New Reporting Requirements for Critical Infrastructure and Businesses

Legal Alert
March 17, 2022
Foster Garvey Newsroom

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("the Act") was signed into law by the President on March 15, 2022, as part of the Consolidated Appropriations Act. The purpose of the Act is to educate critical infrastructure sectors about potential cyber threats and encourage timely sharing of relevant information. The Act also amends the Homeland Security Act of 2002 to add cyber incident reporting requirements for a "covered entity" in a critical infrastructure sector.

You may ask, "Do I need to worry about this?" It's too early to know the answer to that question. The Cybersecurity and Infrastructure Security Agency (CISA) is required to define "covered entity" by rule in a few years. The critical infrastructures that may contain "covered entities" are 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.

A Covered Entity's Responsibilities

Under the Act, a covered entity (as will be defined by rule) that experiences a substantial cyber incident (as will be defined by rule) must report the incident to CISA within 72 hours. A covered entity that makes a ransom payment in connection with a ransomware attack must report the payment to CISA within 24 hours. Covered entities must also provide supplemental information to CISA and preserve any data related to the incident as required by rule. Covered entities are permitted to voluntarily report any cyber incidents or ransom payments to CISA that are not required to be reported.

Related Services

Business & Corporate Finance

Commercial & IP Transactions

Communications, Telecom & Media

Environment & Natural Resources

Financial Services

Food & Beverage

Health Care

Insurance Coverage

IP & Technology

Privacy, Cybersecurity & Data Protection

Transportation & Logistics

Water Quality

Cybersecurity and Infrastructure Security Agency's Responsibilities

CISA will need to draft rules to fill in a number of holes in the Act, such as to define *who* and *what types of incidents* are covered by the Act. (For some peace of mind, the Act does provide guidance on the scope of what should be included and not included in the rules.) CISA has two years to publish a Notice of Proposed Rulemaking (NPRM) and then 18 months following the NPRM to issue final rules. Once the rules are published, CISA is required to conduct an "outreach and education campaign" to ensure that no one is caught off guard by the requirements.

In addition to rulemaking, CISA is given a number of other responsibilities under the Act. Within 24 hours of receiving a report from a covered entity, CISA must share the information with other federal agencies, as appropriate, such as with the FBI. CISA is also required to work with other federal agencies to locate and track ransom payments. Additionally, CISA must assess the potential impact of cyber incidents on public health and safety.

CISA is required to aggregate and analyze cyber incidents to assess the effectiveness of security controls and identify how adversaries get around security controls. CISA will use this information to coordinate efforts with various private and public partners and provide partners with anonymized reports about cyber incidents and trends. CISA must publish quarterly public reports with its findings and recommendations and work with academic institutions to strengthen cybersecurity research. The goal of all of this information sharing is to identify ways to prevent or mitigate similar future cyber incidents.

In a statement released on March 11, 2022, CISA Director Jen Easterly stated, "CISA will use these reports from our private sector partners to build a common understanding of how our adversaries are targeting U.S. networks and critical infrastructure. This information will fill critical information gaps and allow us to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims." While many entities may grumble about the new reporting requirements in the Cyber Incident Reporting for Critical Infrastructure Act of 2022, the purpose of the Act is undoubtedly patriotic – to collectively decrease cybersecurity risks to private and public entities in the United States and protect its citizens.

Our experienced Privacy, Cybersecurity & Data Protection team at Foster Garvey will be tracking any developments in the rulemaking process. If you have any questions, including how to get involved in the rulemaking process or how to stay in compliance with privacy and cybersecurity obligations, please feel free to contact us at any time.