Utilities Technology Council™
2550 South Clark Street Suite 960
Arlington, VA 22202 USA

Cyber Incident Reporting for Critical Infrastructure (CIRCIA)

Background:

In late September 2021, the U.S. House of Representatives and the U.S. Senate introduced two cybersecurity bills respectively: The Cyber Incident Reporting for Critical Infrastructure Act of 2021 and The Cyber Incident Reporting Act of 2021.[iii]

In March of 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA). CIRCA designates DHS's Cybersecurity and Infrastructure Security Agency (CISA) as the lead agency responsible for developing and implementing regulations requiring "**covered entities**" to report "**covered cyber incidents**" and **ransomware payments** to CISA.[iii]

Issue:

As CISA is now positioning to assume authority to perform regulatory functions and have enforcement power, there are several mandatory rulemaking activities CISA must complete before the CIRCIA cyber incident reporting requirements begin:

- CISA is required to develop and publish a Notice of Proposed Rulemaking (NPRM), which is currently open for public comment.
- CISA is required to develop and publish a Final Rule (a rule promulgated by an administrative agency after the public has had an opportunity to comment on the proposed rule)
- CISA is required to consult with various entities, such as Sector Risk Management Agencies (SRMA's), throughout the rulemaking process:
  - DOE for the Energy Sector
  - DHS for Communication Sector
  - DHS for Information Technology
- CISA is required to create a DHS-chaired Cyber Incident Reporting Council
- CISA is and has been receiving input into the NPRM from critical infrastructure owners and operators and other members. However, they are not mandated to do so within required rulemaking schedule required by statue.
- A Request for Information (RFI) through which CISA is soliciting public input for 60 days started September 12, 2022, on potential aspects of the proposed regulation prior to publication of the Final Rule.

CISA hopes the CIRCA will give the agency more insight into threats targeting the homeland's critical infrastructure, quickly deploy resources and assistance to victims who are under attack or have experienced an attack. CISA also hopes that CIRCIA will perform some type of trend analysis derived from threat reporting across the 16 critical infrastructure sectors. As an agency, CISA is required to publish proposed rules implementing the reporting requirements within 24 months of CIRCIA's enactment. Final rules must be published within 18 months of the proposed rules. Although the Request for Information (RFI) from the public ended November 14, 2022, the CIRCIA is still in the beginning stages of defining how and when it will take effect for Critical Infrastructure.

UTC Analysis

UTC strives to support our members in simplifying the task of effectively performing their critical infrastructure duties. There are key items in this bill UTC is highlighting, because they will impact members by adding additional regulatory reporting requirements for critical infrastructure owners and operators, such as:

- CIRCIA requires CISA to develop and issue regulations requiring **covered entities** to report to CISA any **covered cyber incidents** within **72** hours from the time the entity reasonably believes the incident occurred.
  - CIRCIA defines a "covered entity" as an entity that falls within one of the 16 critical infrastructure sectors identified in Presidential Policy Directive 21 (PPD-21)
  - CIRCIA defines a "covered cyber incident" as:
    - "Cyber incident that leads to

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.

- A 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 or 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."

- If a covered entity experiences a ransomware attack and makes a ransomware payment, the covered entity must report that payment to CISA no later than 24 hours of making the payment.
- CIRCIA will provide protections and anonymity for covered entities that report cyber incidents or ransom payments to CISA under both mandatory and voluntary circumstances.

Contact Information

Brett Kilbourne, Senior Vice President for Policy & General Counsel: Brett.Kilbourne@utc.org
Cordell Briggs, Vice President for Policy & Cybersecurity: Cordell.Briggs@utc.org
Eric Wagner, Manager for Advocacy: Eric.Wagner@utc.org
Campbell Baskin, Legislative Assistant: Campbell.Baskin@utc.org

---

References

[i] https://www.congress.gov/bill/117th-congress/house-bill/5440/
[ii] https://www.congress.gov/bill/117th-congress/senate-bill/2875
[iii] https://www.cisa.gov/circia