SULLIVAN & CROMWELL LLP

S&C memo

March 22, 2022

# Federal Legislation Requires Cyber Incident Reporting for Critical Infrastructure Sector

## Implementing Rule Will Require Reporting to CISA of Covered Cybersecurity Incidents and Ransomware Payments by Subsectors That Are Likely to Include Financial Services, Communications, Energy and Others

### SUMMARY

On March 15, 2022, President Biden signed into law the Strengthening American Cybersecurity Act of 2022 (the "Act"), requiring entities in the critical infrastructure sector to report both covered cyber incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency ("CISA").[1] First, the Act requires an entity in the critical infrastructure sector—which will likely encompass subsectors such as financial services, energy, communications, defense industrial base, and food and agriculture, among others—that experiences a "covered cyber incident" to report the incident to CISA no later than 72 hours after the entity reasonably believes the incident has occurred.[2] Second, a critical infrastructure entity that makes a ransom payment as a result of a ransomware attack must report the payment to CISA within 24 hours of making the ransom payment.[3]

The CISA Director (the "Director") will implement the Act through a final rule defining "covered entities" and "covered cyber incidents" and determining the manner and form of required reports.[4] In consultation with other federal agencies, the Director must publish a notice of proposed rulemaking for the final rule within 24 months, and must then issue the final rule within 18 months of the notice of proposed rulemaking.[5]

## BACKGROUND

The Act's passage aligns with recent efforts by the federal government to strengthen U.S. cybersecurity, and similar provisions had been proposed last year, though they were ultimately omitted as an amendment to the 2022 National Defense Authorization Act.[6] In May 2021, President Biden issued an Executive Order aimed at improving the nation's ability to protect against and respond to malicious cyber activity, including through mandates for cybersecurity information-sharing among government service providers.[7] In the months since, numerous federal regulators have issued cybersecurity standards and reporting requirements. For example, in November 2021, federal banking agencies issued a final rule requiring banking organizations to notify their primary federal regulators of certain computer-security incidents within 36 hours.[8] And on March 9, 2022, the Securities and Exchange Commission issued a proposed rule that would require registrants to publicly disclose material cybersecurity incidents within four days.[9] Other initiatives include guidance from the Treasury's Financial Crimes Enforcement Network for reporting of ransomware attacks;[10] and guidance from the Treasury's Office of Foreign Assets Control incentivizing maintenance of adequate cybersecurity programs, reporting of ransom payments, and cooperation with law enforcement during and after a ransomware attack.[11] The Act represents an additional measure to address cybersecurity risks and increase reporting amid growing awareness of the threats posed by cybersecurity attacks for U.S. public and private sectors, heightened by Russia's invasion of Ukraine and its potential impact on U.S. national security.

## THE ACT

### Covered Entities

The Act creates reporting requirements for "covered entities," which are entities "in a critical infrastructure sector" that also satisfy a definition established in the final rule to be promulgated under the Act.[12] The Act adopts the "critical infrastructure sector" definition in Presidential Policy Directive 21, which defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[13] The Directive identifies 16 subsectors, including financial services, energy, communications, defense industrial base, and food and agriculture, that comprise the critical infrastructure sector.[14] When promulgating the final rule to determine which entities that fall under this definition of "critical infrastructure sector" qualify as "covered entities," the Director must also consider the consequences of disruption to national security, economic security, or public health and safety; the likelihood of the entity being targeted by malicious cyber actors, including foreign countries; and the extent to which damage, disruption, or unauthorized access would disrupt the reliable operation of that critical infrastructure.[15]

Based on these considerations and the broad definition of critical infrastructure under Presidential Policy Directive 21, it is reasonable to assume that large entities in financial services, energy, communications, defense, and food and agriculture, among other subsectors, will be considered "covered entities" under the final rule, an approach consistent with CISA's definition of critical infrastructure.[16]

### Reporting Requirements

***Reporting of Cyber Incidents.*** Under the Act, covered entities that experience a covered cyber incident must "report the covered cyber incident to [CISA] not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred."[17] The Act leaves the exact meaning of "covered cyber incident" to be determined by the final rule, while providing that the term must, at a minimum, include the following types of events:

