Cybersecurity Law Report cslawreport.com

May 15, 2024

Incident Response

CISA's Proposed Rule for Critical Infrastructure Cyber Incident Reporting: Analysis of Key Provisions

By Ashden Fein, Caleb Skeath, Web Leslie and Shayan Karbassi, *Covington & Burling*

On April 4, 2024, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) published its much-anticipated Notice of Proposed Rulemaking (Proposed Rule) to implement the requirements of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). While the Proposed Rule is subject to further rulemaking before the Final Rule is issued, it nonetheless represents what will likely be the most sweeping cybersecurity incident notification regulation in the United States to date, covering entities of various sizes across many sectors.

The Proposed Rule outlines the applicability criteria for critical infrastructure entities subject to CIRCIA's incident reporting requirements – 24 hours to report ransom payments and 72 hours to report covered cyber incidents – as well as the types of "substantial" cyber incidents that will be reportable. In this first installment of a two-part article series, we examine the Proposed Rule's key provisions, including what entities and incidents are covered, and time, manner and content of reports. Part two will discuss data and records preservation requirements, limited exceptions and enforcement mechanisms. It also will summarize the next steps for the proposed rulemaking and offer practical compliance measures companies can begin to implement now.

See the Cybersecurity Law Report's two-part series on the new era of cyber incident reporting and cybersecurity regulation: "Key Provisions" (Oct. 12, 2022), and "How Companies Should Prepare and Engage" (Oct. 19, 2022).

Key Definitions

Covered Entity

Under CIRCIA's definition, a "Covered Entity" must be an entity that is in a "critical infrastructure sector," as defined in Presidential Policy Directive 21 (PPD-21), which was rescinded and replaced by

National Security Memorandum 22 (NSM-22) on April 30, 2024. However, CIRCIA directed CISA to further refine this definition through subsequent rulemaking. Accordingly, the Proposed Rule provides two additional applicability criteria. Generally, a critical infrastructure entity will be covered if it *either* (1) exceeds the relevant size standard under the U.S. Small Business Administration's (SBA) small business size regulations; *or* (2) meets certain enumerated sector-based criteria. These criteria, as well as what organizations are "in" a critical infrastructure sector, are discussed below.

16 Critical Infrastructure Sectors

As a threshold matter, CIRCIA requires Covered Entities be within one of the 16 critical infrastructure sectors established by PPD-21 and reiterated in NSM-22. In the commentary to the Proposed Rule, CISA states that, in many cases, this determination will be a "relatively straightforward exercise," such as for organizations that are already members of a critical infrastructure Sector Coordinating Council. However, CISA acknowledges that some entities may need to analyze the critical infrastructure Sector-Specific Plans (SSPs) in order to determine whether they fall within a particular sector or sectors. These SSPs are not limited to owners and operators of critical infrastructure systems and assets, and the commentary thus indicates that other "active participants" in critical infrastructure sectors that impact the security of critical infrastructure may also be within that sector for purposes of the Proposed Rule.

Applicability Criteria

As summarized above, the Proposed Rule establishes additional criteria for the definition of Covered Entity, which includes: (1) the size of an entity; or (2) whether the entity meets certain sector-based criteria. An entity that is in one of the 16 sectors described above need only meet one of these criteria to be a Covered Entity.

- *Size-Based Criteria*: An entity within a critical infrastructure sector that exceeds the SBA's small business size standard as specified by the North American Industry Classification System (NAICS) would be a Covered Entity. These standards vary by industry and are generally based on employee headcount and annual revenue. Under the Proposed Rule, each entity would apply the applicable NAICS code to determine whether it meets the size-based criteria.
- *Sector-Based Criteria*: An entity within a critical infrastructure sector that meets any of the following sector-based criteria would be a Covered Entity, regardless of whether it meets the size-based criteria.

Sector	Sector-Based Criteria
Chemical	Any entity that owns or operates a covered chemical facility subject to the Chemical Facility Anti-Terrorism Standards.

