ECKERT SEAMANS ATTORNEYS AT LAW

September 2024

Cybersecurity, Data Protection & Privacy Update

# Cybersecurity and Infrastructure Security Agency ("CISA") Proposed Cyber Security Incident Reporting Requirements

By Matthew H. Meade, Elizabeth Wilson and Gregory P. Mazmanian

## Overview

On April 4, 2024, CISA[1], an agency under the Department of Homeland Security, released a proposed rule that requires certain covered entities operating in critical infrastructure sectors to report cyber incidents to CISA. CISA issued the rule under the authority provided to it by the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA")[2]. At this time, CISA has only released a proposed rule and the public comment process closed in July, 2024[3]. The final rule requiring notification is expected to be published in 2025 and will go into effect in 2026.[4] When the final rule goes into effect, it will require covered organizations to notify CISA if they experience a "covered cyber incident"[5] or make a ransomware extortion payment.[6] Under the proposed rule, a covered entity experiencing a covered cyber incident would have seventy-two (72) hours to report a covered cyber incident.[7] Additionally, a covered entity would have twenty-four (24) hours to report a ransom payment.[8]

## Who Must Report – Covered Entities

The CISA reporting requirements apply to sixteen critical infrastructure sectors and do not include any entities that are considered a "small business" under 13 C.F.R. part 121[9].[10] The Small Business Administration ("SBA") classifies businesses based on their industry and size standard determined in either millions of dollars or number of employees. A table to assist a business in determining if they qualify as a small business under the SBA can be found here. The sixteen critical infrastructure sectors that are required to report to CISA include:

(1) Covered chemical facilities under the Chemical Facility Anti-Terrorism Standards pursuant to 6 CFR part 27[11];

(2) Wire or radio communications service providers such as radio and television broadcasters, cable television operators, satellite operators, telecommunications carriers, submarine cable licensees, fixed and mobile wireless service providers, voice over internet protocol providers, or internet service providers;

(3) Critical manufacturing sector infrastructure entities that engage in primary metal manufacturing, machinery manufacturing, electrical equipment, appliance, and component manufacturing, or transportation equipment manufacturing;

(4) Entities that provide operationally critical support to the Department of Defense or processes, stores, or transmits covered defense information;

(5) Emergency service providers to a population of at least 50,000 individuals and includes law enforcement, fire and rescue services, emergency medical services, emergency management, or public works that contribute to public health and safety;

(6) Bulk electric and distribution system entities;

(7) Financial services entities;

(8) State, local, Tribal, or territorial government entities with populations of at least 50,000 individuals;

(9) Educational facilities;

(10) Entities involved with information and communications technology to support elections processes including voter registration databases, voting systems, and technologies used to report, display, validate, or finalize election results;

(11) Public health-related providers including certain hospitals and drug or device manufacturers;

(12) Information technology entities that (i) provide products or services to the Federal Government, (ii) sells, licenses, or maintains software with certain attributes[12], (iii) is an original equipment manufacturer, vendor, or integrator of operational technology hardware or software components, or (iv) performs functions related to domain name operations;

(13) Owns or operates a commercial nuclear power reactor or fuel cycle facility;

(14) Transportation system entities;

(15) Entities subject to regulation under the Maritime Transportation Security Act; and

(16) Community water system or publicly owned treatment works owners and/or operators that serve a population of more than 3,300 people.[13]

## What Must Be Reported

Covered entities must report (1) covered cyber incidents and (2) any ransomware payments made, even if the ransomware attack[14] does not qualify as a covered cyber incident.[15] Covered cyber incident is defined as a substantial cyber incident experienced by a covered entity.

A covered cyber incident is defined as a "substantial cyber incident" experienced by a covered entity.[16]

A substantial cyber incident is defined as: (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 (i) compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or (ii) supply chain compromise.[17]

Additionally, a "substantial cyber incident" resulting in the impacts listed above in (1) through (3) includes any cyber incident regardless of cause, including, but not limited to, any of the above incidents caused by (i) a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; (ii) a supply chain compromise; (iii) a denial-of-service attack; (iv) a ransomware attack; or (v) exploitation of a zero-day vulnerability.[18]

The term "substantial cyber incident" does not include: (1) any lawfully authorized activity of a United States Government entity or SLTT[19] Government entity, including activities undertaken pursuant to a warrant or other judicial process; (2) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; or (3) the threat of disruption as extortion, as described in 6 U.S.C. 650(22)[20].[21]

## Reporting Deadlines and How to Report

A covered entity experiencing a substantial cyber incident will have seventy-two (72) hours after the covered entity reasonably believes the covered cyber incident has occurred to report an incident. Additionally, a covered entity would have twenty-four (24) hours after the ransom payment has been disbursed to report a ransom payment.[22] CISA currently has an online portal where reports can be submitted; however, this portal will likely need to be updated to conform to the reporting required under the rule[23]. Currently, reporting through the CISA online portal is voluntary. When the rule goes into effect in 2026, CISA will have four (4) categories of reporting including a (1) Covered Cyber Incident Report (used to report covered cyber incidents), (2) Ransom Payment Report (used to report ransomware payments), (3) Joint Covered Cyber Incident (used to report both covered cyber incidents and ransomware payments), and (4) Supplemental Reports (used to report incident updates).[24] The proposed rule includes detailed requirements on what information needs to be notified to CISA based on each report type.[25]

## Moving Forward

Given the short notification deadlines built into the new CISA reporting requirements, it is essential that organizations determine now whether they are a covered entity under the proposed rule and, if so, regularly test their incident response plans in advance of an actual incident so that notifications can be timely and compliant.

