

Policy Backgrounder: CISA Proposed Rule on Cyber Reporting for Critical Infrastructure Sectors

April 12, 2024

Trusted Insights for What's Ahead™

The Department of Homeland Security published its proposed [regulation](#) to implement the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) that mandates reporting of cyber breaches to the Cybersecurity & Infrastructure Security Agency (CISA) for a wide range of entities designated as part of US critical infrastructure.

- CIRCIA, enacted in March 2022, requires covered entities generally to report cyber incidents within 72 hours and ransomware payments within 24 hours through a specified form on CISA's website, requiring disclosure of incident details and the preservation of related data for two years.
- CISA proposes a broad scope of "covered entities" across its 16 infrastructure sectors, while including exemptions for certain small businesses. The proposal also defines a "substantial" cyber incident broadly, excluding minor disruptions.
- CISA estimates that up to 316,244 entities will be covered under this rule, resulting in approximately 210,525 breach reports over 11 years, with compliance a cost of \$1.4 billion to the industry and \$1.2 billion to the Federal Government. (The total cost of cyberattacks to the economy is far larger.)
- Comments on the regulation are due by June 3, 2024. CISA expects to issue a final rule in late 2025, with implementation in 2026.

CISA Proposes Infrastructure Cyber Reporting Rule

On April 4, the Department of Homeland Security published its long-awaited proposed [regulation](#) implementing the [Cyber Incident Reporting for Critical Infrastructure Act](#) (CIRCIA). The proposal defines a broad scope of covered entities with mandatory requirements to report cyber breaches to the Cybersecurity & Infrastructure Security Agency (CISA). The proposed rule is open for public comment until June 3, 2024, while CISA expects to issue the final rule in late 2025, with implementation likely not beginning until 2026 to comply with the Administrative Procedure Act and Congressional Review Act.

CIRCIA directed CISA to issue rules to define what qualifies as a "covered entity" and "covered cyber event" within its 16 [critical infrastructure sectors](#). In the 450-page rulemaking, CISA defined covered entities to include almost every facet of US critical infrastructure as well as a broad definition of events that trigger a 72-hour reporting requirement. CISA [states](#) that "the overwhelming majority of entities, though not all, are considered part of one or more critical infrastructure sectors," and emphasizes that the scope of entities is not limited to owners or operators of critical infrastructure.

CIRCIA outlined new requirements that covered entities must report a "covered cyber incident" within 72 hours after "reasonably believing" a breach had occurred and report a payment made in response to ransomware within 24 hours. Covered entities will be required to submit reports to CISA through a web-based CIRCIA Incident Reporting Form on CISA's website. All CIRCIA reports must include details about how the incident was carried out, including detail on specific vulnerabilities exploited, security defenses in

place at the reporting entity, the techniques used during the attack, and operational impacts. Entities are also responsible for preserving data and record related to incidents for two years.

For both operational and commercial reasons, the reports will not be public and will be exempt from disclosure under the Freedom of Information Act and similar laws. A covered entity must also designate its CIRCIA report or response “as commercial, financial, and proprietary information” if it contains confidential business information. The reports may, however, be shared as appropriate with other government agencies, although those other agencies may not use information “obtained solely through a CIRCIA Report . . . or a response provided to a [CISA] request for information” for their own regulatory purposes, which provides some protection to covered entities.

Regulatory Definitions

Under the proposal, entities in a critical infrastructure sector are covered if either (1) they exceed the small business size [standard](#) or (2) they meet a sector-based criterion. Small businesses are generally exempt if they fall below the [definition](#) specified by the U.S. Small Business Administration (between 100 and 1,500 employees and annual revenue between \$2.75 million and \$47 million). However, CISA also proposes to cover small businesses that own or operate critical infrastructure through sector-based criteria for 13 of the 16 critical sectors. These [criteria](#) capture a broad range of small businesses, including those in internet or telecommunications services, certain manufacturing categories, financial services, certain information technology services, and school districts with at least 1,000 students.

The proposed rule [defines](#) a “substantial cyber incident” as an event that leads to any of the following: (1) A substantial loss of confidentiality, integrity, or availability of a covered entity’s information system or network; (2) A serious impact on the safety and resiliency of a covered entity’s operational systems and processes; (3) A disruption of a covered entity’s ability to engage in business or industrial operations, or deliver goods or services; or (4) Unauthorized access to a covered entity’s information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a compromise of a cloud, managed service, data hosting, or other supply chain provider. The proposal emphasizes that incidents qualify as substantial based on the impacts of the first three criteria, regardless of how the attack was carried out and what type of data or system was targeted.

In contrast, “cyber incidents that result in minor disruptions, such as short-term unavailability of a business system or a temporary need to reroute network traffic” or an instance in which when “malicious software is downloaded to a covered entity’s system but anti-virus software successfully quarantines the software and precludes it from executing” would typically not be considered substantial, under the proposal.

CISA [estimates](#) the CIRCIA reporting rule will cover up to 316,244 entities and in what it estimates to result in 210,525 cyber breach reports over an 11-year span. CISA expects the cost of CIRCIA reporting to total \$1.4 billion to industry and \$1.2 billion to the Federal Government over that period. This is a small portion of the overall impact of cyberattacks: the Congressional Research Service [estimates](#) that cybercrime will cost the US over \$450 billion in 2024.

