CALL TO ACTION

FOR CRITICAL INFRASTRUCTURE BUSINESSES –

NEW FEDERAL CYBER BREACH REPORTING OBLIGATIONS AND RANSOMWARE PREVENTION STRATEGIES

BY SARAH CRONAN SPURLOCK

"Shields Up" is the name given to the U.S. Cybersecurity & Infrastructure Security Agency's latest educational campaign to encourage businesses across the United States to harden their cyber defenses and better prepare to respond when attacks occur. While security breach reporting obligations have existed under a variety of state and federal laws for years, those reporting obligations are largely concerned with information compromised in a security breach that may place individuals at risk of fraud or identity theft.[1] Historically, the potential for a cyber incident to disrupt business operations has not been part of a business's reporting obligations. That is, until March 2022 and the passage of the new federal cyber incident reporting law titled the "Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA" or the "Act")."[2]

The Act signifies a shift in cyber incident reporting obligations to now include cyber incidents that have the potential to disrupt critical infrastructure operations in the United States. CIRCIA requires reporting and other actions to protect the infrastructure from cybersecurity incidents and ransomware attacks.[3] A primary catalyst for this new law is recognition that disabling or destroying the economic sectors identified in the Act, including energy, food, healthcare, and information technology, would cause great harm to security, economic welfare, public health, and safety in the United States.[4] Once the Act's reporting obligations become effective, businesses in the critical sectors must report certain cyber incidents within 72 hours and, in the case of a ransom payment, as little as 24 hours.[5]

This article provides an overview of compliance obligations and key terms, identifies impacted sectors, outlines reporting obligations, and provides information on additional rulemaking and compliance deadlines. In addition, while the Act's reporting obligations will not take effect for some time, the risk of cyberattacks to businesses exists today. Though additional sector-specific guidance is under development, the Cybersecurity & Infrastructure Security Agency ("CISA") has published general resources and guidance that businesses should consider implementing now to decrease risk and minimize the impact of cyberattacks.[6]

OVERVIEW - CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

Under CIRCIA, cyber incident and ransom payment reporting requirements apply to "covered entities" in the 16 critical infrastructure sectors defined in Presidential Policy Directive 21 ("PPD-21).[7] The sectors are: 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.[8]

Notably, under the Act, the term "covered entity" is defined generally as "an entity in a critical infrastructure sector…that satisfies the definition and criteria established by the Director in the final rule issued" pursuant to the Act.[9] Given this definition, we expect the covered entities within the identified sectors to be clarified by criteria included in future regulations. In identifying additional criteria, CISA will likely consider those businesses and critical infrastructure entities that, if disrupted or taken offline by a cyber incident, have greater potential to disrupt other critical U.S. operations such as national security, public health, and transportation.[10]

REPORTING OBLIGATIONS

CIRCIA includes two main reporting obligations. One for covered cyber incidents and another for ransom payments made following a ransomware attack.[11] Each of these reporting obligations, discussed briefly below, will be subject to supplemental reporting obligations in certain instances.[12] In addition to required reporting obligations, covered entities may voluntarily report other cyber incidents or ransom payments to CISA[13]

REPORTING COVERED CYBER INCIDENTS

CIRCIA's covered incident reporting obligation requires covered entities to report covered cyber incidents to CISA within 72 hours after the entity reasonably believes a covered cyber incident has occurred.[14] The Act does not specifically define covered cyber incidents, or what constitutes a "reasonable belief" that one has occurred for purposes of the reporting obligation. Generally, a "covered cyber incident" is a "substantial cyber incident" experienced by the entity that "satisfies the definition and criteria established by the Director in the final rule issued pursuant to" the Act.[15] As such, covered entities will need to look to the final rule for clarity on what types of cyber incidents and attacks will require a report.

