GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity

March 2022

Congress Passes 72-Hour Federal Breach Reporting Law for Critical Infrastructure

This GT Alert covers the following:

- Applies to critical infrastructure, which potentially consists of up to 16 different, broadly defined industries.
- Requires breach reporting to CISA within 72 hours of a substantial cyber incident and within 24 hours of paying a ransom.
- Gives CISA up to two years to issue proposed rules and an additional 18 months to issue final rules, although it could move much faster in response to recent cyber threats from Russia.
- Substantially increases CISA's budget to address cyber crime.

As part of a larger spending bill signed by President Biden on March 15, 2022, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRA) to increase funding for the federal Cybersecurity and Critical Infrastructure Agency (CISA). CIRA requires companies considered to be in a "critical infrastructure" sector to notify CISA within 72 hours of a significant cyber incident and, in the case of ransomware, within 24 hours of making a payment.

Although Congress has struggled for years to enact comprehensive data privacy and security legislation, CIRA is a significant step towards increasing federal government oversight of data security incidents.

Reporting historically has been required only for companies in certain federally regulated industries, like health care or banking. Importantly, the bill itself does not identify which of the critical infrastructure sectors will be considered "covered entities" under the law and therefore – that definition will be part of CISA's proposed rulemaking. CISA may look to the 16 industries considered "vital" to the United States' physical and economic security and public health or safety:

- 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
- Water and Wastewater Systems

Whether CISA will ultimately include all 16 of these categories, some of which are broadly defined and would ensnare a substantial number of companies that might not consider themselves to be critical infrastructure, remains to be seen. For example, "commercial facilities" would include "a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging," including shopping malls, sports arenas, hotels, office buildings, and condos.

Another unknown is what types of cyber incidents will be considered reportable events. The bill makes it clear that reporting will only be required of a "substantial cyber incident," and defines "cyber incident" as "an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system." The Act provides some examples, like a significant incident with a substantial loss or serious impact on safety and resiliency of operational systems, like a distributed denial of service (DDOS) attack, ransomware attack, or exploitation of a zero day vulnerability. The Act also encourages voluntary reporting of other cyber incidents not specifically required to be reported.

CISA has time to decide how to define what will constitute a reportable event. CIRA gives CISA two years to issue proposed rules and another 18 months to issue final rules. However, in light of increasing warnings from the White House that Russian will continue to use cyberattacks as part of its war chest against Ukraine and countries supporting Ukraine, rulemaking could occur sooner than later.

Takeaways

Companies included among the 16 infrastructure industries as defined by CISA should consider making preparations now while we await proposed rulemaking.

- **Evaluate Data Security Practices**. Given the risk of an imminent attack by Russian interests, and the increasing cyberattacks that have occurred in the last two years for monetary gain, companies should consider conducting a security risk assessment to benchmark the sophistication of their information security practices, including practices to prevent and detect a cyber incident.

- **Review or Audit Service Providers**. Following the Russian attack on SolarWinds Orion, which resulted in 18,000 organizations downloading a security software update that potentially enabled Russian backdoor access to their systems, reviewing vendors whose data security could impact yours is more important than ever. Security questionnaires, a zero-trust program, and invoking contractual audit rights (where applicable), may be advisable.
- **Revise Incident Response Plan**. Companies that have developed a robust incident response plan which covers the business and legal issues associated with a security incident will be better positioned to respond quickly and ensure short reporting time frames are met. Incident Response Plans should identify internal incident response team members, create a process for declaring a security incident, include a communications plan for notifying and updating key stakeholders, including regulators, and include contact information for data security vendors.
- **Practice Wargaming**. Tabletop exercises are essential to test an incident response plan and identify and address any gaps. Senior executives and incident response team members can walk through a cyberattack scenario in a controlled environment to ensure they are prepared in the event of the real thing.

Author

This GT Alert was prepared by:

- Jena M. Valdetero | +1 312.456.1025 | valdeteroj@gtlaw.com