If CISA believes a covered entity has failed to submit a required report, the CISA Director may issue a request for information and can issue a subpoena if the information provided is deemed inadequate. An entity that fails to comply with a subpoena may be subject to a civil action for injunctive relief to enforce the subpoena. Any person who makes a false statement or representation in connection with a CIRCIA Report may face criminal penalties under [18 U.S.C. §1001](#). CISA [notes](#) that it “would not consider scenarios where a covered entity reports information that it reasonably believes to be true at the time of submission, but later learns through investigation that it was not correct and submits a Supplemental Report reflecting this new information, to constitute a false statement or representation.”

Prior to enactment of CIRCIA, there was no Federal statute or regulation supporting a “comprehensive and coordinated approach to understanding cyber incidents across critical infrastructure sectors,” CISA [commented](#). Since September 2022, CISA has [solicited](#) input from public and private sector stakeholders across the infrastructure community through [requests for information](#) and [listening sessions](#), as the agency developed the proposed rule. CISA Director Jen Easterly [said](#), “[CIRCIA] will allow us to better understand the threats we face, spot adversary campaigns earlier, and take more coordinated action with our public and private sector partners in response to cyber threats. We look forward to additional feedback from the critical infrastructure community as we move towards developing the Final Rule.” CISA recommends that entities review available guidance, including publicly available [sector plans](#) for each critical infrastructure sector, to determine whether they are covered entities.

Analysis of the Proposed Rule

CED’s Solutions Brief, [Securing Critical Infrastructure: Building Resilience](#) addressed CIRCIA and several issues that should be addressed in rulemaking under it, calling for expeditious implementation of CIRCIA. In particular, the Brief noted that the “overriding solution is collaboration between public and private sector leaders, which is fundamental to meeting the cyber and resiliency challenge.” CED also noted the importance of smaller and medium-sized businesses to the protection of critical infrastructure, which the proposed rule reflects. Keeping the CIRCIA reports private both reflects CISA’s operational and intelligence needs in its efforts to maintain cybersecurity and defend against attacks while also avoiding a “name-and-shame” approach to information sharing. CED also recommended that the government as a whole harmonize and deconflict reporting requirements as new frameworks, including this rule and the SEC’s cyber reporting rule, are implemented.

CISA’s cyber reporting proposal follows similar [rules](#) from the Security and Exchange Commission (SEC) that began [taking effect](#) in December and apply to all public companies. A key unresolved issue highlighted in public comments is an inconsistent period for disclosure, as the SEC will require reporting within four business days of determining a breach is material. That incompatibility suggests that for public firms, the shorter period for CISA would thus fail to provide investors material information until compliance with the SEC deadline. This issue will likely be addressed in comments on the rule and resolved in the final rule.

Beyond the proposed rule and its eventual implementation, both the public and private sectors have further work to do. CED recommends that CISA update the 2013 Presidential Directive governing how Federal agencies address efforts to protect critical infrastructure, outlining how sectoral and systemic risks are identified, assessed, and managed, clarifying the roles of agencies charged with lead responsibility for a critical infrastructure sector. CISA should also work to coordinate updating of sector plans to strengthen resiliency.

For their part, owners and operators of critical infrastructure must make cybersecurity a top governance priority, including steps such as multifactor authentication, Zero Trust architecture, reviewing systems for the impact of AI on cybersecurity, and reviewing their supply chains for vulnerabilities—particularly important as many of the entities in those supply chains will be covered by the new rule. Lead agencies in critical infrastructure sectors should work with the private sector to help address risks and encourage the private sector to adopt robust security measures, including working jointly with government to pursue development of minimum standards for each critical infrastructure sector.

The publication of the proposal represents a significant step towards bolstering US cybersecurity—a growing focus across government and the private sector. Many important questions around eventual implementation of the rule remain open, including how CISA will enforce the rule and how it will put the trove of data the rule will elicit into action. The broad scope of covered entities will likely lead to numerous comments in response to the proposed rule that CISA must consider as it develops the final rule next

year. Whatever the text of the final rule may be—and it is reasonable to assume that it will retain the basic framework of the proposal, consistent with Congress’ intent—businesses now have an even greater reason to invest in cyber preparedness.

About the Authors

[John Gardner](#) is Vice President, Public Policy at the Committee for Economic Development, the public policy center of The Conference Board.

[Mitchell Barnes](#) is a Senior Economic Policy Analyst at the Committee for Economic Development, the public policy center of The Conference Board.

About The Conference Board

The Conference Board is the member-driven think tank that delivers Trusted Insights for What’s Ahead™. Founded in 1916, we are a non-partisan, not-for-profit entity holding 501 (c) (3) tax-exempt status in the United States. www.ConferenceBoard.org

The Committee for Economic Development (CED) is the public policy center of The Conference Board. The nonprofit, nonpartisan, business-led policy center delivers trusted insights and reasoned solutions in the nation's interest. CED Trustees are chief executive officers and key executives of leading US companies who bring their unique experience to address today’s pressing policy issues. Collectively, they represent 30+ industries and over 4 million employees. www.ConferenceBoard.org/us/committee-economic-development

© 2024 The Conference Board, Inc. All rights reserved.