Future rulemaking may also clarify CIRCIA's timing requirement—when the 72-hour clock begins for purposes of compliance with the law—as part of a final rule. Absent such clarity, however, covered entities may consider looking to existing breach notification laws as a point of reference. For example, under HIPAA's breach reporting law (generally applicable within the healthcare industry), the relevant breach reporting timeframe begins on the day a breach is "known to the [HIPAA] covered entity, or, by exercising reasonable diligence would have been known."[16] The reference to "reasonable diligence" under HIPAA implies an obligation to investigate suspicious activity to confirm whether a reportable breach has occurred rather than relying on a strict knowledge requirement. If CIRCIA adopted or implied a similar standard in a final rule, covered entities in critical infrastructure sectors would be required to implement procedures to monitor for and investigate suspicious activity that may lead to discovery of a reportable covered incident. Reference to other laws for compliance with CIRCIA is, of course, purely speculative at this time. Covered entities should consult the final rule and CIRCIA's implementing regulations to confirm the precise contours of CIRCIA's covered incident reporting obligation. Because it may be years before the release of the final rule, for now the exact parameters of CIRCIA's reporting obligations remain undefined.

REPORTING RANSOM PAYMENTS

The second type of reporting obligation under the Act requires

a covered entity that makes a ransom payment as the result of a ransomware attack to "report the payment to [CISA] not later than 24 hours after the ransom payment has been made."[17] CIRCIA defines a ransomware attack as:

> an incident 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 denial of service attack, to 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 a ransom payment.[18]

The definition of ransomware under CIRCIA does not include "any such event where the demand for payment is…(i) not genuine… [or] (ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system."[19] A "ransom payment" is defined as "the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack."[20] Importantly, the obligation to report a ransom payment exists whether or not the ransomware attack fits the definition of a covered cyber incident.[21] As such, covered entities will need to have procedures in place to ensure accurate and timely reporting in each instance. As with the general reporting obligation, the ransom payment reporting obligation will be developed and clarified through CISA's future rulemaking.[22]

COVERED CYBER INCIDENT REPORT CONTENT

While cyber incident report content requirements are subject to CISA rulemaking, the Act establishes certain minimum content requirements,[23] including (if applicable and available), the following:

- A description of the covered cyber incident, including the description of the unauthorized access and estimated date range;
- The function of the affected information system, network, or device affected;
- The impact to the operations of the covered entity;
- A description of the vulnerabilities exploited and security defenses in place, as well as the tactics, techniques, and procedures used in the incident;
- Identifying or contact information for actor(s) reasonably believed to be responsible;
- Category(ies) of information wrongfully accessed or acquired;
- Identification of the impacted covered entity, including legal and trade name and state of incorporation or formation; and
- Contact information (*i.e.,* telephone number or electronic address) for CISA to contact the covered entity (or an authorized agent or the service provider assisting the entity with the Act's compliance requirements).[24]

Additionally, in the event of substantial new or different information, or if the covered entity makes a ransom payment after submitting the report, an updated or supplemental report is required.[25] Supplemental reports are required until the covered entity notifies CISA that the incident at issue "has concluded and has been fully mitigated and resolved."[26] Covered entities must also preserve data relevant to the covered cyber incident in accordance with procedures that will be established in the final rule.[27]

RANSOM PAYMENT REPORT CONTENT

As with the covered cyber incident reporting obligations, the specifics of ransom payment reports are subject to further rulemaking by CISA.[28] Again, the Act specifies certain minimum reporting content for ransomware payment reports, including:

- A description of the ransomware attack, including estimated date range;
- The vulnerabilities, tactics, techniques, and procedures used in the ransomware attack;
- Identifying or contact information related to the actor(s) reasonably believed to be responsible;
- Name and other information identifying the covered entity that made the ransom payment or on whose behalf the payment was made;
- Contact information (i.e., telephone number or electronic mail address) that CISA may use to contact the covered entity (or an authorized agent or the service provider assisting the entity with the Act's compliance requirements).
- The ransom payment demand, including the type of virtual currency or other commodity requested;
- The ransom payment instructions, including information regarding where to send the payment (i.e., the virtual currency address or physical address the funds were requested to be sent to); and,
- The date and amount of the ransom payment.[29]

Ransom payment reports must also be supplemented if substantial new or different information becomes available after the initial report and until such time as the covered entity notifies CISA that the covered cyber incident at issue has concluded and has been fully mitigated and resolved.[30] Additionally, a covered entity must preserve data relevant to the ransom payment in accordance with procedures established in the final rule.[31]