Communications	Any entity that provides communications services by wire or radio communications, as defined in 47 U.S.C. §§ 153(40), (59), to the public, business or government, including both one-way communications service providers (*e.g.*, radio, television and satellite) and two-way communications service providers (*e.g.*, telecommunications, wireless service, VoIP and internet service).
Critical Manufacturing	Any entity that owns or has business operations that engage in one or more of the following: (1) primary metal manufacturing; (2) machinery manufacturing; (3) electrical equipment, appliance, and component manufacturing; or (4) transportation equipment manufacturing.
Defense Industrial Base	Any entity that is a contractor or subcontractor required to report cyber incidents to the Department of Defense pursuant to the Defense Federal Acquisition Regulation Supplement cyber incident reporting clause, codified at 48 C.F.R. § 252.204-7012 (often referred to as the "DFARS Cyber Rule" or "DFARS 7012 Clause").
Emergency Services	Any entity that provides one or more of the following emergency services or functions to a population of 50,000 or more individuals: (1) law enforcement; (1) fire and rescue; (3) emergency medical services; (4) emergency management; or (5) public works that contribute to public health and safety.
Energy	Any entity required to report cybersecurity incidents under the North American Electric Reliability Corporation's Critical Infrastructure Protection Reliability Standards or required to file an Electric Emergency Incident and Disturbance Report DOE-417 form, or any successor form, to the Department of Energy.
Financial Services	Any entity within the Financial Services sector (1) required to report cybersecurity incidents to their respective primary federal regulator; (2) for whom the primary federal regulator has indicated an intention to require cybersecurity incident reporting; or (3) that is encouraged or expected to report cybersecurity incidents to their primary federal regulator pursuant to an Advisory Bulletin.

Government Facilities	Any entity that falls within one of the following categories: (1) Any state, local, tribal, or territorial (SLTT) government entity for a jurisdiction of 50,000 or more individuals; (2) Any entity that qualifies as either a local educational agency, educational service agency or state educational agency, as defined under 20 U.S.C. § 7801, with a student population of 1,000 or more students; or an institute of higher education that receives funding under Title IV of the Higher Education Act; or (3) Any entity that manufactures, sells or provides managed services for information and communications technology specifically used to support election processes or report and display results on behalf of SLTT governments.
Healthcare and Public Health	Any entity that (1) owns or operates a hospital with 100 or more beds or a critical access hospital; (2) manufactures drugs listed in appendix A of the Essential Medicines Supply Chain and Manufacturing Resilience Assessment; or (3) manufactures a moderate risk (Class II) or high risk (Class III) device as defined by 21 U.S.C. § 360c.
Information Technology	Any entity that (1) knowingly provides IT hardware, software, systems or services to the federal government; (2) developed and continues to sell, license or maintain any software that meets the definition of "critical software" as defined by the National Institute of Standards and Technology (NIST) pursuant to Executive Order 14028; (3) is an original equipment manufacturer, vendor or integrator of operational technology hardware or software components; or (4) performs functions related to domain name operations.
Nuclear Reactors, Materials and Waste	Any entity that owns or operates a commercial nuclear power reactor or fuel cycle facility.
Transportation Systems	Any entity that falls within one of the following categories: 1. Entities identified by the Transportation Security Administration (TSA) as requiring cyber incident reporting and (in some cases) enhanced cybersecurity measures; 2. Owners and operators of freight railroad carriers identified under 49 C.F.R. § 1580.1(a)(1), (4), and (5), and public transportation and passenger railroads identified in 49 C.F.R. § 1582.1;

	3. Owners and operators of critical pipeline facilities and systems identified in 49 C.F.R. part 1586; 4. Entities required to implement a TSA-approved security program under 49 C.F.R. parts 1542, 1544, 1548, and 1549 (airports, passenger and all-cargo aircraft operators, indirect air carriers and Certified Cargo Screening Facilities); or 5. Entities that own or operate assets subject to the Maritime Transportation Security Act.
Water and Wastewater Systems	Any entity that owns or operates a Community Water System or Publicly Owned Treatment Works, as defined in 42 U.S.C. § 300f(15) or 40 C.F.R. § 403.3(q), respectively, for a population greater than 3,300 people.