- A cyber incident that leads 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;[18]
- A disruption of business or industrial operations, including due to an attack or exploitation against an information system, network, or operational technology system or process;[19] or
- Unauthorized access or disruption of business or industrial operations due to compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or due to a supply chain compromise.[20]

The report submitted to CISA must include a description of the covered cyber incident, and, where applicable, "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."[21]

***Reporting of Ransom Payments.*** Additionally, the Act requires that a covered entity that makes a payment as a result of a ransomware attack report that payment to CISA within 24 hours after it has done so.[22] "Ransomware attack" is defined to include not only deploying malicious computer code to encrypt the contents of digital devices or systems, but also the use or threatened us of other "digital mechanism[s]" like a denial-of-service attack "to interrupt or disrupt the operations of an information system" or to "compromise the confidentiality, availability, or integrity of electronic data . . . to extort a demand for a ransom payment."[23] The report regarding the ransom payment must provide a "description of the ransomware attack, including the estimated date range of the attack" and, where applicable, "a description of the vulnerabilities, tactics, techniques, and procedures used to perpetrate the ransomware attack."[24]

***Third-Party Reporting.*** The Act permits a covered entity to use a third party, such as an "incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm," to submit a covered cyber incident report or ransom payment report.[25]

***Supplemental Reporting.*** After submitting a covered cyber incident report to CISA, a covered entity must promptly submit an update or supplement if "substantial new or different information" becomes available or

if the covered entity makes a ransom payment after submitting the initial cyber incident report.[26] A covered entity is permitted to submit one report for both a covered cyber incident and a ransom payment if the entity makes a ransom payment within the 72-hour window for reporting the covered cyber incident.[27]

***Exemptions from Reporting.*** A covered entity is exempt from the Act's requirements for covered cyber incident, ransom payment, and supplemental reporting if the covered entity is "required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe" and an agency agreement and sharing mechanism is in place between CISA and the federal agency.[28] Such an agreement must be documented and must establish policies and mechanisms for sharing of reports in compliance with the 72-hour and 24-hour windows for cyber incident reports and ransom payment reports, respectively.[29]

***Protections Afforded to CISA Reporting.*** The Act affords several protections to covered entities that submit reports to CISA. In particular, the Act provides that "no report submitted to [CISA]" or "document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or political subdivision thereof."[30] The Act makes clear, however, that neither this protection nor any other provision in the Act creates a defense to discovery or otherwise affects the discovery of any communication, document, material, or other record "not created for the sole purpose of preparing, drafting, or submitting such report."[31]

In the regulatory enforcement context, the Act provides that a "Federal, State, local or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to [CISA] . . . to regulate, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment, unless the government entity expressly allows entities to submit reports to [CISA] to meet regulatory reporting obligations of the entity."[32]

Additionally, reports submitted to CISA by covered entities are exempt from disclosure under the Freedom of Information Act and State, Tribal, and local equivalents.[33] The Act further provides that a report will be considered the commercial, financial, and proprietary information of the covered entity if the covered entity designates it as such.[34] And submission of a required report to CISA will not be considered a waiver of "any applicable privilege or protection provided by law."[35]

***Federal Sharing of Reported Information.*** Within 24 hours of receiving covered cyber incident reports and ransom payment reports, CISA is required to "make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies."[36] A Sector Risk Management Agency is a "Federal department or agency designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector."[37] Likewise, any federal agency

that receives a report of a cyber incident, including a ransomware attack, from a covered entity must provide the report to CISA within 24 hours of receiving the report, unless a shorter period is required by an agreement between CISA and the other federal agency.[38]

The Act provides that, immediately upon receiving a covered cyber incident report or ransom payment report, CISA must determine whether the report "is connected to an ongoing cyber threat or security vulnerability" and, where applicable, "rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures."[39]

With regard to the descriptions of security vulnerabilities that may be contained in cyber incident and ransom payment reports, the CISA Director must "develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards."[40]

### Measures to Enhance Federal Support for and Coordination of Cybersecurity

The Act includes several measures aimed at strengthening federal support for and coordination of cybersecurity initiatives. These include:

