Bond Case Briefs

Municipal Finance Law Since 1971

President Biden Signs Bill Expanding Cybersecurity Reporting Obligations.

President Biden signed the Consolidated Appropriations Act, 2022 into law on March 15, 2022. Section Y of the new omnibus appropriations bill is titled The Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("the Act"). Importantly, the Act significantly expands federal cybersecurity incident and ransom demand reporting requirements for critical infrastructure entities. In light of these new requirements, critical infrastructure entities who suspect that they may be subject to the Act should begin investigating how the Act will impact their business and consider establishing protocols which may be necessary to ensure compliance.

Notably, the Act does not directly define many necessary terms and obligations. Instead, the Department of Homeland Security's Director of the Cybersecurity and Infrastructure Security Agency ("CISA") has been tasked with promulgating a final rule finalizing these definitions and obligations. Within 24 months of the Act's enactment, CISA is required to begin the notice-an--comment rulemaking process. The final rule must then be published within the 18 months following the start of the rulemaking process. Interested stakeholders will want to review the proposed rule promptly when it is released and consider submitting comments as appropriate.

Incident Reporting Obligations

With respect to incident reporting, the Act requires covered entities to comply with new and expanded obligations when they experience a "covered cyber incident." The term "covered entity" means a critical infrastructure entity—as defined by Presidential Policy Directive 21 ("the Directive")—that satisfies the criteria established in CISA's final rule. Although CISA's criteria will remain unknown until the final rule is promulgated, the Directive clarifies the types of entities that may be subject to the expanded requirements.

Under the Directive, critical infrastructure entities are those operating in the following sectors:

- **Chemical sector.** Including manufacturing, storing, using, or transporting potentially dangerous chemicals.
- **Commercial facilities sector.** Includes a range of sites that are open to the public and draw large crowds for shopping, business, entertainment or lodging.
- **Communications sector.** Includes satellite, wireless and wireline providers, which depend on each other to carry and terminate their traffic.
- **Critical manufacturing sector.** Encompasses the production of primary metals; machinery; electrical equipment, appliances and components; and transportation equipment that may be susceptible to man-made and natural disasters.
- **Dams sector.** Delivers water retention and control services in the United States, including hydroelectric power generation, municipal and industrial water supplies, agricultural irrigation, sediment and flood control, river navigation for inland bulk shipping, industrial waste management and recreation.
- **Defense industrial base sector.** Encompasses research and development, as well as the design,

production, delivery and maintenance of military weapons systems, subsystems and components to meet U.S. military requirements. The sector provides products and services for mobilizing, deploying and sustaining military operations. It does not include the commercial infrastructure of those who provide services such as power, communications, transportation or utilities, which are covered under other sectors.
- **Emergency services sector.** Includes law enforcement, fire and rescue services, emergency medical services, emergency management and public works.
- **Energy sector.** Includes entities that focus on electricity, oil and natural gas.
- **Financial services sector.** Includes depository institutions, providers of investment products, insurance companies, and other credit and financing organizations, as well as the providers of the critical financial utilities and services that support these functions.
- **Food and agriculture sector.** Includes farms, restaurants, and registered food manufacturing, processing and storage facilities.
- **Government facilities sector.** Includes general-use office buildings and special-use military installations, embassies, courthouses, national laboratories and structures.
- **Healthcare and public health sector.** Focuses on protecting all sectors of the economy from terrorism, infectious disease outbreaks and natural disasters.
- **IT sector.** Covers hardware, software, and IT systems and services, along with the communications sector and the internet.
- **Nuclear reactors, materials and waste sector.** Encompasses most aspects of America's civilian nuclear infrastructure, such as nuclear facilities, materials and waste, as well as any cybersecurity related to these facilities.
- **Transportation systems sector.** Focuses on safely, securely and efficiently moving people and goods through the country and overseas. Subsectors include aviation, highway and motor carrier, maritime transport system, mass transit and passenger rail, pipeline systems, freight rail, postal and shipping.
- **Water and wastewater systems sector.** Concentrates on ensuring the supply of drinking water and wastewater treatment.

Similar to the definition of "covered entity," the full definition of "covered cyber incident" will not be available until CISA publishes the final rule. However, the Act establishes that the definition of "covered cyber incident" will contain certain key elements. Pursuant to the Act, the final rule's definition of "covered cyber incident" must require, at minimum, the occurrence of:

- 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.

CISA's final rule will also outline many substantive requirements such as incident reporting obligations and ransom reporting obligations. In each instance, the final rule shall require a covered entity to report the following within 72 hours of the covered entity's reasonable belief that a covered cyber incident has occurred:

- A description of the "covered cyber incident including i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably

believed to have been, affected by such cyber incident, ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations, iii) the estimated data range of such incident, and iv) the impact to the operations of the covered entity;"
- 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 "covered cyber incident;"
- Any identifying or contact information related to each actor reasonably believed to be responsible for such cyber incident;
- The category or categories of information that were, or are reasonably believed to have been, subject to unauthorized access or acquisition;
- Identification information of the impacted entity; and
- Contact information for the impacted entity or an authorized agent of the entity.

In the event that a covered entity makes a ransom payment, the final rule will also require the covered entity to make the following disclosures to CISA within 24 hours of such payment:

- A description of the ransomware attack, including the estimated date range of the attack;
- A description of the vulnerabilities, tactics, techniques, and procedures used to perpetrate the ransomware attack;
- Any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack;
- The name and other information that clearly identifies the covered entity that made the ransom payment or on whose behalf the payment was made;
- The contact information of the covered entity or authorized agent that made the ransom payment;
- The date of the ransom payment;
- The ransom payment demand, including the type of virtual currency or other commodity requested;
- The ransom payment instructions; and
- The amount of the ransom payment.

