Lowenstein Sandler

Cyber Incident Reporting Requirements To Be Implemented Under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)– NPRM Expected Late 2023–Early 2024

By Abbey E. Baker and Kei Komuro

Background:
In March 2022, President Joe Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) into law, ushering in a new era of enhanced cybersecurity measures. This legislation addresses the critical need for rapid response and coordination in the face of cyber incidents targeting vital infrastructure.

Mandates and Objectives:
CIRCIA mandates the Cybersecurity and Infrastructure Security Agency (CISA) to take a central role in this effort. As outlined in Section 681b, CISA is tasked with developing and enforcing regulations that compel covered entities to report cyber incidents and ransom payments to CISA. The primary objectives of this reporting are to provide timely assistance to victims, analyze incident trends, and share vital information to bolster the capabilities of network defenders.

Rulemaking Timeline:
CISA is required to publish a Notice of Proposed Rulemaking (NPRM) within 24 months of CIRCIA's enactment – making the NPRM deadline March 2024. Following the NPRM, a Final Rule will be issued within 18 months. CISA Director Jen Easterly has stated that CISA is finishing the NPRM and expects it to be published by early 2024.

CISA's Key Functions:
CIRCIA empowers CISA with a range of functions described in Section 681b. These extend beyond mere data collection and encompass:

1. **Rapid Deployment:** CISA's responsibility includes swiftly deploying resources and support to affected entities to mitigate ongoing cyberthreats.
2. **Incident Analysis:** CISA will analyze reported incidents to identify patterns and trends, enhancing the ability to respond effectively to emerging threats.
3. **Threat Intelligence Sharing:** CISA will facilitate efficient sharing of threat intelligence among entities, fostering a collective cybersecurity defense posture.

Defining Critical Infrastructures and Covered Entities:
Section 681b defines a Covered Entity as an entity in a critical infrastructure sector—industries and services integral to national security, economic stability, and public welfare. These sectors, essential for societal functioning and economic vitality, include but are not limited to:

- Transportation
- Communications
- Financial Services
- Healthcare and Public Health
- Food and Agriculture
- Emergency Services
- Chemical
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Information Technology
- Commercial Facilities
- Government Facilities
- Nuclear Reactors, Materials, and Waste

Health Care and Public Health Sector:
Section 681b delves into the specifics of the Healthcare and Public Health sector within critical infrastructure. This sector includes subsectors like:

- **Health Information Technology:** Encompasses medical research institutions, information standards bodies, and electronic medical record systems vendors. The adoption of electronic health records is widespread due

to incentives from the Patient Protection and Affordable Care Act (ACA).
- **Medical Materials:** Involves medical equipment and supply manufacturing and distribution. Pharmaceutical distributors play a crucial role in delivering medicines and health care products.
- **Laboratories, Blood, and Pharmaceuticals:** Combines government and private assets, including pharmaceutical manufacturers, drugstore chains, laboratory associations, and blood banks. E-prescribing and electronic transmission of prescriptions are common within this subsector.

Future Developments:
Given the recent enactment of CIRCIA, Section 681b highlights that detailed rules and rulemakings will be issued by CISA (Section 681f). These rules will provide comprehensive guidance for reporting cyber incidents and ransom payments. They will also outline collaboration procedures between CISA and affected entities, ensuring a coordinated response to cyberthreats.

Reporting Start Date:
Until the Final Rule takes effect, organizations are not required to report cyber incidents. However, proactive information sharing during the rulemaking period is encouraged. Stay tuned for updates on the implementation of reporting deadlines.

How Companies Should Respond:
When the NPRM is published, companies should review the proposed rule and identify whether they may fall within the scope of the proposed reporting requirements. Affected companies will then have 18 months to develop draft procedures implementing appropriate reporting policies and preparing for implementation of the Final Rule.

In Summary:
CIRCIA, as detailed from Section 681a to Section 681g, is a significant advancement in national cybersecurity. It mandates reporting of cyber incidents within critical infrastructure, with CISA at the forefront. The legislation's emphasis on key sectors, including Healthcare and Public Health, underscores the importance of their protection. As detailed rules evolve (Section 681f), they will guide compliance and coordinated responses, fortifying the nation's cyber resilience.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

ABBEY E. BAKER
Counsel
T: 202.753.3806
abaker@lowenstein.com

KEI KOMURO
Associate
T: 212.419.5948
kkomuro@lowenstein.com