masuda funai

News & Types: Client Advisories

The Cyber Incident Reporting for Critical Infrastructure Act: Preventing Cyber-Attacks or Promoting a Race Against the Clock?

3/30/2023

By: Christen J. McGlynn

Practices: Litigation

Over the course of the COVID-19 pandemic, the United States experienced a rise in high-profile cyber-attacks. In March 2022, President Joe Biden signed the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA") into law, creating a federal reporting obligation for both public and private companies operating in a critical infrastructure. Entities designated as "critical infrastructures" under the Act will be required to report cyber incidents within **72 hours** to the Cybersecurity and Infrastructure Security Agency (CISA) of the United States Department of Homeland Security and ransomware payments within **24 hours**. Although the Act was designed to assist and prevent victims of cyber-attacks—it may also come with a hefty price for companies that lose their race against the clock.

The Act casts a wide net encompassing a variety of sectors that will be considered critical infrastructures, including chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services, energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

To promote accurate reporting and address concerns involving sensitive information becoming the subject of lawsuits, the Act provides some protection for companies. For example, any cyber incident or ransom payment report cannot be used by a federal, state or local government to regulate any of the activities disclosed in the report. Additionally, the reports will be exempt from disclosure under freedom of information laws; be considered commercial, financial and proprietary business information; and cannot be used as evidence in **any proceeding**, including both state and federal court, as well as any regulatory bodies. This Act will have an interesting effect on litigation as it prevents both the report and any information used to prepare the report from being discoverable.

Owners and operators of entities that fall under one of these sectors need to be aware of the changes and repercussions of this new Act and how it may affect business moving forward. The Act will not go into effect

until the Director of CISA finalizes all the required regulatory mandates. However, failure to comply with the new reporting requirements may result in serious consequences, including:

1. significant monetary penalties for each day the violation continues; and/or
2. being denied the protections mentioned above.

Between September and November 2022, CISA sought public input regarding the process and procedure for submitting reports, as well as term definitions and interpretations. Although the Act is currently in effect, these requirements are stilling pending. Companies currently operating in one of the above-mentioned sectors are encouraged to reach out to their attorney to stay updated and in compliance with the requirements and regulations of the Act once they have been finalized by CISA.

Christen McGlynn is a member of the Masuda Funai Litigation Practice Group and would be happy to answer any questions you have regarding CIRCIA or other cyber-security issues. She can be reached at CMcGlynn@masudafunai.com.