An Overview of the Strengthening American Cybersecurity Act

Client Alert

3.31.22

What You Need to Know

- The Strengthening American Cybersecurity Act will impose cyber incident and ransomware attack response protocol for a broad spectrum of businesses operating in numerous core industry sectors of the U.S. economy.
- These industry sectors include chemical, communications, energy, financial services, food & agriculture, government facilities, healthcare, IT, transportation, and waste management.
- The Act, although targeted towards organizations constituting critical infrastructure, will potentially have far-reaching implications for businesses of all types and sizes.

By: Meredith C. Sherman

The Strengthening American Cybersecurity Act, signed into law on March 15, 2022 by President Joe Biden, underscores an increased focus on rapid disclosures and robust protections for the private sector in the cybersecurity space, intensified by Russia's invasion of Ukraine and the corresponding potential threat to U.S. national security.

As outlined below, the Cybersecurity and Infrastructure Security Agency (CISA), an operational component of the federal Department of Homeland Security, will be promulgating implementing regulations that will clarify the scope of the Act, including the definition of "covered entities" within the "critical infrastructure" sectors that will have reporting obligations under the Act.

That said, businesses of all types and sizes are well advised to familiarize themselves with the information presented in this Alert. Additionally, the updating of cybersecurity-related policies, procedures and incident response plans should take into consideration an assessment of how the Act may impact that business's industry sector and specific operations.

Reporting Requirements

The Strengthening American Cybersecurity Act requires that certain organizations constituting critical infrastructure submit reports to CISA under certain timelines. Specifically, the Act imposes requirements on "covered entities" within the "critical infrastructure" sectors to report to CISA within 72 hours of discovery of a cybersecurity incident and within 24 hours following any ransomware payments.

These new reporting obligations will not take effect until CISA promulgates implementing regulations. With regard to timing, CISA's notice of proposed rulemaking must be promulgated within 24 months, with the final rule to be issued within 18 months of the notice of proposed rulemaking.

Critical Infrastructure and Covered Entities

CISA's implementing regulations will clarify the breadth of the Act by defining "covered entities" within the "critical infrastructure" sectors.

The Strengthening American Cybersecurity Act refers to Presidential Policy Directive 21 from 2013, which defines "critical infrastructure sector" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Presidential Policy Directive 21 defines the following sectors as critical infrastructure:

- 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
- Waste and Wastewater Systems

Given that these sectors comprise a significant portion of the U.S. economy, the Act has far-reaching implications for a broad spectrum of business operations.

Covered Cyber Incidents

The CISA final rule will also clarify the definitions of "covered cyber incidents" as well as providing rules regarding the manner and form of the reports to be submitted.

A "covered cyber incident" will at least include an incident that "leads to substantial loss of confidentiality, integrity, or availability of an 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...," or "unauthorized access or disruption of business or industrial operations due to compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or due to a supply chain compromise."

Reports submitted to CISA will be required to include a description of the covered cyber incident, and, where applicable, "a description of the vulnerabilities exploited and the security defenses that were in place, as well as the tactics, techniques, and procedures used to perpetrate the covered cyber incident." Reports regarding ransom payments will be required to provide a "description of the ransomware attack, including the estimated date range of the attack" and, where applicable, "a description of the vulnerabilities, tactics, techniques, and procedures used to perpetrate the ransomware attack."

Given the short turnaround time for reporting, all information may not be available at the time of the original report, which will likely prompt submissions of an updated or supplemental report if "substantial new or different information" becomes available.

Companies in many sectors will be potentially impacted by the Strengthening American Security Act and the reporting requirements to be more specifically defined when the final CISA rules are promulgated. We will continue tracking all related developments and will issue additional advisories accordingly, including an update when CISA releases its proposed implementing regulations.

Please contact the author of this Alert, **Meredith C. Sherman**, with any questions or to discuss your specific business circumstances.

Related Attorneys

Meredith C. Sherman

Partner

732.476.2672

Email