Updates
September 12, 2022

CISA Seeks Input on New Cybersecurity Reporting Requirements

President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) on March 15, 2022. The background and contours of CIRCIA are discussed in a previous update. CIRCIA authorizes and directs the Cybersecurity and Infrastructure Security Agency (CISA) to issue rules that require "covered entities"—a subset of critical infrastructure providers that CISA will define—to report "covered cyber incidents" and payments made in response to ransomware attacks. Such reports will be mandatory, and CIRCIA provides the government with enforcement authority.

As part of the rulemaking process, CISA has issued a public Request for Information (RFI) and scheduled public listening sessions. The RFI solicits public comment for 60 days, beginning September 12, 2022. Written comments are due on November 16, 2022. The listening sessions are scheduled in different cities around the United States through November 16, 2022, with a Washington, D.C., session that has not yet been scheduled.

Every company in critical infrastructure sectors has an interest in the outcome of the rulemaking process. CIRCIA specifically requires reporting based on compromises of supply chains, third-party hosting services, cloud service providers, and managed service providers. As a result, companies in those industries may also take on new requirements, whether directly through regulations or indirectly through contractual obligations.

The new CIRCIA rules will govern the scope and depth of reporting requirements for companies in critical infrastructure sectors as defined in Presidential Policy Directive 21 (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 waste and wastewater systems). They will determine which companies must submit reports, prescribe a reporting process, and set reporting thresholds based on the severity of events. Specific examples of topics on which CISA seeks comment include the following:

- What critical infrastructure entities will be subject to the new requirements as "covered entities."
- What types of incidents will fall under the reporting requirements as "covered cyber incidents" or "substantial cyber incidents."
- What constitutes a "supply chain compromise" for reporting purposes.
- When a covered entity has a "reasonable belief" that a reportable incident has occurred, which starts a 72-hour mandatory reporting period.
- What triggers the 24-hour reporting period for ransomware payments.
- How CISA will balance the government's need for information with companies' needs to respond to and remediate incidents.
- The manner in which companies and third parties, such as cybersecurity companies and law firms, can collaborate to meet reporting requirements.
- Deconfliction with other legal requirements.
- Costs that potential regulatory requirements may impose.

Takeaway

CIRCIA reporting requirements will be enforceable and may be substantial. All companies in critical infrastructure sectors and those that provide support services may be affected by forthcoming regulations, and they should strongly consider responding to CISA's request for input.

Authors

David Aaron

Senior Counsel
DAaron@perkinscoie.com

Explore more in

Privacy & Security | National Security | Technology Transactions & Privacy Law | Environment, Energy & Resources | Infrastructure Development | Communications | Financial Services & Investments | Energy & Natural Resources | Oil & Gas | Mining | Aerospace & Transportation

Related insights

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights

Update

FDA Food Import and Export Updates for Industry