Cybersecurity and Information Security Newsletter

Issue 17 | April 13, 2022

Table of Contents

Daniel Shin, research scientist with the Commonwealth Cyber Initiative (CCI) Coastal Virginia region, wants to hear from you! Submit any cybersecurity and information security news items or request related topics via e-mail to dshin01@wm.edu.

This newsletter supports the mission of CCI. To learn more about CCI, including upcoming events, funded research, and news, please visit cyberinitiative.org.

Cyber Incident Reporting for Critical Infrastructure Act of 2022 signed into law

On March 15, 2022, President Biden signed the *Consolidated Appropriations Act, 2022*, in order to fund the federal government through the current fiscal year. *Bill Signed: H.R. 2471*, available here. Various non-budgetary matters are included in the legislation, which became law after the President's signing. Critically, this includes the *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (Cyber Incident Reporting Act), which expands the federal government's role in the nation's critical cybersecurity infrastructure. *H.R.2471 - Consolidated Appropriations Act, 2022, under Division Y--Cyber Incident Reporting for Critical Infrastructure Act of 2022*, available here. Specifically, the Act seeks to improve cyber threat information sharing by requiring covered entities to disclose cyber incident and ransom payment reports to the Cybersecurity and Infrastructure Security Agency (CISA).

Legislative History

In the past few years, members of the U.S. Senate introduced various proposals focusing on mandatory cyber incident reporting requirements for critical infrastructure operators. The Cyber Incident Reporting Act is the culmination of these legislative efforts to harden cyber defenses across the national critical infrastructure while encouraging cyber threat information sharing among private and public entities.

For example, on July 21, 2021, U.S. Senator Mark Warner of Virginia introduced the *Cyber Incident Reporting Act of 2021* that would have mandated certain cyber breach notifications by federal agencies, federal contractors, and critical infrastructure operators. *Issue 10: CLCT Cybersecurity and Information Security Newsletter - Senator Warner introduced legislation to bolster cyber breach notification*, available here. At present, that bill has been referred to the U.S. Senate Committee on Homeland Security and Government Affairs. *All Actions: S.2407 - Cyber Incident Notification Act of 2021*, available here.

Subsequently, on March 1, 2022, the U.S. Senate passed a separate bill, the *Strengthening American Cybersecurity Act of 2022*, which was introduced by Senator Gary C. Peters of Michigan. *S.3600 - Strengthening American Cybersecurity Act of 2022*, available here. The legislation contains three acts: the *Federal Information Security Modernization Act of 2022*, the *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, and the *Federal Secure Cloud Improvement and Jobs Act of 2022*. The bill addressed cybersecurity threats targeting the federal government and critical infrastructure operators. The *Federal Information Security Modernization Act of 2022* proposed to improve cybersecurity incident response among federal agencies by giving the CISA a central role of providing resources and expertise to mitigate future incidents. The *Cyber Incident Reporting for Critical Infrastructure Act of 2022* mandated disclosure of certain cyber incidents and ransom payments by critical infrastructure operators. Finally, the *Federal Secure Cloud Improvement and Jobs Act of 2022* facilitated the process of acquiring and using securely cloud-computing products and services for the federal government. The U.S. House of Representatives has not passed a similar bill.

The *Consolidated Appropriations Act, 2022*, was originally introduced by Representative Hakeem S. Jeffries of New York's 8th congressional district as the *Haiti Development, Accountability, and Institutional Transparency Initiative Act*, which revised the reporting and strategy requirements related to the U.S. recovery and assistance efforts for Haiti. The Haiti

bill was passed in the U.S. House of Representatives on June 29, 2021, and the U.S. Senate on January 13, 2022. *Actions Overview H.R.2471 — 117th Congress (2021-2022)*, available here. In March, both houses of Congress changed the original Haiti bill into a budget bill by amending it to include federal budgetary matters. *See House agreed to Senate amendment (03/09/2022)*, available here; *Senate agreed to House amendment (03/10/2022)*, available here. Both houses of Congress also agreed to attach non-budgetary items to the bill as divisions, and the Cyber Incident Reporting Act was incorporated into Division Y of the bill. After President Biden signed the *Consolidated Appropriations Act, 2022*, the Cyber Incident Reporting Act became public law.

The Cyber Incident Reporting Act contains similar provisions to Senator Warner's *Cyber Incident Reporting Act of 2021* and the *Cyber Incident Reporting for Critical Infrastructure Act of 2022* from Senator Peters' bill. Both previous cyber incident bills garnered strong bipartisan support at the U.S. Senate. *See STRENGTHENING AMERICAN CYBERSECURITY ACT OF 2022; Congressional Record Vol. 168, No. 37 (Senate - March 01, 2022)*, available here; *see Cosponsors: S.2407 — 117th Congress (2021-2022)*, available here.

