Published on *The National Law Review* https://natlawreview.com

Proposed Cyber Incident Reporting Requirements for DIB Contractors Under CIRCIA

Article By:

Cassidy Kim

Eleanor M. Ross

Jeffery M. Chiow

Go-To Guide:

- The U.S. Department of Homeland Security's Cybersecurity and Infrastructure and Security Agency (CISA)'s proposed rules (the Rules) would institute extensive cyber incident reporting requirements for over 300,000 entities, which may overlap with existing reporting requirements under federal and state laws and regulations.
- Contractors operating in the Defense Industrial Base (DIB) critical infrastructure sector would likely be subject to reporting requirements under both the Rules and Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, which relate to incidents involving the Department of Defense (DoD)'s Controlled Unclassified Information. Much like the DoD's response to small business concerns under recent CMMC rulemaking activities, DIB small business contractors should not expect CISA to provide exemptions or other relief from their Rules.
- The Rules are open for public comment until July 3, 2024. The final rules are expected to be implemented in late 2025.

On April 4, 2024, CISA published its long-awaited Notice of Proposed Rulemaking to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). If passed in their current form, the Rules would create extensive reporting obligations for an estimated 316,244 covered entities across 16 critical infrastructure sectors. The expansive nature of the Rules reflects both the gravity and the salience of the ever-shifting cyberthreat landscape, including the impact of the 2021 ransomware attack on Colonial Pipeline that precipitated CIRCIA's bipartisan enactment. By mandating the active collection and reporting of threat information, CISA seeks to coordinate the deployment of resources across critical infrastructure sectors to help network defenders mitigate risks and curb cyberthreats.

Covered Events and Reporting Fundamentals

The Rules would impose reporting requirements for a Covered Entity (further defined below) that experiences a substantial cyber incident, which is an incident that has any of the following *impacts*:

(1)	Substantial loss of confidentiality, integrity, or availability of an entity's IT systems or networks;
(2)	Serious impact on the safety or resiliency of an entity's operational technology systems or processes;
(3)	Disruption of the entity's ability to conduct its business; or
(4)	Exposure of the entity's data held by a third party, such as a cloud service provider or managed service provider, or through a supply-chain compromise.

An entity's substantiality assessment of a cyber incident would turn on multiple factors, including the type, volume, result, and duration of the incident. CISA recognizes that there could be a variety of incidents that imminently threaten information systems but that do not actually jeopardize them—examples include blocked phishing attacks, failed attempts to penetrate systems, or missing credentials that have not been exploited and have since been inactivated.[1] Without a resulting impact, as defined above, such incidents would not trigger the reporting requirements.

Incidents that meet the substantiality threshold would need to be reported to CISA no later than 72 hours after the covered entity *reasonably believes* a covered event has occurred. While the Rules explicitly recognize that an entity often requires time to conduct a preliminary analysis before a reasonable belief can be established, the entity would need to report a substantiated incident even if it had not yet confirmed the actual cause of the incident. Additionally, where an entity makes a payment in response to a ransomware attack, that payment would need to be reported to CISA within 24 hours.[2]

An entity that reports a substantial cyber incident to CISA would need to provide significant disclosures, including:

- Technical details and timeline of the incident, including identification of the impacted systems and physical locations of devices.
- Description of the techniques, tactics, and procedures to execute the attack, including exploitation of any known vulnerabilities.
- Description of the security defenses and measures in place prior to the incident.
- Information attributable to the adversary.
- Description of the entity's response, including mitigation efforts.
- Any engagement of law enforcement agencies or cybersecurity firms.

Covered Entities may face a further obligation to submit a supplemental report within 24 hours if new or different information becomes available, or if a ransom payment is made after a covered event is already reported. Third parties, such as a cybersecurity firm, insurance company, or law firm, may submit the report(s) on the Covered Entity's behalf.

Covered Entity Determinations

As a threshold matter, entities would need to determine whether they are a "Covered Entity" under the Rules. As noted, CISA estimates that over 300,000 entities across specified critical infrastructure sectors would be covered under the Rules. These include (1) chemicals; (2) commercial facilities; (3) communications; (4) critical manufacturing; (5) dams; (6) DIB; (7) emergency services; (8) energy; (9) financial services; (10) food and agriculture; (11) government facilities; (12) health care and public health; (13) information technology; (14) nuclear reactors, materials, and waste; (15) transportation systems; and (16) water and wastewater systems.[3]

The Rules clarify that Covered Entities are not limited to just the owners and operators of critical infrastructure systems and assets. Instead, the relevant scope broadly encompasses entities that are "active participants in critical infrastructure sectors and communities."[4]
The scope of a Covered Entity is further determined by the following considerations:

- Size-Based Criteria; Small Business Exemption. To address concerns that the Rules would impose burdensome requirements on small businesses, CISA adopted the Small Business Administration (SBA)'s size standards to inform size-based exemptions to the reporting requirements. Accordingly, subject to the sector-based criteria below, entities that do not exceed specified staffing and revenue thresholds under sector- and subsector-specific NAICS classifications (as provided in the SBA's table of small business size standards) would not qualify as Covered Entities and, therefore, would not be subject to the reporting requirements under the Rules.