The Proposed Rule does not include sector-based criteria for the Commercial Facilities, Dams, or Food and Agriculture sectors. However, entities in these sectors would still be covered if they meet the size-based criteria or any of the sector-based criteria for other sectors.

See "How to Prepare for the Cybersecurity Incident Reporting for Critical Infrastructure Act" (Aug. 3, 2022).

Covered Cyber Incidents and Ransom Payments

CIRCIA requires that Covered Entities report to CISA (1) a Covered Cyber Incident within 72 hours; and (2) a Ransom Payment within 24 hours. As discussed further below, CIRCIA also requires Covered Entities to promptly submit a Supplemental Report when they have substantial new or different information about the incident following the initial report.

Covered Cyber Incident

A Covered Cyber Incident is a (1) Cyber Incident; (2) experienced by a Covered Entity; (3) that meets one or more impact-based criteria for a Substantial Cyber Incident. A Cyber Incident is defined in the Proposed Rule as an occurrence that "actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually jeopardizes, without lawful authority, an information system."

The Proposed Rule sets forth with specificity what types of incidents would constitute a reportable Covered Cyber Incident.

A Cyber Incident that meets any of the following impact-based criteria is a Substantial Cyber Incident:

- *Substantial Loss of Confidentiality, Integrity or Availability*: The first criterion is a "substantial" loss of confidentiality, integrity, or availability (CIA) of an information system (including operational technology) or a network. The Proposed Rule's commentary notes that whether loss is "substantial" will depend on a variety of factors, including the type, volume, impact and duration of the loss, such as an attack that cuts off services for an extended period or persistent access to information systems by a threat actor.
- *Serious Impact on Safety and Resilience*: The second criterion is a "serious" impact on the safety and resiliency of operational systems and processes. The Proposed Rule's commentary cites to NIST definitions of safety and operational resilience, and notes that "serious" will also depend on a variety of factors, such as the safety hazards posed by an incident.
- *Significant Operational Disruption*: The third criterion is a disruption of the ability to engage in business or industrial operations, or deliver goods or services, due to: (1) an attack (including but not limited to a denial-of-service attack, ransomware attack, or exploitation of a zero-day vulnerability) against (a) an information system or network or (b) an operational technology system or process; or (2) a loss of service facilitated through, or caused by, a compromise of a cloud service provider (CSP), managed service provider (MSP), other third-party data hosting provider or by a supply chain compromise. The Proposed Rule's commentary notes that the disruption must be significant, akin to the "substantial" and "serious" qualifiers discussed above.
- *Significant Third-Party Compromise*: The last criterion is unauthorized access to an information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either a compromise of a CSP, MSP, other third-party data hosting provider or a supply chain compromise. While similar to the loss of CIA, this criterion is focused on compromise caused by a third-party or a downstream incident within an entity's supply chain. Again, the Proposed Rule's commentary notes that the impacts must be significant to meet this criterion.

The commentary to the Proposed Rule provides specific examples of incidents that are likely and unlikely to qualify as a Substantial Cyber Incident, which are outlined in the tables below. However, the commentary notes that these examples are not exhaustive, nor do they constitute a formal declaration that a similar incident would or would not be a Substantial Cyber Incident.

Examples of Incidents That Likely Would Qualify As a Substantial Cyber Incident
1. A distributed denial-of-service attack that renders a Covered Entity's service unavailable to customers for an extended period of time.

2. Any cyber incident that encrypts one of a Covered Entity's core business systems or information systems.
3. A cyber incident that significantly increases the potential for a release of a hazardous material used in chemical manufacturing or water purification.
4. A cyber incident that compromises or disrupts a Bulk Electric System cyber system that performs one or more reliability tasks.
5. A cyber incident that disrupts the ability of a communications service provider to transmit or deliver emergency alerts or 911 calls, or results in the transmission of false emergency alerts or 911 calls.
6. The exploitation of a vulnerability resulting in the extended downtime of a Covered Entity's information system or network.
7. A ransomware attack that locks a Covered Entity out of its industrial control system.
8. Unauthorized access to a Covered Entity's business systems caused by the automated download of a tampered software update, even if no known data exfiltration has been identified.
9. Unauthorized access to a Covered Entity's business systems using compromised credentials from a managed service provider.
10. The intentional exfiltration of sensitive data in an unauthorized manner for an unauthorized purpose, such as through compromise of identity infrastructure or unauthorized downloading to a flash drive or online storage account.

