June 3, 2024

Submitted electronically via Regulations.gov

Mr. Todd Klessman
CIRCIA Rulemaking Team Lead
Cybersecurity and Infrastructure Security Agency
circia@cisa.dhs.gov

Re: Federal Register No. CISA 2022-0010
Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA")
Reporting Requirements

Dear Mr. Klessman:

The American Investment Council ("AIC") appreciates the opportunity to comment on the proposed rulemaking concerning reporting of critical infrastructure cybersecurity incidents. AIC is a leading advocacy and resource organization established to develop and provide information about the private investment industry and its contributions to the long-term growth of the U.S. economy and retirement security of American workers. Member firms of the AIC consist of the country's leading private equity and growth capital firms united by their successful partnerships with limited partners and American businesses.

As you are aware, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") requires the Cybersecurity and Infrastructure Security Agency ("CISA") to promulgate regulations implementing the statute's covered cyber incident and ransom payment reporting requirements.[1] The Proposed Rule contemplates establishing a comprehensive regime to require reporting of cybersecurity incidents to CISA and coordination with other federal agencies.

Our members support efforts to enhance cybersecurity and to coordinate reporting of cybersecurity incidents so that companies have a clear and responsive avenue for cybersecurity assistance from the federal government. Many of our members are already subject to multiple cybersecurity reporting requirements, each with different thresholds, timelines, and required contents of reports.

Although the Proposed Rule Preamble states that "the process for an entity to determine if it is within a critical infrastructure sector will usually be a relatively straightforward exercise,"[2] it also mentions that more than 300,000 entities are likely critical infrastructure – suggesting that the proposed scope could include a third of the

[1] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Proposed Rule, 89 Fed. Reg. 23644 (April 4, 2024) [hereinafter Proposed Rule].
[2] *Id*. at 23678

roughly one million operating U.S. companies.[3] The Preamble underscores that the Proposed Rule was intended to be expansive, noting that "[t]he overwhelming majority of entities, though not all, are considered part of one or more critical infrastructure sectors."[4]

Our members are concerned the Proposed Rule gives little comfort to the investment community as to what sort of entities are excluded, providing only a few "illustrative examples of entities that generally are not considered part of one or more critical infrastructure sector include advertising firms, law firms, political parties, graphic design firms, think tanks, and public interest groups."[5]

Many operating companies are owned and controlled by private investment funds and other entities designed for various commercial, tax, and regulatory reasons. Adding these entities to the already long rolls of entities considered to be critical infrastructure will do nothing to enhance cybersecurity while creating confusion and needless complexity. In particular, pass-through entities, private investment funds, and advisers to private investment funds should be explicitly excluded from the definitions of critical infrastructure. An investment adviser to a private fund is closely analogous to the other professional services firms mentioned, such as law firms, and they should have certainty that they are not covered by the requirements applicable to critical infrastructure.

Likewise, all corporate entities that do not actually operate critical infrastructure should be explicitly excluded from the relevant definitions of critical infrastructure. Although we do not believe that it was CISA's intention to include such entities, ambiguity as to their inclusion will create uncertainty as cybersecurity incidents are reporting up through ownership and management chains. Clearly the responsibility to report to CISA should remain with operating entities only.

CISA should want to make abundantly clear which entities are excluded so as to not induce confusion, additional reporting, and cost. By CISA's own estimates the Proposed Rule is already estimated to result in a total of 210,525 CIRCIA Reports over the next decade, resulting in $1.4 billion in cost to industry and $1.2 billion in cost to the Federal Government.[6]

Congress did not enact CIRCIA with the intention to include our members as covered entities. CIRCIA directs CISA to make that determination based on a few factors none of which weigh in favor of inclusion. Furthermore, there is no support for the idea that that Presidential Policy Directive 21, which sets the outer bounds for entities that could be covered by the Proposed Rule, encompasses non-operating entities. Ultimately this approach is sound policy; our members have never been considered critical infrastructure

[3] *Id*. at 23648
[4] *Id*. at 23678
[5] *Id*.
[6] *Id*. at 23648

as understood in the cybersecurity and national security context and there is no reason to include them.

Our members strongly recommend that CISA provide clear examples of excluded entities so that the initial comments about the scope of coverage are not misconstrued. The elaboration of this exemption is entirely consistent with enhancing cybersecurity and working with industry to develop rapid awareness of cybersecurity risks.

* * *

We appreciate your consideration of this request.

Sincerely,

/s/ Rebekah Goshorn Jurata

Rebekah Goshorn Jurata
General Counsel
American Investment Council