ALERT MEMORANDUM

Cyber Incident Reporting for Critical Infrastructure Act Signed Into Law

March 18, 2022

On March 15, 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which imposes federal reporting requirements for cyber incidents and ransomware attack payments. The legislation will require covered critical infrastructure entities—which will be defined in rulemaking—to report to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours of forming a reasonable belief that a substantial cyber incident has occurred and within 24 hours of making a ransom payment following a ransomware attack. The reporting requirements will not take effect until implementing regulations are enacted by CISA, which will take time to navigate the rulemaking process.

The new legislation was described by CISA's director as "a game-changer" that "marks a critical step forward in the collective cybersecurity of our nation," and represents the culmination of years of debate in Congress. The legislation aims to enhance the federal government's ability to provide assistance to victimized entities and to investigate ransomware attacks and other cyber incidents. Following the law's enactment, the focus shifts to the rulemaking process, which will flesh out the specific obligations for critical infrastructure entities to report to CISA. Entities that believe they will be covered by the Act should consider whether to participate in the rulemaking process and should begin analyzing whether they have sufficient policies, procedures, and systems in place to meet the eventual reporting requirements.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

NEW YORK

Joon H. Kim
+1 212 225 2950
jkim@cgsh.com

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Anthony M. Shults
+1 212 225 2693
ashults@cgsh.com

Background

As we detailed in a previous post on the Cleary Cybersecurity and Privacy Watch blog, cyber incident reporting has been a key focus of federal legislative proposals over the past several years. The political support for implementing reporting requirements has intensified in light of the United States' assistance to Ukraine, which has increased the potential for retaliatory cyberattacks on key U.S. infrastructure by the Russian government.

On March 15, 2022, President Biden signed the Consolidated Appropriations Act, 2022, an omnibus spending bill that includes the Cyber Incident Reporting for Critical Infrastructure Act (the Act). The text of the Act was derived from an earlier legislative proposal introduced by Senators Gary Peters (D-MI) and Rob Portman (R-OH).

The Cyber Incident Reporting for Critical Infrastructure Act

Required Reporting of Certain Cyber Incidents

The Act requires covered critical infrastructure entities to report substantial cyber incidents to CISA "not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred." Separately, any such entities that make a ransom payment as the result of a ransomware attack must report the payment to CISA "not later than 24 hours after the ransom payment has been made."

Covered entities have an obligation to update or supplement their initial report to CISA when substantial new or different information becomes available, until such time that they notify CISA "that the covered cyber incident at issue has concluded and has been fully mitigated and resolved." The entities must also preserve data relevant to the underlying incident or ransom payment as set forth in regulations to be adopted by CISA.

Covered entities may rely on a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit a required cyber incident report or a ransom payment report. Entities that have a legal or contractual obligation to make substantially similar reports to another federal agency may be exempt from the Act's reporting requirements if that agency has an agreement and mechanism in place to share the reports with CISA.

The reporting requirements described above will only take effect after CISA enacts regulations to implement the Act's provisions. To this end, the Act directs CISA to publish a notice of proposed rulemaking (NPRM) within 24 months of the statute's enactment and, subsequently, to issue a final rule within 18 months of publishing the NPRM. CISA's regulations will address:

— The Definition of Covered Entities. Covered entities must be in one of the 16 critical infrastructure sectors as defined in Presidential Policy Directive 21, which include 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 water and wastewater systems. CISA's regulations must adopt a definition of covered entities that includes some or all of the entities in these critical infrastructure sectors based on:

- "the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety";
- "the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country"; and
- "the extent to which damage, disruption, or unauthorized access to such an entity . . . will likely enable the disruption of the reliable operation of critical infrastructure."

— The Definition of Covered Cyber Incidents. The Act requires that the regulatory definition of

"covered cyber incidents" include "substantial cyber incidents" that, at a minimum: "lead[] to substantial loss of confidentiality, integrity, or availability of [an] information system or network, or a serious impact on the safety and resiliency of operational systems and processes"; cause "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 . . . an information system or network . . . [or] an operational technology system or process"; or involve "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." The definition will also consider the sophistication or novelty of the tactics used to perpetrate the cyber incident, the sensitivity of the data involved, the number of impacted individuals, and the potential impact on industrial control systems.

— The Contents of Cyber Incident Reports. The Act sets out baseline requirements for the contents of a covered entity's cyber incident report, which will be expanded upon by CISA rulemaking. The baseline requirements cover, where applicable:

- a description of the covered cyber incident, including the information systems, networks, or devices that were affected; the nature and estimated date range of the unauthorized access; and the impact to the entity's operations;
- a description of any vulnerabilities exploited and the cyber defenses that were in place, and the tactics, techniques, and procedures (TTPs) used to perpetrate the incident;
- any identifying information for the actor or actors believed to be responsible;
- the categories of information believed to have been accessed or acquired; and
- the name and contact information of the covered entity.

— The Contents of Ransom Payment Reports. For ransom payment reports, the baseline disclosure requirements of the Act cover, where applicable:

- a description of the ransomware attack, including the estimated date range;
- a description of the vulnerabilities and TTPs used to perpetrate the attack;
- any identifying information for the actor or actors believed to be responsible;
- the name and contact information of the covered entity that made the ransom payment or on whose behalf the payment was made;
- the ransom payment demand and instructions, including the type of virtual currency or other commodity requested, if any; and
- the date and amount of the ransom payment.

