open, competitive bidding based on safety, quality and value.

ABC's Comments in Response to the Notice of Proposed Rulemaking

ABC understands and supports the need for the CISA to craft effective regulations aimed at protecting America's critical infrastructure from cybersecurity threats in order to safeguard the nation's security and economic future. We have worked to support these efforts by educating contractor members on important cybersecurity topics through webinars, guides and other resources.[5]

However, ABC is concerned that the proposed rule as currently drafted will be counterproductive to these important goals, and instead place excessive burdens on contractors, including many small businesses.

As detailed in the comments below, ABC urges the CISA to make key revisions to tailor reporting requirements to entities that are truly engaged in critical infrastructure sectors, limit excessive recordkeeping requirements and avoid unnecessarily punitive approaches to regulatory enforcement.

I. The Proposed Rule's Scope of Covered Entities and Covered Cyberincidents Are Overly Broad.

In the proposed rule, the CISA defines an extremely wide range of entities subject to reporting requirements and requires reporting of an expansive set of possible cyber incidents. ABC is concerned that this approach unduly burdens the regulated

[3] 2023 Small Business Profile, U.S. Small Business Administration Office of Advocacy (2023), at page 4, https://advocacy.sba.gov/wp-content/uploads/2023/11/2023-Small-Business-Economic-Profile-US.pdf.

[4] U.S. Census County Business Patterns by Legal Form of Organization and Employment Size Class for the U.S., States and Selected Geographies: 2021, available at https://data.census.gov/table/CBP2021.CB2100CBP?q=CBP2021.CB2100CBP&hidePreview=true.

[5] https://www.abc.org/Technology/Cybersecurity-Resource-Guide.

community, while also impairing the CISA's ability to effectively protect critical infrastructure.

1. **Only Entities That Have Meaningful Involvement With Critical Infrastructure Should be Covered.**

As written, the proposed rule subjects any entity to reporting requirements that is deemed a member of 1 of 16 critical infrastructure sectors[6] laid out in Presidential Policy Directive 21[7] and either:

- Exceeds the applicable small business size standard set by the U.S. Small Business Administration, or;
- Meets certain sector-based criteria.

The proposed rule itself admits to the broad nature of this definition, stating that the vast majority of entities in the United States are members of at least one critical infrastructure sector[8] and estimates that over 316,000 entities would be covered by the rule's reporting requirements.[9] The CISA further estimates that it will receive approximately 15,000 annual incident reports, which would appear to be a drastic underestimation based on the overly inclusive nature of the definitions of both covered entities and covered cyberincidents.

ABC urges the CISA to pursue a narrower, more focused method of determining which entities are covered under the proposed rule. In addition to unnecessarily burdening many construction contractors that may have limited involvement with critical infrastructure, the proposed rule also raises questions regarding the CISA's capacity to quickly assess and deter cyberthreats while monitoring hundreds of thousands of entities and reports.

Further, narrowing the proposed definition would better align the regulation with the intent of Congress in passing CIRCIA. At a recent hearing on May 1, 2024,[10] multiple members of Congress on the House Committee on Homeland Security's Subcommittee on Cybersecurity and Infrastructure Protection questioned the CISA's proposed definitions and directed the CISA to narrow its definitions.

---

[6] https://www.federalregister.gov/d/2024-06526/p-621.
[7] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.
[8] https://www.federalregister.gov/d/2024-06526/p-643.
[9] https://www.federalregister.gov/d/2024-06526/p-1367.
https://www.federalregister.gov/d/2024-06526/p-1370.
[10] House Homeland Security Cybersecurity and Infrastructure Protection Subcommittee hearing on "Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking," May 1, 2024.
https://homeland.house.gov/hearing/surveying-circia-sector-perspectives-on-the-notice-of-proposed-rulemaking.

2. Interagency Agreements Should Be Utilized.

ABC is pleased the proposed rule includes CIRCIA agreements, which are defined as interagency agreements between the CISA and other federal agencies that would exempt entities already subject to substantially similar cybersecurity reporting requirements.[11] In particular, many of ABC's federal contractor members working with the U.S. Department of Defense are already subject to stringent cybersecurity reporting requirements. ABC supports the swift implementation of a CIRCIA agreement between CISA and the DOD to avoid unnecessarily duplicative reporting requirements impacting contractors that play a critical role in America's national defense.

II. The Proposed Rule Imposes Excessive and Costly Data Preservation Requirements.

Under the proposed rule, entities that submit CIRCIA incident reports are required to preserve extensive data and records relating to the incident, including communications with threat actors, indicators of compromise, network data and more.[12] Entities are required to preserve these records for at least two years following report submission.[13]

These requirements will impose excessive costs for many covered contractors such as small businesses and other contractors who may not employ a sufficient number of information technology experts as they will be forced to outsource record preservation to third parties. This is especially concerning given the wide range of businesses that will be considered covered entities under the proposed rule.

The CISA should revise the requirements to reduce this burden and target data preservation requirements where they are needed most. This could be accomplished by reducing the length of the preservation period and limiting the applicability of preservation requirements to incidents where the CISA deems further investigation is likely. This will have the additional benefit of allowing contractors to focus limited IT resources on proactive measures to enhance cybersecurity.

III. The Proposed Rule Takes an Overly Punitive Approach to Enforcement of Reporting Requirements.

The proposed rule provides for enforcement of reporting requirements through subpoenas and civil action by the U.S. Department of Justice.[14] Federal contractors in particular face increased legal risk, with the potential for criminal enforcement by the DOJ[15] or debarment from federal procurement.[16]

---

[11] https://www.federalregister.gov/d/2024-06526/p-1718.
[12] https://www.federalregister.gov/d/2024-06526/p-1830.
[13] https://www.federalregister.gov/d/2024-06526/p-1842.
[14] https://www.federalregister.gov/d/2024-06526/p-1854.
[15] https://www.federalregister.gov/d/2024-06526/p-1896.
[16] https://www.federalregister.gov/d/2024-06526/p-1895.

ABC is concerned that the outlined approach fails to consider that companies suffering cyberincidents are victims, often under extreme pressure from malicious actors. Rather than building trust between the public and private sector in order to create strong partnerships that are useful in preventing future cyberincidents, the proposed rule's punitive methods instead create an adversarial relationship between companies and the federal government that will only inhibit the sharing of critical information.

The CISA should instead maintain its focus on improving collaboration with the private sector and the provision of technical guidance to help the industry deal with emerging cyberthreats.

Conclusion

ABC believes that, while well-intentioned, as currently proposed the regulations would impose unnecessary burdens, strain the CISA's ability to process a massive influx of incident reporting, impose unfeasible data preservation requirements and risk inhibiting collaboration on cybersecurity between the public and private sector. ABC urges the CISA to seriously consider the above recommendations and stands ready to partner with the CISA to improve cybersecurity awareness within the construction industry.

Thank you for the opportunity to submit comments on this matter.

Respectfully submitted,

Ben Brubeck
Vice President of Regulatory, Labor and State Affairs
Associated Builders and Contractors
brubeck@abc.org