## Resources

- Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 6 CFR Part 226, https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements
- CIRCIA: Notice of Proposed Rule Making: In Brief, https://crsreports.congress.gov/product/pdf/R/R48025#:~:text=1%20This%20NPRM%20aims%20to,comment%20until%20June%203%2C%202024.
- What Would Be A Covered Entity Under CIRCIA As Proposed in 6 CFR § 226.2, https://www.cisa.gov/sites/default/files/2024-05/24-0630-Covered-Entity-Infographic-04242024-508c.pdf.
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.
- Cyber Incident Reporting for Critical Infrastructure Act of 2022, Notice of Proposed Rulemaking Informational Overview, https://www.cisa.gov/sites/default/files/2024-05/CIRCIA%20NPRM%20Overview%20May_508cL.pdf.

## How We Can Help

ECKERT SEAMANS ATTORNEYS AT LAW

This Cybersecurity, Data Protection & Privacy Alert is intended to keep readers current on developments in the law and is not intended to be legal advice. If you have any questions, please contact Matthew H. Meade at 412.566.6983 or mmeade@eckertseamans.com, Elizabeth Wilson at 215.851.8497 or ewilson@eckertseamans.com, Gregory Mazmanian at 215-851-8439 or gmazmanian@eckertseamans.com a member of our Cybersecurity, Data Protection & Privacy Practice Groups, or any other attorney at Eckert Seamans with whom you have been working for further information and assistance.

[1] https://www.cisa.gov/.

[2] 6 U.S.C. 681-681(g).

[3] CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, DHS, PROPOSED RULE, CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT (CIRCIA) REPORTING REQUIREMENTS, [Docket No. CISA–2022–0010] ("CISA Proposed Rule"), *available at: https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements*.

[4] *See* CONGRESSIONAL RESEARCH SERVICE, CIRCIA: NOTICE OF PROPOSED RULE MAKING: IN BRIEF, ("CISA Rule Summary") at p. 1, *available at:* https://crsreports.congress.gov/.

[5] *See* CISA Proposed Rule at § 226.1.

[6] CISA Rule Summary at 1.

[7] *See* 6 U.S.C. 681b(a)(1)(A); CISA Proposed Rule at §226.5(a).

[8] *See* 6 U.S.C. 681b(a)(2)(A); CISA Proposed Rule at §226.5(b).

[9] *See* Small Business Size Regulations, https://www.ecfr.gov/current/title-13/chapter-I/part-121.

[10] CISA Proposed Rule at § 226.2(a).

[11] DEPARTMENT OF HOMELAND SECURITY, CHEMICAL FACILITY ANTI-TERRORISM STANDARDS, 6 CFR Part 27, *available at*: https://www.ecfr.gov/current/title-6/chapter-I/part-27.

[12] Must have one of the following attributes: (A) Is designed to run with elevated privilege or manage privileges; (B) Has direct or privileged access to networking or computing resources; (C) Is designed to control access to data or operational technology; (D) Performs a function critical to trust; or (E) Operates outside of normal trust boundaries with privileged access. CISA Proposed Rule at § 226.2(b)(12)(ii).

[13] *See Id.* at § 226.2(b)(1)-(16).

[14] CISA defines ransomware attack to mean an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or that actually or imminently jeopardizes, without lawful authority, an information system that involves, but need not be limited to, the following: (1) The use or the threat of use of: (i) Unauthorized or malicious code on an information system; or (ii) Another digital mechanism such as a denial-of-service attack; (2) To interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system; and (3) To extort a ransom payment. (4) Exclusion. A ransomware attack does not include any event where the demand for a ransom payment is: (i) Not genuine; or (ii) Made in good faith by an entity in response to a specific request by the owner or operator of the information system. *Id.* at § 226.1.

[15] *Id.* at § 226.3(a)-(d).

[16] *Id.* at § 226.1.

[17] *Id.*

[18] *Id.*

[19] State, local, tribal, and territorial ("SLTT").

[20] 6 U.S.C. 650(22) refers to the definition of ransomware as above in endnote IV. https://uscode.house.gov/.

[21] CISA Proposed Rule at § 226.1.

[22] *See Id.* at § 226.5(a)-(d).

[23] *See* https://www.cisa.gov/report.

[24] CISA Proposed Rule at § 226.5(a)-(d).

[25] *See* CISA Proposed Rule at § 226.7-11.