Examples of Incidents That Likely Would *Not* Qualify As a Substantial Cyber Incident

1. A denial-of-service attack or other incident that only results in a brief period of unavailability of a Covered Entity's public-facing website that does not provide critical functions or services to customers or the public.
2. Cyber incidents that result in minor disruptions, such as short-term unavailability of a business system or a temporary need to reroute network traffic.
3. The compromise of a single user's credential, such as through a phishing attempt, where compensating controls (such as enforced multifactor authentication) are in place to preclude use of

those credentials to gain unauthorized access to a Covered Entity's systems.
4. Malicious software is downloaded to a Covered Entity's system, but antivirus software successfully quarantines the software and precludes it from executing.
5. A malicious actor exploits a known vulnerability, which a Covered Entity has not been able to patch but has instead deployed increased monitoring for tactics, techniques and procedures (TTPs) associated with its exploitation, resulting in the activity being quickly detected and remediated before significant additional activity is undertaken.

Ransom Payments

The Proposed Rule also defines a Ransom Payment, which must be reported to CISA within 24 hours, as any transfer of money, property or asset delivered in response to an extortion demand in connection with a Ransomware Attack. The proposed definition of Ransomware Attack generally covers any occurrence that actually or imminently jeopardizes an information system or the information on that system without lawful authority that involves, but is not limited to, the use or threat of use of malicious code, denial-of-service, or "another digital mechanism" to interrupt or disrupt operations or the confidentiality, integrity or availability of data in order to extort payment. This definition would include the use of malware to encrypt a victim's system, but, if broadly read, may also include the theft or copying of data followed by an extortion demand.

See "Ransomware and Incident Response Considerations for Global Companies" (Nov. 29, 2023).

Timing, Manner and Content of Required Reports

The Proposed Rule would mandate four types of reports: Covered Cyber Incident Reports, Ransom Payment Reports, Joint Covered Cyber Incident and Ransom Payment Reports, and Supplemental Reports (collectively, CIRCIA Reports).

Covered Cyber Incident Reports

Covered Cyber Incident Reports must be submitted to CISA not later than 72 hours after the Covered Entity develops a reasonable belief that the Covered Cyber Incident occurred. While the Proposed Rule does not provide a specific definition for "reasonable belief," the commentary states that an entity may need to conduct a preliminary analysis to develop a reasonable belief that a Covered Cyber Incident occurred, which it says is a "much lower threshold" than confirmation of an incident. The commentary goes on to say that this preliminary analysis should be within hours (rather than days), and that "reasonable belief" would be viewed from the perspective of a subject matter expert (not at the "executive officer level").

Ransom Payment Reports

Ransom Payment Reports must be submitted within 24 hours of disbursing payment, regardless of whether the payment relates to a reportable Covered Cyber Incident.

Joint Covered Cyber Incident and Ransom Payment Reports

A Covered Entity can also submit a Joint Covered Cyber Incident and Ransom Payment Report if the payment relates to the Covered Cyber Incident. The report must be submitted to CISA within 72 hours after the Covered Entity reasonably believes a Covered Cyber Incident occurred, but only if the Ransom Payment was also submitted within that 72-hour time frame.

Supplemental Reports

Until a Covered Cyber Incident "has concluded and has been fully mitigated and resolved," a Covered Entity must "promptly" submit a Supplemental Report whenever "substantial new or different information" arises. Covered Entities can optionally submit a Supplemental Report solely to inform CISA that a Covered Cyber Incident "has concluded and has been fully mitigated and resolved."

According to the commentary, "substantial new or different information" includes, but is not limited to:

- information the Covered Entity was required to provide as part of an earlier report but did not have at the time of submission;
- other information to correct or supplement an earlier report; and
- information required for a Ransom Payment Report, if the Covered Entity makes a Ransom Payment after submitting an initial Covered Cyber Incident Report (in such case, the Supplemental Report regarding the Ransom Payment must be submitted within 24 hours of disbursing payment).