Notably, a covered entity may submit a single report to comply with reporting requirements for both a covered cyber incident and a ransom payment if the entity is a victim of a covered cyber incident and makes a ransom payment prior to the 72-hour reporting

requirement.[32] Single reports of this nature will need to comply with procedures established in the final rule issued by the CISA Director.[33]

CIRCIA REPORTING EXCEPTIONS

Exceptions to CIRCIA's reporting obligations will apply in limited circumstances. For example, the Act provides that CIRCIA's reporting requirements "shall not apply to a covered entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar time frame."[34] This exception, however, will only take effect "once an agency agreement and sharing mechanism is in place between [CISA] and the respective Federal agency."[35] This exception may be of particular interest to organizations that fall within a critical infrastructure sector that is already subject to federal breach reporting obligations, such as certain health care entities regulated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Notably, however, the timeframe to report a breach to the relevant federal agency under HIPAA ranges from 60 calendar days to 14 months depending on how many individuals are impacted by the breach and the calendar month in which the breach occurs.[36] Meaning, under any circumstance, the current time to report under HIPAA is substantially longer than the 72-hour timeframe that will be required for compliance with CIRCIA, raising a question as to whether an agency agreement will be possible for existing reporting laws like HIPAA that afford significantly longer reporting timeframes than CIRCIA.[37] As such, until appropriate agency agreements are established, those entities already under an obligation to report security breaches to a federal regulator should assume that CIRCIA will create a new, distinct reporting obligation to CISA when a covered cyber incident or ransom payment occurs.

In addition, CIRCIA's reporting requirements will not apply to certain entities concerning "the Domain Name System," which include "the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority."[38]

NONCOMPLIANCE WITH REQUIRED REPORTING OBLIGATIONS

In the event of reporting noncompliance, CISA may engage a covered entity directly to inquire about a cyber incident or ransom payment.[39] If no response is received within 72 hours, CISA may issue a subpoena to compel disclosure.[40] The Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena.[41] And, a covered entity failing to comply with a subpoena may be held in contempt of court.[42]

CISA INFORMATION SHARING

CIRCIA requires CISA to share reports received from covered entities with the appropriate Sector Risk Management Agency (SRMA) within 24 hours.[43] These agencies include, for example, U.S. Departments of Homeland Security, Energy, Defense, and Transportation.[44] Further, CIRCIA allows CISA to share reported information with other federal agencies for specific, limited purposes, including identifying cyber threats and their sources, investigating and prosecuting offenses arising out CIRCIA reporting noncompliance, and responding to, preventing, and mitigating specific threats in the nature of: serious economic harm; terrorist acts; use of weapons of mass destruction; and, sexual exploitation and physical threats to minors.[45] Upon receipt of a cyber incident or ransom payment report, CISA is required to review the information to determine if it is a part of an ongoing threat or vulnerability and use the report "to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures."[46]

Both the information shared with CISA in the context of a required report, and the information sharing required or permitted under CIRCIA among federal agencies, raise potential concerns for reporting covered entities with respect to issues such as waiver of privilege, discovery of reported information in potential litigation, and the possibility that sensitive security information could be accessible or vulnerable to unauthorized access or disclosure. CIRCIA addresses some of these concerns by affording certain protections to reports made under the Act.[47] These protections include:[48]

- Security for reports and reported information that, at a minimum, meets requirements for Federal Information Systems.
- Prohibitions on state and federal agencies' use of information contained in CIRCIA reports for regulatory and enforcement activities, unless the agency expressly allows the entity to submit reports to CISA to meet regulatory reporting obligations of the entity.
- Protection for reports as commercial, financial, and proprietary information of the covered entity when so designated by the covered entity.
- Exemption from Freedom of Information Act (FOIA) disclosures, as well as other similar laws requiring disclosure of information or records.
- Non-waiver of any applicable privilege or protection provided by law, including trade secret protections.
- Excluding reports from a rule of any federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.
- Specifying that reports submitted to CISA (and any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting a report pursuant to CIRCIA) may not be received into evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceedings.
- Anonymization of the reporting victim when sharing reports and information with critical infrastructure owners and operators and the general public.

