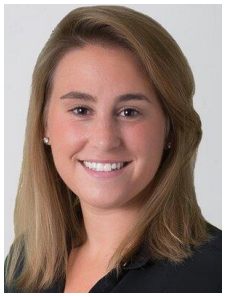
Navigating Ambiguities In New Cyber Reporting Law

By **Shardul Desai, Joel Roberson and Marissa Serafino** (March 30, 2022)

Shardul Desai

Joel Roberson



Marissa Serafino

After years of debate, Congress has passed bipartisan legislation requiring owners and operators of critical infrastructure to report cyber incidents to the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, or CISA, within 72 hours, and ransomware payments within 24 hours.

The Cyber Incident Reporting for Critical Infrastructure Act, or CIRCIA, was included in the fiscal year 2022 omnibus appropriations bill.[1] The U.S. House of Representatives approved the spending bill on March 9, and the U.S. Senate approved it on March 11. President Joe Biden signed the bill into law on March 15.

The cyber reporting provision, Division Y, in the appropriations bill was derived from the Strengthening American Cybersecurity Act,[2] a legislative package that was unanimously approved by the Senate on March 1.

After failing to pass similar proposed legislation over the last few years, Congress approved these cyber incident reporting requirements due to growing concerns of potential cyberattacks in retaliation for the U.S. response to Russia's invasion of Ukraine.

Congress has become keenly aware of how these attacks can affect the American public after the past year of high-profile ransomware attacks on entities within critical infrastructure sectors, such as the attack on Colonial Pipeline Co., which resulted in a gasoline shortage to parts of the South and the East Coast, and the attack on JBS SA, which disrupted meat production and distribution in the U.S.

The new cyber reporting obligations will not become effective until CISA promulgates rules to define the entities within the critical infrastructure sectors that will be affected by this law and the types of substantial cyber incidents it covers. The bill requires CISA to issue a notice of proposed rulemaking on these definitions within 24 months from the date of the bill's enactment and issue a final rule within 18 months of issuing the proposed rule.

The following is a summary of the new cyber incident reporting requirements along with some key takeaways for potentially affected critical infrastructure owners and operators. These owners and operators should begin to prepare for implementation of the act in anticipation of having to disclose to CISA their cybersecurity defense and response practices.

Cyber Incident Reporting Requirements and Protections for Reporting Entities

Covered Entities, Covered Cyber Incidents and Time Period for Reporting

CIRCIA requires covered entities to report a covered cyber incident to CISA within 72 hours after it reasonably believes a covered cyber incident has occurred.

The law, however, does not specifically define "covered entities," "covered cyber incident," or "reasonably believes." Instead, the law provides minimum parameters for some of these definitions and requires CISA, through rulemaking, to provide a "clear description of the types of entities that constitute covered entities" and "a clear description of the types of substantial cyber incidents that constitute covered cyber incidents."

Covered Entities

At a maximum, the term "covered entities" cannot be broader than those entities that fall within the designated critical infrastructure sectors identified in Presidential Policy Directive 21.[3] Under PPD-21, the following 16 critical infrastructure sectors[4] were identified: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services, energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems.[5]

However, Congress specifically did not define "covered entities" to include each and every entity in these critical infrastructure sectors, which suggests its intention that a subset of such entities should be subject to these cyber incident reporting obligations.

In deciding what entities should be covered, CISA must consider the national security, economic, and public health and safety consequences of a cyberattack on the entity and the extent that a cyberattack will likely enable disruption of the reliable operation of critical infrastructure.

Covered Cyber Incidents

The bill defines a "covered cyber incident" as "a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule."

Although "substantial" is not defined in the bill, the bill 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,[6] or actually or imminently jeopardizes, without lawful authority, an information system."

A cyber incident does not include an occurrence that imminently, but not actually, jeopardizes information on information systems or information systems.

The bill further requires CISA, through rulemaking, to provide a clear description of the type of substantial cyber incidents that constitutes a covered cyber incident. At a minimum, CISA's description must include the following:

- A cyber incident that leads to substantial loss of confidentiality, integrity or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;

- A disruption of business or industrial operations, including due to a denial-of-service attack, ransomware attack or exploitation of a zero-day vulnerability against (1) an information system or network, or (2) an operational technology system or process; or

- Unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider or other third-party data hosting provider, or by a supply chain compromise.