- Within 180 days of enactment, the development of a Joint Ransomware Task Force by the CISA Director in consultation with the National Cyber Director, the Attorney General, and the Federal Bureau of Investigation "to coordinate an ongoing nationwide campaign against ransomware attacks" and advance international cooperation.[41]
- The establishment of a Cyber Incident Reporting Council (the "Council") by the Secretary of the Department of Homeland Security in consultation with the Office of Management and Budget, the Attorney General, the National Cyber Director, Sector Risk Management Agencies, and other appropriate agencies. The Council will "coordinate, deconflict, and harmonize Federal incident reporting requirements"[42] by identifying duplicative, conflicting, or burdensome requirements for reporting cyber incidents and submitting to appropriate congressional committees within 180 days of the Council's establishment a list of duplicative reporting requirements, challenges in harmonizing them, and actions the Director intends to take to do so, as well as proposed legislative changes to address them.[43]
- A ransomware vulnerability warning pilot program created by CISA, which will identify security vulnerabilities in information systems and notify information system owners of such vulnerabilities to prevent ransomware attacks.[44]

## IMPLICATIONS

The Act imposes tight timing requirements on reporting entities to share information that may be sensitive and not fully understood at the outset of a serious cyber incident. Meeting the 72-hour and 24-hour windows for covered cyber incident reporting and ransom payment reporting, respectively, with the prescribed content required in each may pose challenges for entities working to mitigate the harm caused by cyber incidents and ransomware attacks.

Specifically, details such as the functions of affected information systems, the nature of the unauthorized access, the operational impact of the incident, a description of security defenses, and information about

how cyber incidents and ransomware attacks were perpetrated, including the vulnerabilities exploited, may be challenging to collect, analyze, and prepare into a report for any entity in the midst of a significant cyber attack. This is particularly true for companies in critical infrastructure subsectors, such as financial services, which are already subject to a host of mandatory reporting requirements in the initial days of a serious cyber incident. Financial services entities, for example, may be subject to reporting requirements under the Act, the federal banking regulators' rule, the New York State Department of Financial Services ("DFS") cybersecurity regulation, and the proposed SEC rule. Each of these measures imposes distinct timing requirements for reporting obligations: 72 hours and 24 hours under the Act;[45] 36 hours under the federal banking regulators' rule;[46] 72 hours under the DFS regulation;[47] and four business days under the proposed SEC rule.[48] Each establishes unique triggering events for determining when reporting windows begin, including reasonable belief that a covered cyber incident has occurred and the payment of ransom under the Act;[49] determination that a notification incident has occurred under the federal banking regulators' rule;[50] occurrence of a cybersecurity event that has a reasonable likelihood of materially harming any material part of normal operations of a DFS-regulated entity;[51] and determination that a cybersecurity incident is material under the proposed SEC rule.[52] And each imposes different requirements as to the content that must be reported: a detailed description of the incident and vulnerabilities under the Act;[53] notification of a computer security incident under the federal banking regulators' rule;[54] a description of the event and its impact on the DFS-regulated entity;[55] and a description of the incident and its operational impact in a Form 8-K under the proposed SEC rule.[56]

While the Act suggests that "sharing agreements" designed to alleviate some of this reporting burden may be entered into with agencies that require substantially similar information to be reported, it is unclear how widely such sharing agreements will be implemented given that the nature and extent of the information to be disclosed to CISA appears to be more extensive than what is required to be disclosed pursuant to many existing cyber reporting requirements. Potentially affected companies should consult with their regulators regarding whether the exemption may apply.

The Act's language stating that no report or materials created for the sole purpose of reporting may be "received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority" is clearly intended to provide a measure of protection to entities complying with the detailed reporting obligations created by the Act. This protection appears to leave open, however, that enforcement authorities that receive copies of reports submitted pursuant to the Act may seek to obtain discovery or information from reporting entities based on information provided in the reports, even though the Act precludes the agencies from using the reports themselves in any proceeding. The extent to which the agencies may be allowed to do so may be the subject of future litigation. In addition, the Act's use limitation does not apply to agencies that receive the reports pursuant to sharing agreements. Thus, it remains to be seen to what extent the Act will provide meaningful protection

in the context of investigations and claims that may follow a cybersecurity incident reported pursuant to the Act.

