Baker McKenzie.

Cybersecurity
FACT SHEET

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

Who?

- The **Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)** applies to "covered entities" that operate in a "critical infrastructure sector."
- "**Covered entity**" will be defined by Rules published by the Cybersecurity and Infrastructure Security Agency (CISA). CISA proposed Rules on April 4, 2024 that indicate CIRCIA will apply to entities in critical infrastructure sectors that either exceed the small business size standard (as set by the Small Business Administration) or meets any "sector based criterion" as follows:
  - Own or operate a chemical facility
  - Provide wire or radio communications
  - Own or operate critical manufacturing infrastructure
  - Provide operationally critical support to the Department of Defense or processes defense information
  - Perform an emergency service
  - Own or operates financial services infrastructure
  - State, local, Tribal, or territorial government entities
  - Education facilities
  - Information and communications technology to support elections processes
  - Essential public health services
  - Information technology entities
  - Own or operate a nuclear power reactor or fuel cycle facility
  - Transportation system entities
  - Subject to the Maritime Transportation Security Act
  - Own or operate a community water system or publicly owned treatment work

What?

- CIRCIA will require covered entities that operate in critical infrastructure sectors to report "substantial cyber incidents" and ransom payments to CISA. The Proposed Rules include four types of "impacts" that may be considered "substantial cyber incidents." Under the Proposed Rule, a covered entity may satisfy its incident reporting obligation by reporting substantially similar information in a substantially similar timeframe to another federal agency.
- "Covered cyber incident" is defined as a "substantial cyber incident." Under the Proposed Rule "substantial cyber incidents" are ones that result in (1) substantial loss of confidentiality, integrity or availability of a covered entity's information system or network, (2) serious impact on the safety and resiliency of a covered entity's operational systems and processes, (3) disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services, (4) unauthorized access to a covered entity's information system or network that is facilitated through or caused by supply chain compromise or the compromise of a cloud service provider.
- "Cyber incident" is defined as "an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system."

Where?

- CIRCIA applies to covered entities within the United States (US).
- CIRCIA does not expressly state any geographic restrictions if the cyber incident occurs outside the US. Accordingly, businesses that operate critical infrastructure within the US may be required to report even if the cyber incident did not occur within the US.
- CISA may provide additional detail on the geographical application of CIRCIA when defining "covered entities" subject to rulemaking.

Why?

- Approximately 85% of the United States' critical infrastructure is owned by the private sector.
- The purpose of CIRCIA is to improve the cybersecurity of critical infrastructure by requiring covered entities to report cybersecurity incidents and ransom payments to CISA. Such information will provide CISA with information to identify cyber threats and vulnerabilities, respond to cyber incidents, and prevent threats of harm.
- Failure to adhere to CIRCIA reporting obligations could result in court proceedings.

When?

- CIRCIA requires covered entities that operate in critical infrastructure sectors to report covered cyber incidents within **72 hours** of the companies' reasonable belief that a cyber incident has occurred and to report ransom payments within **24 hours** after a payment is made.
- Mandatory reporting is not required until the effective date of the final rule, which is likely in September 2025. CISA encourages voluntary reporting until then.
- CISA published a Notice of Proposed Rulemaking (NPRM) on April 4, 2024. CIRCIA requires CISA to issue final rules within 18 months of the publication of the NPRM (i.e., by September 2025)

How Baker McKenzie can help

- **Consult with outside counsel to issue a legal opinion as to whether you are a covered entity**
- **Refresh playbooks and develop frameworks for determining whether a cyber incident is reportable and/or a "substantial cyber incident"**
- **Train and exercise your incident response team to understand the new reporting obligations**
- **Stay updated on new developments and regulations by subscribing to Connect on Tech, our blog and podcast series**

PROUD SPONSOR OF
INFRAGARD NATIONAL MEMBERS ALLIANCE
2024

CONTACT: Justine Phillips | Partner | Los Angeles | justine.phillips@bakermckenzie.com | +1 310 269 7698

bakermckenzie.com