Under this last prong, a cyberattack on a third-party service vendor may trigger an entity's notification requirements. This highlights the importance of conducting cybersecurity due diligence reviews of such service providers and requiring incident notification obligations in those contractual agreements.

Time Period for Reporting

The bill also does not define the term "reasonably believes," and it does not require CISA to define this term through rulemaking. Unless CISA provides additional clarity, this term may be subject to hindsight analysis and agency interpretation.

Separately, a covered entity must report to CISA a ransom payment resulting from a ransomware attack within 24 hours of making the payment. The law provides that the ransomware attack need not fall within the definition of "covered cyber incident" in order to trigger this payment reporting obligation.[7]

However, if a ransomware incident qualifies as a covered cyber incident, and a covered entity makes a ransom payment prior to the 72-hour cyber incident reporting requirement, the entity may submit one report to satisfy both reporting requirements.

Report Contents

As part of the rulemaking process, CISA must establish the specific content required in cyber incident and ransomware payment reports. At a minimum, these reports must include the following information to the extent that it is applicable and available:

- A description of the covered incident or ransomware attack;

- A description of the vulnerabilities exploited and the security defenses that were in place, as well as the tactics, techniques and procedures used to perpetrate the cyber incident or ransomware attack;

- Any identifying or contact information related to each actor reasonably believed to be responsible for such cyber incident or ransomware attack;

- For cyber incidents, the category or categories of information that were or are reasonably believed to have been subject to unauthorized access or acquisition;

- For ransomware payment, the date of the ransom payment, ransom payment demand, ransom payment instructions, information regarding where to send the payment and amount of the payment;

- Identification information of the affected entity; and

- Contact information for the affected entity or an authorized agent of the entity.

Preservation, Supplemental Reports and Voluntary Reports

CIRCIA requires covered entities to submit updated and supplemental reports when substantial new or different information becomes available until the entity notifies CISA that the cyber incident has concluded and been fully mitigated and resolved. As a result of this provision, entities may have to make several reports to CISA while managing a cyberattack and remediating their systems.

The act also provides that covered entities "shall preserve data relevant to the covered cyber incident or ransom payment," and CISA is required to clearly describe the types of data to be preserved through rulemaking. This requirement could potentially create a heavy burden on an entity's information technology and information security team in the middle of responding to a cyberattack.

The bill also directs CISA to aggregate and analyze submitted reports to facilitate intelligence-gathering concerning cyberattacks and information-sharing. As part of that effort, the law permits noncovered entities to voluntarily submit cyber incident or ransomware payment reports to CISA and provides these reports with the same level of protection as those filed by covered entities.

Protections for Reporting Entities

Unlike many cyber incident reporting laws, the bill recognizes some concerns with the waiver of privilege, potential litigation and regulatory risks, and public access to information associated with reporting cyber incidents to regulatory agencies.

Specifically, the law provides the following protections:

- The reports cannot be used in regulatory actions, including enforcement actions, against the covered entity;

- The reports are exempt from disclosure under Freedom of Information Act requests;

- The reports shall be considered the commercial, financial and proprietary information of the covered entity when so designated by the entity;

- The reports shall not constitute a waiver of any applicable privileges or protections provided by the law, including trade secret protections;

- No cause of action shall lie in or be maintained by the submission of the report;

- No report — and any communications or records created for the sole purpose of preparing, drafting or submitting the report — may be received in evidence, subject to discovery or otherwise used in any trial, hearing or other proceedings; and

- CISA shall anonymize the victim when engaging in information-sharing.

These protections far exceed other agencies' cyber and data breach notification obligations, which often fail to recognize the legal concerns that victim companies may face in providing notifications.

Noncompliance

Entities that do not comply with the cyber incident or ransomware payment reporting requirements may be subject to contempt of court proceedings. Under the act, CISA is authorized to request information from entities suspected of noncompliance.