Additionally, the Act also requires a covered entity to submit updated reports to supplement previously provided information when substantial new information is discovered. Once a report is submitted, all data relevant to the "covered cyber incident" or ransom payment must then be preserved by the covered entity pursuant to procedures yet to be established through the rulemaking process.

Exceptions to Reporting Obligations

The exceptions to these reporting obligations are fairly narrow. For instance, while a covered entity would otherwise be required to make two reports to cover both a covered cyber incident and a ransom payment, the Act allows such an entity to combine all required information into a single report. Similarly, in the event that a covered entity is subject to certain reporting requirements to other Federal agencies, the report to the other agency may satisfy the entity's reporting obligations to CISA provided that a sharing agreement between the agencies exists.

Using a Third Party to Submit a Required Report or Make a Ransom Payment

A covered entity may either submit a required report itself or use a third party to do so. Such a third party can include an entity such as an "incident report company, insurance provider, service provider, Information Sharing and Analysis organization, or law firm." In the event that a covered entity utilizes a third party, it must be aware that the use of such a third party does not relieve the covered entity from its reporting requirement. Rather, a covered entity utilizing a third party is

subject to the same reporting obligations and timelines as it would be had it submitted the report or made the ransom payment itself.

Notably, third parties are largely exempt from independent obligations under the Act. Importantly, where a third party submits a report or makes a ransom payment on behalf of a covered entity, that third party is not obligated to submit a separate report on its own behalf. However, such a third party does have an obligation to advise the covered entity of their responsibilities regarding the covered entity's reporting obligations. Thus, businesses who act as third parties and provide reporting services to covered entities should remain apprised of all reporting requirements and prepare to advise their clients.

Incident Report Sharing and Data Use

Though the Act establishes substantial reporting obligations, it also limits CISA's ability to use and share the information provided by covered entities in the reports. Importantly, such information may only be used by the Federal Government for:

- Cybersecurity purposes;
- Identifying a cyber threat or security vulnerability;
- Purposes of responding to, "or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm;"
- Purposes of "responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor;" or
- Purposes of "preventing, investigating, disrupting, or prosecuting an offense arising out of a reported cyber incident."

In addition to the limitations on use, similar to other cyber threat information-sharing opportunities provided by the Federal Government, information contained in required reports is afforded further protections. Importantly, information obtained by CISA via a required report may not act as the basis for any cause of action. Similarly, such information is also protected from admission into evidence in any future proceeding. Thus, any information contained in a required report may not be received into evidence, subjected "to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other proceeding."

In providing these protections, the Act intends to enable covered entities to fully disclose all relevant information regarding a covered cyber incident without incurring the risk of potentially exposing itself to liability due to the content of the report. Additional protections establish that information disclosed to CISA pursuant to the Act:

- Is considered to be the "commercial, financial, and proprietary information of the covered entity when so designated by the covered entity;
- Is exempt from disclosure under the Freedom of Information Act (FOIA);
- Is exempt from disclosure required by any "State, Tribal, or local freedom of information law;"
- Is not considered to be a waiver of any "applicable privilege or protection provided by law, including trade secret protection;" and
- May be shared externally only when the victim's identity is anonymized.

Enforcement

In the event that a covered entity fails to comply with the new cyber incident reporting obligations, CISA's director may request information if it suspects the entity of noncompliance. If the covered entity fails to respond within 72 hours, CISA may then issue an administrative subpoena. Should the

covered entity subsequently fail to comply with the subpoena, CISA may turn the matter over to the U.S. Attorney General for civil enforcement and covered entity may potentially held in contempt of court.

However, prior to exercising their enforcement authority, the CISA director must first consider i) the complexity of determining whether a covered cyber event has occurred as well as ii) the covered entity's previous interactions with the agency and the likelihood that the entity is aware of its reporting obligations.

Other Notable Provisions

In addition to expanding reporting obligations, the Act also creates several entities and programs intended to improve the state of cybersecurity in the U.S. These additional provisions call for the creation of:

- The Cyber Incident Reporting Council, led by the Secretary of Homeland Security, which will be responsible for coordinating, deconflicting, and harmonizing Federal incident reporting requirements;
- A ransomware vulnerability warning pilot program intended to "leverage existing authorities and technology to specifically develop processes and procedures for . . . identifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners of those vulnerable systems of their security vulnerability;" and
- The "Joint Ransomware Task Force to coordinate an ongoing national campaign against ransomware attacks, and identify and pursue opportunities for international cooperation."

Key Takeaways

Though there is much that will remain unclear until CISA promulgates the final rule, businesses should, at the very least, be aware of the following:

To whom does the Act apply? The Act applies to covered entities as defined by CISA.

What does the act mandate? Reports must be made to CISA when the covered entity makes a ransom payment or experiences a covered cyber incident.

When must the report be made? Reports must be made to CISA within 72 hours of a business's reasonable belief that a covered cyber incident has occurred and 24 hours of any ransom payment.

How is the information contained in the reports protected? CISA may only use the information in the reports for very limited purposes outlined above. Such information is further protected from disclosure via discovery, FOIA requests, or other open records requirement, etc.

How is the Act enforced? The CISA may request information in the event that it believes a covered entity may be noncompliant. If the entity fails to respond to the request within 72 hours, the CISA may issue a subpoena. If the entity fails to respond to the subpoena, the CISA may turn the matter over to the U.S. Attorney General who may enforce the subpoena.

Crowell & Moring LLP – Sarah Rippy, Matthew B. Welling, Evan D. Wolff, Maida Oringher Lerner, Alexander Urbelis and Michael G. Gruden

March 24 2022