Key Statutory Definitions

The Cyber Incident Reporting Act defines "covered entity" as an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that will be set forth after the Director of CISA promulgates relevant regulations pursuant to the Act. *Consolidated Appropriations Act, 2022, H.R.2471, 117th Cong. (2022)* at 991, available here. Based on Presidential Policy Directive 21, covered entities will include both public and private owners and operators of critical infrastructure in 16 sectors, including: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems. *Presidential Policy Directive -- Critical Infrastructure Security and Resilience*, available here.

The Cyber Incident Reporting Act defines cyber incidents as an actual or imminent occurrence that unlawfully jeopardizes the integrity, confidentiality, or availability of information in an information system, or an actual or imminent occurrence that unlawfully jeopardizes an information system. *Id.*; 6 U.S.C. § 659(a)(5), available here. A significant cyber incident (Covered Cyber Incident) refers to a cyber incident that the Secretary of Homeland Security determines to harm the national interests, foreign relations, the national economy, the confidence of the economy, civil liberties, or public health and public safety of people in the U.S. *Consolidated Appropriations Act, 2022, H.R.2471* at 992, *supra*.

The Act defines "ransomware attack" as an act that includes the use or *threat of use* of unauthorized or malicious code on an information system, or the use or *threat of use* of another digital mechanism, such as a denial of service attack. *Id.* This definition is more expansive than a cyber attack simply involving ransomware as it covers a wide range of incidents involving any unauthorized use or any use of malicious code in an information system that disrupts normal operations. Furthermore, this definition also includes the *threat of use* of unauthorized use or use of malicious code, which means that actual disruption of information systems is not a necessary component of the ransomware attack.

Finally, a "supply chain compromise" refers to an incident within the supply chain of an information system that a threat actor can jeopardize or does jeopardize the "confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle." *Id.* Similar to the ransomware attack definition, this definition includes both the actual act and the potential act of a supply chain compromise.

Responsibilities of the National Cybersecurity & Communications Center

Under the Cyber Incident Reporting Act, the National Cybersecurity & Communications Integration Center (NCCIC) of CISA will take on additional responsibilities in gathering and analyzing cyber incident reports from covered entities to assess the current security measures against threat actors. *Id.* at 992-94. The Act also requires the NCCIC to coordinate with other federal departments and agencies to identify and track ransom payments, including those transmitted through virtual currencies (e.g., cryptocurrencies).

Covered Entities Requirements

The Cyber Incident Reporting Act imposes certain requirements on a covered entity impacted by a Covered Cyber Incident, including:

(1) disclosing Covered Cyber Incidents to CISA within 72 hours of incident discovery,
(2) disclosing any ransom payments as a result of a ransomware attack to CISA within 24 hours after the payment has been made,
(3) disclosing promptly any updates of any ongoing Covered Cyber Incident or ransomware payment to CISA until the matter is resolved, and
(4) preserving information that is relevant to a Covered Cyber Incident or ransom payment. *Id.* at 994-96.

With respect to ransomware payments, the Act allows a covered entity to use a third party (e.g., incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm) to make a ransom payment on behalf of the entity. *Id.* at 1000. By acting on behalf of the covered entity, the third party undertakes new legal requirements under the Act, including advising the covered entity of the ransom payment reporting requirements to CISA.

If the Director of CISA believes that a covered entity has encountered a Covered Cyber Incident or made a ransom payment as a result of an attack but failed to disclose it to the Agency, the Cyber Incident Reporting Act allows the Director to directly request the covered entity to supply information. *Id.* at 1001-02. If the covered entity does not respond to the Director's initial inquiry within 72 hours, the Director is empowered to issue a subpoena (a legal written order to compel an individual or organization to give testimony on a particular issue) to legally force the covered entity to disclose relevant information. The Director may ask the U.S. Attorney General to enforce the subpoena in a U.S. district court, and the court may punish the non-complying covered entity by finding it in contempt of court. *See 18 U.S. Code § 402*, available here. Except for punishment arising out of contempt of court, the Act does not provide any further punitive enforcement mechanisms for the covered entity's failure to disclose Covered Cyber Incidents or ransom payments.

Finally, the Cyber Incident Reporting Act explicitly excludes the Internet Corporation for Assigned Names and Numbers (ICANN) (a not-for-profit public-benefit corporation that is responsible for determining how the domain name system functions) and the Internet Assigned Numbers Authority (IANA) (the organization responsible for allocating and managing unique codes and numbering systems that impact domain names, IP addresses, and certain internet protocols) from the cyber incident reporting requirements. *Consolidated Appropriations Act, 2022, H.R.2471* at 996. This exclusion ensures that the global multi-stakeholders' interests of both organizations are not affected by the Act's regulations.

