Updates
April 08, 2022

Answers to Common Questions Regarding New CIRCIA

President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) on March 15, 2022. The enactment of CIRCIA follows attacks on critical infrastructure, such as the May 2021 ransomware attack on Colonial Pipeline and the Russian government attacks against the energy sector alleged in two indictments unsealed on March 24, 2022. CIRCIA comes in the context of an overall government focus on enhancing cybersecurity, as reflected in a recent executive order and proposed U.S. Securities and Exchange Commission (SEC) rules. Together, these measures bring to bear federal procurement policies, corporate transparency requirements, targeted reporting mandates, and (ideally) enhanced threat analysis and information sharing. Accordingly, the collection of new rules should be taken seriously. In the particular context of critical infrastructure, the threat is real, and as President Biden recently stated, "[m]ost of America's critical infrastructure is owned and operated by the private sector and critical infrastructure owners and operators must accelerate efforts to lock their digital doors."

Although CIRCIA's private-sector requirements will not take effect until the Cybersecurity and Infrastructure Security Agency (CISA) director promulgates a new rule, understanding it now can help affected entities understand the potential scope of their upcoming obligations and anticipate how CIRCIA will fit into the broader cybersecurity architecture and regulatory environment.

Common Questions About CIRCIA

When do new reporting requirements take effect?

CIRCIA requires the CISA director to propose a rule within two years of its enactment. A final rule must be issued within 18 months of the initial notice of the proposed rule.

What will CIRCIA require?

"Covered entities" (see next question) will be required to report two categories of events. These include "covered cyber incidents" (CCIs) and ransom payments in response to ransomware attacks. The CISA director's rule will define CCIs based on factors such as the following:

- Substantial loss of confidentiality, integrity, or availability of information systems or networks.
- Serious impact on safety or resiliency of operational systems; disruption of business or industrial operations.
- Disruptions accomplished through compromises of cloud service providers, managed service providers, third-party hosting providers, or supply chains.

The CCI definition will also account for the sophistication and novelty of an attack, the data affected by an attack, the scope of affected individuals, and the potential impact of an attack on industrial control systems (ICS) such as supervisory control and data acquisition (SCADA), distributed control systems (DCS), and programmable logic controllers (PLCs).

The rule will require a covered entity to report a CCI within 72 hours and to report a ransom payment in response to a ransomware attack within 24 hours. Covered entities will be required to submit updates and supplemental reports as information is discovered.

Under the rule, entities of any type may also voluntarily report information to CISA about cyber incidents or ransom payments, and covered entities may include in their required reports additional information that may enhance situational awareness of cyber threats.

What companies will be affected?

The rule will define "covered entities," which will be subject to mandatory reporting requirements. "Covered entities" will consist of entities in one of the 16 critical infrastructure sectors defined in Presidential Policy Directive 21: (1) chemical, (2) commercial facilities, (3) communications, (4) critical manufacturing, (5) dams, (6) defense industrial base, (7) emergency services, (8) energy, (9) financial services, (10) food and agriculture, (11) government facilities, (12) healthcare and public health, (13) information technology, (14) nuclear reactors, (15) materials and waste transportation systems, and (16) waste and wastewater systems.

Entities within these sectors will be selected based on the consequences of their disruption or compromise, the likelihood that they would be targeted, and the extent to which their compromise would disrupt critical infrastructure operations. CIRCIA directs CISA to conduct outreach to likely covered entities.

One point of issue, based on CIRCIA's specific reporting requirement regarding compromises through third parties, is whether supply-chain vendors and providers of cloud services, managed services, or third-party hosting will incur reporting requirements, either to CISA or to clients who are covered entities.

How will covered entities make the required reports?

The CISA director will prescribe the manner and form of reports. A covered entity may use a third party, such as a law firm or incident response company, to submit reports on its behalf.

How will the rule be enforced?

CIRCIA authorizes the CISA director to request information from a covered entity to help determine whether a CCI or ransom payment occurred. If the covered entity does not adequately respond, the CISA director may use a subpoena and, if necessary, refer the matter to the U.S. Department of Justice (DOJ) for enforcement.

What protections does CIRCIA offer?

Information contained in required or voluntary reports belongs to the entity making the report. It is exempt from freedom-of-information laws and reporting such information does not waive any privilege or legal protection.

Submission of a report that conforms to the rule cannot predicate any cause of action. It is important to note that this only applies to actions based "solely" on the submission of a report. Similarly, no report or related communication, document, or material can be used in evidence, be subject to discovery, or otherwise be used in a proceeding, as long as it was created for the "sole purpose" of preparing or submitting the report.

What will the government do with reported information?

CIRCIA expands the role of the U.S. Department of Homeland Security (DHS) in receiving, analyzing, and disseminating threat information. Reported information may be disclosed to federal agencies for a "cybersecurity purpose" such as protecting information systems; identifying cyber threats; and responding to, preventing, or

mitigating a specific threat of serious bodily or economic harm. Reported information may also be used to respond to or investigate—or to prosecute—offenses involving serious threats to minors and certain crimes relating to espionage, economic espionage, and computer fraud and abuse.

Information about a CCI or ransom payment that the government obtains "solely through" reporting to CISA under CIRCIA cannot be used to regulate or take action against the reporting entity (unless a regulatory agency allows regulated companies to satisfy regulatory obligations by reporting to CISA). Regulators can use reported information to develop or implement regulations.

Information provided in response to a subpoena, however, can predicate a regulatory enforcement action or a criminal prosecution.

CIRCIA requires CISA to anonymize victim information when sharing the information in reports with nonfederal entities, such as critical infrastructure owners and operators, and the general public.

Takeaway

As the scope and content of the new requirements become clear, companies may wish to seek counsel for advice on data privacy and security, as well as on specific critical infrastructure sectors, and for assistance in meeting new security and reporting requirements.

Authors

David Aaron

Senior Counsel
DAaron@perkinscoie.com

Explore more in

Privacy & Security National Security Infrastructure Development Communications Oil & Gas Aerospace & Transportation

Related insights

Update

Coming Soon: Judicial and Agency Interpretations of Washington's Pay Disclosure Law

Update

October Tip of the Month: U.S. Department of Labor Issues Guidance on AI in the Workplace