- Sector-Based Criteria. Entities that are otherwise classified as small under SBA size standards may still be Covered Entities if they meet one or more of the 16 sector-based criteria—these include an entity that (1) owns or operates a chemical facility; (2) provides wire or radio communications service; (3) owns or operates critical manufacturing sector infrastructure; (4) ***provides operationally critical support to the DoD or processes, stores, or transmits covered defense information***; (5) performs an emergency service or function; (6) is a bulk electric and distribution system entity; (7) owns or operates financial services sector infrastructure; (8) qualifies as a state, local, tribal, or territorial government entity; (9) qualifies as an education facility; (10) is involved with information and communications technology to support election processes; (11) provides essential public health-related services; (12) is an information technology entity; (13) owns or operates a commercial nuclear power reactor or fuel cycle facility; (14) is a transportation system entity; (15) is subject to regulation under the Maritime Transportation Security Act; and (16) owns or operates a qualifying community water system or publicly owned treatment works.[5]

What Does This Mean for Government Contractors?

CISA estimates that of the Covered Entities that qualify under the sector-based criteria, approximately 72,000 are entities that "provide operationally critical support to the DoD or process, store, or transmit covered defense information." This accounts for *nearly 23%* (and the highest share) of the entire estimated population of affected entities by sector criteria.[6] CISA further estimates that

310,855 entities would be considered small entities, accounting for *over 98%* of the total affected population.[7] Accordingly, the Rules would significantly impact DIB small businesses.

Moreover, many entities that participate in the DIB are already subject to similar reporting requirements under DFARS 252.204-7012 and potentially face duplicative and burdensome obligations under the Rules.[8] Indeed, in the pre-publication version of the Rules, CISA recognized that DIB entities would be subject to duplicative reporting requirements but affirmed their decision to include them under the Rules due to "their criticality to national security." While the Rules contemplate the potential for relief if CISA and DoD come to an agreement allowing for subject entities to satisfy both DFARS 7012 and CIRCIA requirements with a single submission, it is not yet clear whether the agencies will be able to meaningfully harmonize the reporting requirements.[9]

Short of such an agreement, the Rules would impose broader reporting obligations than those currently required under the 7012 regulations, which are fundamentally concerned with securing and tracking incidents related to DoD's information. DIB contractors should be prepared to have systems and processes in place to meet the extensive reporting requirements under the Rules or engage third-party managed service providers to help them meet those requirements. For small businesses that have been following recent DoD rulemaking activities and have been denied categorical cost relief under the CMMC, these Rules may present further compliance costs.

Enforcement Mechanisms

Under the Rules, the Director of CISA may issue a request for information (RFI) to a Covered Entity if there is reason to suspect a failure to report a substantial cyber incident or ransom payment, such as through media reporting or other sources. If the entity fails to adequately respond or otherwise comply with the RFI, CISA may issue a subpoena to compel information. Failure to comply with the subpoena would entitle CISA to refer the matter to the Department of Justice for civil action, or to another federal agency for criminal prosecution or other regulatory enforcement action. Additional penalties may include suspension and debarment actions.

What Can Contractors Do Now?

Comments on the Rules are due by July 3, 2024. CISA has solicited comments on 73 sub-topics, including the proposed scope of applicable entities based on sector-based criteria and a size-based criterion, including the use of the SBA's size standards. Interested contractors may submit comments on areas of concern or places where further clarification is required. Once the comments have been received and reviewed, the agency will respond to each comment, explaining why it has or has not made a corresponding change in the final rule. CISA is required to publish the final rule within 18 months of the Notice of Proposed Rulemaking.

While the final rules are not expected to be implemented until late 2025, efforts to update internal procedures and coordinate external suppliers to comply with even the broad strokes of CIRCIA may be time-intensive and costly. Contractors seeking to get ahead of CIRCIA implementation, particularly DIB small businesses, may find it useful to review where the Rules would expand on existing incident reporting obligations and assess where it may make sense to improve internal systems and engage managed service providers over the next year.

---

[1] 89 Fed. Reg. 66, 23644, 23664.

[2] Joint reports within 72 hours may be submitted if both a covered event and a ransom payment

occurred.

[3] The Rules do not otherwise provide a definition for each sector and, instead, further direct entities to Sector-Specific Plans to determine the operative scope of each critical infrastructure sector.

[4] 89 Fed. Reg. 23644, Sec. IV.B.I.

[5] *See* 6 C.F.R. §§ 226.2(b)(1)-(16); 89 Fed. Reg. at 23684-702.

[6] *See* 89 Fed. Reg. at 23742.

[7] *See id*. at 23763.

[8] These are in addition to any state data breach notification laws that an entity might be subject to, none of which CIRCIA preempts.

[9] The Congressional Research Service has expressed doubt "that federal regulators will relinquish their specific reporting requirements in deference to CISA because existing regulations and the proposed CISA rule serve different purposes." CIRCIA: Notice of Proposed Rule Making: In Brief (April 11, 2024)

National Law Review, Volume XIV, Number 177

Source URL:https://natlawreview.com/article/proposed-cyber-incident-reporting-requirements-dib-contractors-under-circia