Analysis

On May 7, 2021, the Colonial Pipeline company was forced to shut down its pipeline system after suffering a ransomware attack. *Colonial Pipeline Cyber Incident*, available here. As a result, the White House implemented a series of federal responses to mitigate gasoline shortages and enhance cybersecurity for the nation's critical infrastructure. *FACT SHEET: The Biden-Harris Administration Has Launched an All-of-Government Effort to Address Colonial Pipeline Incident*, available here. In an attempt to resolve the situation, Colonial Pipeline reportedly paid nearly $5 million in ransom to get the decryption key to unlock its systems, even though such practice was discouraged by federal law enforcement. *See Issue 8: CLCT Cybersecurity and Information Security Newsletter - The Ransomware Task Force issues a comprehensive strategic framework against ransomware*, available here. The Colonial Pipeline ransomware attack demonstrated the real potential of ransomware causing enormous disruptions to the nation's infrastructure.

The Cyber Incident Reporting Act balances the need for the federal government to monitor the cyber threat landscape of the nation's critical infrastructure and the burden of critical infrastructure operators to report sensitive cyber incidents and ransom payments through an administrative process. The Act clearly states the federal government's national security interest in gathering cyber threat intelligence across the nation's infrastructure.

At the same time, this law does not impose automatic criminal penalties for non-compliant covered entities. It requires the Director of CISA to contact the non-compliant covered entity to direct it to produce the required cyber incident and ransom payment reporting. Despite the Director's demand for information, if the covered entity fails to respond or fails to produce an adequate report, the Act provides the Director to issue a subpoena to compel information disclosure. The non-compliant covered entity would have the benefit of a judicial review before penalties are imposed through a contempt of court charge.

If the Cyber Incident Reporting Act were in effect during the Colonial Pipeline ransomware attack, Colonial Pipeline would have been required to alert CISA within 72 hours of the ransomware attack discovery (whether the company actually alerted CISA within 72 hours is not clear). During the cyber incident recovery phase, Colonial Pipeline would have had to provide continuous up-to-date information to the Agency until the situation was resolved. From the federal government's perspective, CISA would have taken the lead to coordinate with other agencies on how to resolve the current situation (including determining whether other critical infrastructure operator's IT systems were at risk of a similar attack), and it would have informed leadership in U.S. Congress on the latest development on the cyber attack recovery efforts.

Although a first glance may suggest that this Act only focuses on ransomware, its definition of a "ransomware attack" is written broadly enough to cover not only a wide range of malicious code but also scenarios where the *threat* of disruptions caused by a cyber attack constitutes a ransomware attack. The definition focuses on digital mechanisms that "*interrupt* or *disrupt* the operations of an information system or *compromise the confidentiality*, *availability*, or *integrity* of *electronic data* stored on, processed by, or transiting an information system to extort a demand for ransom payment." *Consolidated Appropriations Act, 2022, H.R.2471* at 992 (emphasis added). Any malicious attack or the threat of an attack that can interrupt or disrupt an information system or data within fits the definition of a ransomware attack as long as there is an accompanying demand for a ransom payment.

This would mean that any form of a denial of service or a data breach attack could be considered as a ransomware attack under the Act, as long as the threat actor demands ransom to the victim critical infrastructure operator. Also, a legitimate threat of an attack with a demand for ransom would be considered a ransomware attack under the Act, *despite the absence* of a realized cyber attack.

The key result of the new broad definition of a ransomware attack is that covered entities must report all ransom payments to CISA regardless of whether a cyber attack was commenced. This may discourage covered entities from paying ransom due to the ransom payment reporting requirements from the Act. By requiring ransom payments disclosures, entities may incur reputational harm due to their perceived inability to resolve a cyber attack without having to pay ransom to threat actors. Covered entities will likely respond to this provision of the law by hardening their cybersecurity defense to be resilient against ransom demands.

Although the Cyber Incident Reporting Act has a narrower focus than Senator Peters' *Strengthening American Cybersecurity Act of 2022*, it nevertheless provides streamlined mechanisms for critical infrastructure operators to provide cyber incident intelligence to CISA, which has a *non-law enforcement* approach to strengthening the nation's cybersecurity landscape. By improving the nation's cyber threat visibility, CISA can provide a more effective and coordinated response to mitigate ongoing cyber attacks targeting our critical infrastructure.