EFFECTIVE DATE AND FUTURE RULEMAKING

CIRCIA's reporting requirements will not be effective until implemented as part of the future rulemaking required under the Act.[49] The Director must publish a notice of proposed rulemaking within 24 months of CIRCIA's March 2022 enactment.[50] And, not later than 18 months after publication of that notice of proposed rulemaking, the Director must issue a final rule.[51] Effective dates for the required reporting obligations will be prescribed in the final rule.[52]

PREPARATION, PREVENTION, AND RISK MITIGATION

Even though compliance plans will need to be supplemented and informed through future rulemaking and development of the required regulations, organizations in the critical infrastructure sectors should begin considering procedures necessary to comply with CIRCIA's reporting obligations. And, while taking steps to prepare for compliance is prudent, increasing cyber defenses to avoid or lessen the risks of an incident occurring in the first place is of vital importance. Taking steps to prevent a cyber incident will not only reduce the possibility of operational disruptions in critical industries, but will also save an organization the time and resources required to respond and recover, and may also eliminate the need for compliance with CIRCIA reporting obligations altogether.

A May 2021 Executive Order on "Improving the Nation's Cybersecurity" recognized the need to make "prevention, detection, assessment, and remediation of cyber incidents" a top priority across the federal government declaring that Federal Information Systems should meet or exceed the cybersecurity standards and requirements issued pursuant to the order.[53] Shortly thereafter, recognizing the increasing threat of ransomware to businesses in the private sector, the Biden administration issued an open letter to corporate executives and business leaders calling for action to combat the ransomware threat.[54] The letter urged businesses to implement "five best practices" to reduce the risk of a ransomware attack, including: (1) use of multifactor authentication; (2) endpoint detection and response; (3) encryption; (4) a skilled security team; and, (5) sharing and incorporating threat information into defense strategies.[55] In addition to implementing the five best practices outlined above, the letter urged businesses to take the following actions:[56]

- Regularly test backups and maintain them offline to minimize the risk of certain ransomware;
- Update and patch systems promptly to maintain security;
- Test incident response plans and improve response processes;

- Utilize third party penetration testing for system security;
- Segment networks to separate functions and limit access to operational networks and sensitive information; and,
- Test contingency plans to confirm operations can continue during a cyber incident.

The letter also provides information on additional best practice resources available from CISA via its website "StopRansomware.gov" which includes a ransomware resources and a response checklist.[57] The site also includes a risk management page identifying the designated Sector Risk Management Agency (or SRMA) for each critical infrastructure sector.[58] CISA indicates sector-specific guidance will be added to its website when available and recommends that businesses act now to implement the general guidance currently available.[59] B&B

ABOUT THE AUTHOR

SARAH CRONAN SPURLOCK is a member of Stites & Harbison, PLLC, where she practices in the areas of privacy & data security and health care regulatory law. Spurlock regularly advises clients on a wide range of health care and privacy matters, including compliance with information privacy and security laws, data breach prevention and response, fraud and abuse laws, and physician and hospital contracting. She holds the Certified Information Privacy Professional (CIPP/US) credential from the International Association of Privacy Professionals. Her practice focuses on compliance, regulatory, and transactional matters.

ENDNOTES

1 For example, security breach notification laws exist in all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands. See generally, National Conference for State Legislatures overview at https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited August 12, 2022).

2 For example, security breach notification laws exist in all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands. *See generally,* National Conference for State Legislatures overview at https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited August 12, 2022).
Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 116th Cong., Public Law No: 117-103, (March 15, 2022).

3 *Id.*

4 *See* resources available via the official government website Stop Ransomware.gov available at https://www.cisa.gov/stopransomware/resources (last visited August 15, 2022).

5 *See* H.R. 2471 §2242(a)(1) and H.R. 2471 §2242(a)(2)(A).

6 *See* discussion of ransomware prevention and response resources *infra.*

7 H.R. 2471 §2240(5).

8 Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience, DCPD-201300092 (Feb. 12, 2013). PPD-21 is available at https://www.energy.gov/ceser/presidential-policy-directive-21 (last visited August 15, 2022).