If an entity fails to comply with an initial request for information, CISA may use subpoenas to obtain the information. If an entity fails to comply with the subpoena, CISA may refer the matter to the U.S. attorney general for civil action to enforce the subpoena, and a court may punish a failure to comply with the issued subpoena with contempt of court.

Harmonization Efforts With Other Agencies

Finally, the law authorizes federal agencies to coordinate, deconflict and harmonize federal incident reporting obligations. To achieve this objective, the law provides for agencies to enter into agreements and sharing mechanisms and, thereby, exempts covered entities to report cyber incidents to CISA in lieu of making a substantially similar report to another federal agency.

Although the harmonizing of reporting obligations is necessary and welcomed, covered entities may want to ensure that the aforementioned legal protections apply to these substantially similar reports made to other federal agencies.

Key Takeaways

Without CISA's proposed rules, owners and operators of critical infrastructure will not know whether they will qualify as a covered entity subject to these new reporting obligations. By not defining "covered entity" to include all entities in the critical infrastructure sectors, Congress granted CISA broad discretion to narrow the law's applicability related to owners and operators of critical infrastructure.

Although these reporting obligations will not become effective until CISA promulgates agency rules, owners and operators of critical infrastructure should take steps now to prepare for this new law.

One suggested step is for owners and operators to update their incident response plans to comply with these reporting obligations should they apply. The 72-hour and 24-hour requirements create a short window of time between when an entity reasonably believes it is experiencing a covered cyber incident and when it must report.

Moreover, the incident response plan should consider decision making regarding the structure for determining when an entity reasonably believes it is experiencing or had experienced a covered cyber incident. In some instances, an information technology and security professional could come to this conclusion far earlier than the entity's management or its attorneys. The uncertainty with respect to when the cyber incident reporting obligation starts may cause entities, out of an abundance of caution, to report incidents in an even shorter window of time.

The act also requires supplemental reporting for substantially new or different information. As such, many entities will be required to file multiple reports for the same cyber incident. Entities may want to consider how best to include checks within their incident response plans to ensure and account for supplemental reporting obligations.

In addition, cyberattacks on third-party vendors and service providers may affect a covered entity's reporting obligations. Therefore, owners and operators of critical infrastructure may want to reassess cybersecurity and data privacy risks within their vendor management program and be prepared to update its third-party vendor and service contracts accordingly. Such entities may want to consider strong due diligence reviews, periodic cybersecurity audits, data privacy flow-down provisions and contractual provisions requiring timely and detailed cyber incident notifications.

The preservation requirement also may require entities to reassess their information technology and security team's initial response to cyber incidents. When initially confronted by a cyber incident, information technology and security teams are focused on triage, containment and remediation. In many instances, information technology and security teams are not directly focused on evidence preservation. Depending on CISA's preservation rules, these teams may need to consider evidence preservation as part of the initial triage.

Finally, the explicit protections provided in this bill far exceed most cyber incident and data breach obligations. These protections likely will result in more detailed reporting. Yet, they raise concerns related to the lack of explicit protection in other agencies' cyber and data

breach notification obligations. The bill's requirement that federal agencies seek to harmonize the various notification laws is necessary given the myriad reporting obligations that companies face.

However, if an interagency agreement exists, an entity may only be required to report to another federal agency that may not apply the act's protections. Thus, it is advantageous for entities to report to CISA, unless the act's protections carry over.

Shardul Desai and Joel E. Roberson are partners, and Marissa C. Serafino is an associate, at Holland & Knight LLP.

Holland & Knight legislative and communications assistant Hannah M. Coulter contributed to this article.

[1] FY 2022 Omnibus Appropriations Bill (H.R. 2471), available at https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

[2] Strengthening American Cybersecurity Act, S.3600, available at https://www.congress.gov/bill/117th-congress/senate-bill/3600.

[3] Presidential Policy Directive 21, available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[4] Id.

[5] Each critical infrastructure sector has a sector-specific plan that addresses cybersecurity.

[6] "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. 44 U.S. Code § 3502. This includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems and programmable logic controllers.

[7] This provision, thus, suggests that not all ransomware attacks will qualify as a covered cyber incident.