SOPHOS

Sophos Guidance on the Cyber Incident Reporting for Critical Infrastructure Act of 2022

A Sophos Whitepaper. February 2024

About CIRCIA

In March 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) into law in the United States. Its enactment requires the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA, within 24 months of passing the law. The new law grants CISA with its first-ever enforcement powers.

CISA is expected to deliver a Notice of Proposed Rulemaking (NPRM) in early 2024 that will highlight the proposed reporting requirements, which are expected to be available for feedback before final publication in 2025. For updated guidance and feedback opportunities, organizations can visit https://www.cisa.gov/CIRCIA.

Who will be affected by this legislation?

The legislation implements regulations on United States "Covered Entities" in the critical infrastructure sector, as defined by Presidential Policy Directive 21[1]. Covered entities are organizations within industry sectors considered to be "critical infrastructure," listed in the table below. The sectors and their Sector Specific Agencies (SSAs) include, but are not limited to:

SECTOR	SECTOR SPECIFIC AGENCY (SSA)
Chemical	Department of Homeland Security
Commercial Facilities	Department of Homeland Security
Communications	Department of Homeland Security
Critical Manufacturing	Department of Homeland Security
Dams	Department of Homeland Security
Defense Industrial Base	Department of Defense
Emergency Services	Department of Homeland Security
Energy	Department of Energy
Financial Services	Department of the Treasury
Food and Agriculture	U.S. Department of Agriculture Department of Health and Human Services
Government Facilities	Department of Homeland Security General Services Administration
Healthcare and Public Health	Department of Health and Human Services
Information Technology	Department of Homeland Security
Nuclear Reactors, Materials, and Waste	Department of Homeland Security
Transportation Systems	Department of Homeland Security Department of Transportation
Water and Wastewater Systems	Environmental Protection Agency

It is worth noting that Education is considered a subsector of the Government Facilities Sector,[2] and the Education Facilities Subsector encompasses pre-kindergarten through 12th grade, as well as post-secondary public, private, and proprietary education facilities.

1 https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf
2 https://www.dhs.gov/xlibrary/assets/nppd/nppd-ip-education-facilities-snapshot-2011.pdf

What are the requirements of the legislation?

Reporting is not required until CISA's Final Rule implementing CIRCIA's reporting requirements goes into effect, which is expected in 2025. Until then, organizations are strongly encouraged to voluntarily share cyber incident information with CISA, and they can be reached 24/7 at report@cisa.gov, or (888) 282-0870[3], or their online portal at https://www.cisa.gov/report. More information regarding the final legislation and voluntary reporting can be found here[4].

However, once the Final Rule goes into effect, it will likely require "Covered Entities" to:

- Report a covered cyber incident within 72 hours
- Report a ransomware payment within 24 hours of making the transaction
- Submit updates on a previously submitted report if new information becomes available, or a ransomware payment was made after submitting a report
- Preserve data relevant to the incident or ransom payment according to procedures to be outlined in the final legislation

If a "Covered Entity" is a victim of a cyber incident and makes a ransomware payment prior to the 72-hour reporting requirement, they may likely be allowed to submit one single report, however, final reporting procedures are still to be determined.

What constitutes a covered cyber incident?

The final definition is yet to be proposed, however it will likely include at a minimum:

- Substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes
- Disruption of business or industrial operations, including due to a denial-of-service attack, ransomware attack, or exploitation of a zero-day vulnerability, against:
  - an information system or network
  - an operational technology system or process
- Unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise

The final legislation will also likely account for the sophistication or novelty of tactics used to perpetrate a cyber incident, as well as:

- The type, volume, and sensitivity of the data at issue
- The number of individuals directly or indirectly affected or potentially affected by such a cyber incident
- Potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers

3 https://www.cisa.gov/sites/default/files/2022-11/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf
4 https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

What must the contents of a report include?

The final required reporting content may vary, and will be available after publication, but as a best practice in incident response management, Covered Entities should be prepared to report:

1. Incident date and time
2. Incident location
3. Type of observed activity
4. Detailed narrative of the event
5. Number of people or systems affected
6. Company/Organization name
7. Point of Contact details
8. Severity of event
9. Critical Infrastructure Sector if known
10. Anyone else that was informed

Other information that may be required could include:

- The impact to the operations of the covered entity
- A description of exploited vulnerabilities where applicable and actor TTPs (tactics, techniques, and procedures) used to perpetrate the cyber incident
- Categories of information believed to have been accessed
- Any identifying information or contact information related to the attacker if available, ie in the case of a ransomware event
- Contact information for an entity that may have made a ransom payment on behalf of the affected organization
- The ransom instructions, demand, and type of currency used

Which third parties can report on the affected party's behalf?

Entities deemed critical infrastructure that are required to report a cyber incident or ransom payment may be allowed to use a third party to submit the report on their behalf. The final guidance on how to use a third party will be available with the final regulations, but it is expected that the list of third parties will likely include:

- Incident response companies
- Insurance providers
- Service providers
- Information Sharing and Analysis Organizations (ISAOs)
- Law firms

What happens if an affected entity fails to comply with reporting requirements?

If an impacted organization misses the 72-hour deadline, a subpoena may be issued by the Director of CISA to compel disclosure of information deemed necessary. The final regulations will fully define enforcement methods and what can be expected.

What protections do reporting parties have?

CIRCIA reports are expected to be considered the commercial, financial, and proprietary information of the covered entity and are likely exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the 'Freedom of Information Act'), as well as any provision of State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records. Such an exemption is likely to require the reporting entity to assert its rights in writing under this section.

This document does not constitute legal advice nor does it reflect the views of Sophos or its employees. Companies should consult their own counsel for legal guidance on any laws and regulations.

2024-02-07 (WP-NP)

SOPHOS