* * *

## ENDNOTES

1 Strengthening American Cybersecurity Act, S. 3600, 117th Congress (2022), *available at* https://www.congress.gov/bill/117th-congress/senate-bill/3600/text?r=3&s=1#toc-H726F16E30F0545219360034278644 5B4.

2 § 2242(a)(1)(A).

3 § 2242(a)(2)(A).

4 § 2242(c).

5 § 2242(b).

6 *See* Cyber Incident Reporting Act, S. 2875, 117th Congress (2021).

7 *See* President Issues Executive Order on Improving the Nation's Cybersecurity, Sullivan & Cromwell Memo (May 14, 2021), *available at* https://www.sullcrom.com/sc-publication-president-issues-executive-order-improving-nations-cybersecurity.

8 *See* Federal Banking Agencies Issue Final Rule Regarding Cybersecurity Incident Notification Requirements, Sullivan & Cromwell Memo (Nov. 22, 2021), *available at* https://www.sullcrom.com/sc-publication-federal-banking-regulators-mandate-cybersecurity-incident-notification.

9 *See* SEC Proposes New Cybersecurity Disclosure Rules for Public Companies, Sullivan & Cromwell Memo (Mar. 11, 2022), *available at* https://www.sullcrom.com/sc-publication-sec-proposes-new-cybersecurity-disclosure-rules-for-public-companies.

10 *See* FinCEN Updates Ransomware Advisory, Sullivan & Cromwell Memo (Nov. 11, 2021), *available at* https://www.sullcrom.com/sc-publication-fincen-updates-advisory-regarding-reporting-ransomware-payments.

11 *See* OFAC Updates Ransomware Advisory, Sullivan & Cromwell Memo (Sept. 23, 2021), *available at* https://www.sullcrom.com/sc-publication-ofac-updates-ransomeware-advisory-designates-crypto-exchange.

12 § 2240(5).

13 *See* Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (Feb. 12, 2013), *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

14 *Id.*

15 § 2242(c)(1).

16 *See* Cybersecurity and Infrastructure Security Agency, Guidance on the Essential Critical Infrastructure Workforce, *available at* https://www.cisa.gov/critical-infrastructure-sectors.

17 § 2242(a)(1)(A).

18 § 2242(c)(2).

19 *Id.*

20 *Id.*

21 § 2242(c)(4).

22 § 2242(a)(2)(A).

23 § 2240(14).

24 § 2242(c)(5).

## ENDNOTES (CONTINUED)

25 § 2242(d).

26 § 2242(a)(3).

27 § 2242(a)(5)(A).

28 § 2242(a)(5)(B).

29 § 204(a)(5).

30 § 2245(c)(3).

31 § 2245(c)(3).

32 § 2245(a)(5).

33 § 2245(b)(2).

34 § 2245(b)(1).

35 § 2245(b)(3).

36 § 2241(a)(10).

37 6 U.S.C. § 651 (2022).

38 § 204(a).

39 § 2245(a)(2)(A).

40 § 2245(a)(2)(B).

41 § 206(a).

42 § 2246(a).

43 §§ 204(b), 207(d).

44 § 205(a).

45 § 2242(a).

46 Office of the Comptroller of the Currency, Federal Reserve System, and Federal Deposit Insurance Corporation, Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (Nov. 18, 2021), *available at* https://www.occ.treas.gov/news-issuances/bulletins/2021/bulletin-2021-55.html (the "Federal Banking Regulators' Rule") at 70.

47 N.Y. Comp. Codes R. & Regs. tit. 23, § 500.17 ("DFS Regulation").

48 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, SEC Release Nos. 33-11038; 34-943529; IC-34529 (Mar. 9, 2022), *available at* https://www.sec.gov/rules/proposed/2022/33-11038.pdf (the "SEC Proposing Release") at 18.

49 § 2242(a).

50 Federal Banking Regulators' Rule at 70.

51 DFS Regulation § 500.17.

52 SEC Proposing Release at 22.

53 §§ 2242(c)(4), (5).

54 Federal Banking Regulators' Rule at 31.

55 DFS Regulation § 500.17.

56 SEC Proposing Release at 21.

## ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

## CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.