Data Privacy and Cybersecurity

The Cyber Incident Reporting for Critical Infrastructure Act of 2022

By: Shoba Pillay, Aaron R. Cooper and Ashwini Bharatkumar

On March 15, 2022, President Biden signed into law the "Cyber Incident Reporting for Critical Infrastructure Act of 2022" (the Act) as part of the 2022 federal funding bill.[1]

Among other things, the Act requires critical infrastructure sector entities to report cybersecurity breach incidents and ransomware payments to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).

Key Takeaways

- The Act covers entities "in a critical infrastructure sector" as further defined by CISA's final rule.
- Covered entities must report covered cyber incidents to CISA within **72 hours** after reasonably believing a covered incident has occurred.
- Covered entities must report ransomware payments within **24 hours** of making a payment.
- The Act specifies enforcement authority for CISA and information protection provisions.

CISA to Issue Final Rule

The Act directs CISA, in consultation with Sector Risk Management Agencies,[2] the Department of Justice, and other federal agencies, to issue a Notice of Proposed Rulemaking to develop a final rule implementing the Act's cyber incident reporting requirements. CISA must publish its Notice of Proposed Rulemaking within two years of the Act's promulgation and must issue a final rule within 18 months of publishing the Notice of Proposed Rulemaking. The Act authorizes CISA to subsequently amend or revise its final rule.

The scope of key language in the Act will depend on definitions set forth by CISA's final rule. An entity covered by the Act's reporting requirements, referred to as a "covered entity," is defined in the Act as "an entity in a critical infrastructure sector" that meets criteria to be specified in CISA's final rule. CISA's final rule must consider the following factors:

1. the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;
2. the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and
3. the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

"Covered cyber incident" is similarly defined as "a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established" in CISA's final rule. The Act sets forth minimum criteria of covered cyber incidents, including substantial loss of or impacts on information or operational systems, business or industrial process disruption, or unauthorized access or disruption caused by a loss of third party services or by a supply chain compromise.

Covered entities must report covered cyber incidents to CISA within **72 hours** "after the covered entity reasonably believes that the covered cyber incident has occurred," and report ransomware payments

within **24 hours** of payment. If a covered entity learns "substantial new or different information" or makes a ransomware payment after providing an incident report, it must provide a supplement or update to CISA. The statute also instructs covered entities to "preserve data relevant to the covered cyber incident or ransom payment in accordance with" CISA's final rule.

Covered entities may submit reports through third parties such as "an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit the required report."

Incident Report Sharing

The Act includes provisions for incident report sharing between federal agencies, seeking to streamline reporting burdens. In particular, any federal agency receiving a report of a cyber incident from a covered entity must share that report with CISA within 24 hours of receipt, unless a shorter period is agreed-upon. The Act also directs any federal agency "that receives incident reports from entities" to enter into an agreement to share such reports with CISA. Federal incident report sharing requirements may yield exemptions from CISA's reporting requirements if covered entities report "substantially similar information to another Federal agency within a substantially similar timeframe." This exemption applies once a federal agency to which a covered entity reports institutes a cyber incident report sharing agreement with CISA. Federal agencies such as the Securities and Exchange Commission have recently proposed rules requiring cyber incident reporting from regulated entities. *See* Jenner & Block's client alert on the SEC's proposed rule. Such reporting obligations—if accompanied by an information sharing agreement with CISA and if providing information substantially similar to that required by CISA, on a timeline substantially similar to that required by CISA—may fulfill CISA's incident reporting requirements.

Enforcement Powers

Significantly, the Act also empowers CISA to issue a subpoena for information about an incident or ransomware payment if a covered entity does not report the incident and does not respond to an information request from CISA. Failure to respond to a subpoena can be referred to the Attorney General for civil enforcement action.

Information Protection

Reports submitted in compliance with the Act, or submitted voluntarily, will be considered "commercial, financial, and proprietary information of the covered entity" if the covered entity indicates that such information protection is required. Reports are exempt from FOIA and from state, tribal, and local freedom of information laws, and report submission will not automatically waive privileges or other legal protections (such as trade secret protection). The Act also specifies that an entity cannot face legal action simply for submitting a covered cyber incident report or ransom payment report to CISA, and it further specifies that incident reports and communications associated with preparing such reports are not subject to discovery or use as evidence in adjudication.

Ransomware Initiatives

Additionally, the Act directs CISA to pursue two ransomware-related initiatives. First, the Act directs CISA to establish a "ransomware vulnerability warning pilot program" to develop capabilities to identify information systems vulnerable to common ransomware attacks, and to notify owners of such systems of their security vulnerability. Second, the Act requires the Director of CISA, in consultation with the National Cyber Director, the Attorney General, and the Director of the Federal Bureau of Investigation, to establish and chair a Joint Ransomware Task Force to "coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation."

In sum, the Act expands cyber incident reporting requirements for critical infrastructure entities and expands CISA's authority to implement the rules governing cyber incident reporting. Entities likely to be covered by the Act's requirements should consider engaging in CISA's rulemaking process, including by submitting comments in response to CISA's Notice of Proposed Rulemaking.

Jenner & Block will continue to monitor the expansion of cybersecurity incident reporting requirements and the CISA rulemaking process.

---

[1] The full text of the federal funding bill is available here: https://www.congress.gov/bill/117th-congress/house-bill/2471/text. The Act is found in Division Y of the funding bill.

[2] A Sector Risk Management Agency (SRMA), is a federal agency identified by *Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience* as the federal government liaison for each of the 16 critical infrastructure sectors.

Contact Us

Shoba Pillay
spillay@jenner.com | Download V-Card

Aaron R. Cooper
acooper@jenner.com | Download V-Card

Ashwini Bharatkumar
abharatkumar@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower
Co-Chair
dbitkower@jenner.com
Download V-Card

Madeleine V. Findley
Co-Chair
mfindley@jenner.com
Download V-Card

Kelly Hagedorn
Co-Chair
khagedorn@jenner.com
Download V-Card

Shoba Pillay
Co-Chair
spillay@jenner.com
Download V-Card