Voluntary Reporting of Other Cyber Incidents

The Act also encourages entities to voluntarily report to CISA cyber incidents or ransom payments that do not fall within the statutory and regulatory definitions, or additional information regarding reportable incidents that goes beyond any required content. Such voluntary reports will be provided the same level of protection as mandatory reports, as detailed below.

Noncompliance with Required Reporting

The Act authorizes CISA to engage directly with an entity the agency believes was required to submit a cyber incident report or a ransom payment report but failed to do so. If the entity does not respond to CISA's request for information within 72 hours, CISA is authorized to issue a subpoena to compel disclosure of the information necessary to determine whether a reportable incident occurred and to satisfy the reporting obligations under the Act and its implementing regulations.

The Act does not include specific fines or other penalties for noncompliance with the reporting requirements. However, if an entity fails to comply

with a CISA subpoena, CISA is authorized to refer the matter to the Department of Justice to bring a civil action to enforce the subpoena. Such failure to comply may be punishable as contempt as court.

Moreover, information obtained pursuant to a subpoena issued by CISA can be provided to the Justice Department or to other federal regulatory agencies for use in a regulatory enforcement action or criminal prosecution against the relevant covered entity concerning the cyber incident or ransom payment at issue. By contrast, information shared by covered entities in compliance with the statute's reporting requirements can only be used for limited cybersecurity purposes.

Information Shared with or Provided to the Federal Government

Importantly, the Act sets out various protections for the information submitted by covered entities to CISA. A cyber incident or ransom payment report summited pursuant to the statute is exempt from disclosure under the Freedom of Information Act and its state and local equivalents, and a report designated as commercial, financial, or proprietary information will retain that designation. In addition, submission of a report does not effect a waiver of any applicable legal privilege or protection, including trade secret protection.

The Act also contains liability protections that bar litigation based on the submission of a covered cyber incident report or ransom payment report to CISA, except for actions by the Justice Department to enforce compliance with a subpoena from CISA. Moreover, reports and work product created for the sole purpose of preparing a report may not be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court or regulatory body.

Other Provisions

— Cyber Incident Review. The Act directs CISA to "receive, aggregate, analyze, and secure" reports submitted by covered entities to, among other things:

- assess the effectiveness of security controls and identify TTPs used to overcome those controls;
- coordinate and share information with appropriate federal agencies to identify and track ransom payments, including those utilizing virtual currencies;
- enhance information sharing and coordination efforts with other governmental agencies, technology providers, critical infrastructure owners and operators, cybersecurity and cyber incident response firms, and security researchers;
- provide reports of cyber trends, threat indicators, and defensive measures; and
- identify and disseminate ways to prevent or mitigate future cyber incidents and ransomware attacks.

— Cyber Incident Reporting Council. The Act directs the Secretary of Homeland Security to lead an intergovernmental council in consultation with the Director of the Office of Management and Budget, the Attorney General, the National Cyber Director, Sector Risk Management Agencies, and other appropriate federal agencies "to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations."

— Ransomware Vulnerability Warning Pilot Program. The Act directs the Director of CISA to establish within one year a ransomware vulnerability warning pilot program, which is tasked with identifying common security vulnerabilities utilized in ransomware attacks and determining which information systems used by government agencies and private companies contain those security vulnerabilities. The Director is authorized to notify the owners or operators of any system identified to be vulnerable to ransomware attacks to support mitigation efforts.

— Joint Ransomware Task Force. The Act also directs the Director of CISA, in consultation with the National Cyber Director, the Attorney General, and the Director of the Federal Bureau of Investigation, to create a Joint Ransomware Task Force within six months "to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation." The Task Force will be made up of federal government employees, and is responsible for: consulting with private sector entities and state and local governments to identify ransomware-related needs and priorities; identifying a list of "highest threat ransomware entities" to facilitate investigative priorities; collecting and sharing analysis of ransomware trends; creating after-action reports and sharing lessons learned following a federal response to a ransomware attack; and "[d]isrupting ransomware criminal actors, associated infrastructure, and their finances."

Takeaways

The Cyber Incident Reporting for Critical Infrastructure Act is one of the federal government's strongest responses to date to the threat of malicious cyber activity. In addition to arming the federal government with tools to keep abreast of developing cyber threats, the legislation represents a significant expansion of the obligations for entities in critical infrastructure sectors to report cyber incidents. The increased urgency for cybersecurity reform prompted by the ongoing war between Russia and Ukraine, coupled with the growing number of ransomware attacks and cyber intrusions, greatly increased the speed by which the legislation passed the House and Senate and cleared the President's desk.

Now that the law is in place, companies in critical infrastructure sectors in particular should monitor developments with the rulemaking process and consider whether and to what extent they should participate through public comments or other advocacy. While the statute's reporting obligations will not take effect until the rulemaking process is completed, companies should begin to assess whether their cyber-related policies and procedures are adequate to meet the baseline requirements under the statute for incident response, analysis, and recordkeeping. They should also prepare to implement and maintain reporting policies and procedures that are designed to comply with the statute's short 72- and 24-hour timeframes for cyber incident and ransom payment reporting, respectively.

…

CLEARY GOTTLIEB