The commentary also states that the completion of two particular milestones is a "good indication" that an incident "has concluded and has been fully mitigated and resolved": (1) the entity has completed an investigation of the incident, gathered all necessary information and documented all relevant aspects of the incident; and (2) the entity has completed steps required to address the root cause of the incident (*e.g.*, completed any necessary containment and eradication actions, identified and mitigated all exploited vulnerabilities, and removed any unauthorized access).

Additionally, the commentary provides that a Covered Entity should have a good-faith belief that further investigation would not uncover any "substantial new or different information" about the Covered Cyber Incident.

Specifics on Content of CIRCIA Reports

The Proposed Rule creates differing content obligations for each type of required report. In general, Covered Entities must include identifying information about the Covered Entity, a description of the incident (including its impact), the TTPs of the threat actor, indicators of compromise (IOCs), the identity of the threat actor, if known, and, if a Covered Entity makes a ransom payment, details about the transaction. The table below summarizes the contents of a Covered Cyber Incident Report and Ransom Payment Report.

Category	Details
Description of the Covered Cyber Incident or Ransomware Attack	1. Description of affected information systems, networks or devices, including the technical details and physical locations of such networks, devices and/or information systems (including whether any such resources support the Intelligence Community or contain certain national defense-related information); 2. Description of any unauthorized access, informational impacts or compromise, and network locations where activity was observed; 3. Dates pertaining to the incident (*e.g.*, detection date, date it began, duration of access); and 4. Description of operational impacts to the Covered Entity, as well as information related to potential economic, public health and safety, and national security impacts.
Impacted Data	The categories of information that were, or are reasonably believed to have been, accessed or acquired without authorization.
Vulnerabilities, Defenses, TTPs and IOCs	A description of any exploited vulnerabilities and security defenses the Covered Entity had in place, as well as the TTPs used to perpetrate the incident and IOCs associated with the threat actor. This may include, as applicable, a description or sample of any malware used by the threat actor, if available.
Identity of the Threat Actor	If known, identifying or contact information related to the threat actor, and information or evidence supporting the entity's attribution of the threat actor.
Mitigation/ Response	Description of any mitigation and response activities taken by the Covered Entity in response to the incident, including an assessment

	of effectiveness and any law enforcement entities that have been engaged.
Information Specific to Ransomware Attacks	The ransom payment date, demand and instructions, as well as information that may help identify the completed transaction and what occurred as a result of the Covered Entity making the payment (*e.g.*, data was returned or decrypted by the threat actor).

The Proposed Rule indicates that CIRCIA Reports would be submitted through an online form on CISA's web-based portal with exceptions for cases where the portal is not available to a Covered Entity (*e.g.*, due to an ongoing cyberattack).

Ashden Fein is the vice chair of Covington's global cybersecurity practice, where he advises clients on cybersecurity and national security issues. In particular, he specializes in advising clients on cybersecurity incident response, risk and crisis management, government and internal investigations, and regulatory compliance.

Caleb Skeath is a partner in Covington's data privacy and cybersecurity group. He advises clients on a broad range of cybersecurity and privacy issues, including cybersecurity incident response, cybersecurity and privacy compliance obligations, internal investigations, regulatory inquiries, pre-incident compliance and preparation, and defending against class-action litigation.

Web Leslie is an associate in Covington's data privacy and cybersecurity group. He previously served in government in various roles at the DHS, including at the National Protection and Programs Directorate, the predecessor to CISA, where he specialized in cybersecurity and critical infrastructure, public-private partnerships and interagency cyber operations.

Shayan Karbassi is an associate in Covington's data privacy and cybersecurity group. He assists clients with cyber and data security incident response and preparedness, government and internal investigations, and regulatory compliance. He previously served in government as a member of the U.S. Intelligence Community.

Covington associate Kristen Chapman also contributed to this article.

© 2024 Mergermarket Limited. All rights reserved.