9 H.R. 2471 §2240(5). "Director" refers to the Director of the Cybersecurity and Infrastructure Security Agency (CISA). H.R. 2471 §102(2).

10 *E.g.* The Colonial Pipeline attack: *See Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. Times, (May 8, 2021), www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

11 H.R. 2471 §2242(a)(1) and (2).

12 H.R. 2471 §2242(a)(3).

13 H.R. 2471 §2243(a).

14 H.R. 2471 §2242(a)(1).

15 H.R. 2471 §2240(4).

16 *See* HIPAA's Breach Notification Rule, Notification to Individuals at 45 CFR 164.404(a)(2).

17 H.R. 2471 §2242(a)(2)(A).

18 Definition set forth at H.R. 2741 §2240(14). In more general terms, the CISA's website dedicated to ransomware resources describes ransomware as "a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable, [where malicious actors] then demand ransom in exchange for decryption." *See* description at "StopRansomware.gov" available at https://www.cisa.gov/stopransomware (last visited August 15, 2022).

19 H.R. 2471 §2240(14).

20 H.R. 2471 §2240(13).

21 *See* H.R. 2471 §2242(a)(2)(B) (The reporting requirement applies even if the ransomware attack is not a covered cyber incident subject to the reporting requirements for a covered cyber incident).

22 H.R. 2471 §2242(a)(5).

23 H.R. 2471 §2242(c)(4).

24 *Id.*

25 H.R. 2471 §2242(a)(3).

26 *Id.*

27 H.R. 2471 §2242(a)(4).

28 H.R. 2471 §2242(c)(5).

29 H.R. 2471 §2242(c)(5).

30 H.R. 2471 §2242(a)(3).

31 H.R. 2471 at §2242(a)(4).

32 H.R. 2471 §2242(a)(5)(A).

33 *Id.*

34 H.R. 2471 §2242(a)(5)(B)(i).

35 H.R. 2471 §2242(a)(5)(B)(ii).

36 The HIPAA Breach Notification Rule, found at 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

37 If a HIPAA-covered breach affects 500 or more individuals, HIPAA requires covered entities to notify the Secretary of The U.S. Department of Health and Human Services, Office for Civil Rights without unreasonable delay and in no case later than 60 days following a breach. If, however, fewer than 500 individuals are affected, notification is due to the Secretary no later than 60 days after the end of the calendar year in which the breach is discovered. *See* 45 CFR §164.408.

38 H.R. 2471 §2242(a)(5)(C).

39 H.R. 2471 §2244(a).

40 H.R. 2471 §2244(c)(1).

41 H.R. 2471 §2244(c)(2).

42 H.R. 2471 §2244(c)(2)(C).

43 H.R. 2471 §2241(a)(10).

44 The list of Sector Risk Management Agencies for each of the 16 critical infrastructure sectors is available at https://www.cisa.gov/stopransomware/sector-risk-management-agencies (last visited August 15, 2022).

45 H.R. 2471 §2245(a).

46 H.R. 2471 §2245(a)(2)(A).

47 H.R. 2471 §2245(a)(4)-(5), and §§ (b)-(d).

48 *Id.*

49 H.R. 2471 §2242(a)(7).

50 H.R. 2471 §2242(b).

51 H.R. 2471 §2242(b).

52 H.R. 2471 §2242(a)(7).

53 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (last visited August 12, 2022).

54 June 2, 2021, Open Letter from White House deputy national security adviser for cyber and emerging technology, Anne Neuberger, available at https://image.connect.hhs.gov/lib/fe3915707564047b761078/m/1/8eeab615-15a3-4bc8-8054-81bc23a181a4.pdf (last visited August 12, 2022).

55 *Id.*

56 *Id.*

57 The Ransomware Response Checklist is available at https://www.cisa.gov/stopransomware/ive-been-hit-ransomware and the Ransomware Guide is available at https://www.cisa.gov/stopransomware/ransomware-guide.

58 The list of Sector Risk Management Agencies for each of the 16 critical infrastructure sectors is available at https://www.cisa.gov/stopransomware/sector-risk-management-agencies (last visited August 15, 2022).

59 *See* resources are available at https://www.cisa.gov/stopransomware/resources (last visited August 15, 2022).