Simpson Thacher

Memorandum

Newly Enacted Federal Cybersecurity Disclosure Statute Will Significantly Expand Data Breach and Ransomware Reporting Obligations

April 5, 2022

Tucked into the recently enacted 2022 Consolidated Appropriations Act is the Cyber Incident Reporting for Critical Infrastructure Act (the "Act"), which will—once effective—significantly expand the obligation of[1] companies in the energy, communications, financial services and other critical infrastructure sectors to report a range of cyberattacks and ransomware payments. It marks the first broad-based federal cyber incident reporting requirement and comes on the heels of cyber disclosure rules recently proposed by the Securities and Exchange Commission for public companies.[2] While these broader obligations will not take effect until the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issues an implementing rule in 2024, this legislation is yet another expansion of regulatory disclosure obligations relating to cybersecurity matters.

In light of state data breach notification statutes, existing securities disclosure obligations, and other considerations, many companies already have processes in place to evaluate disclosure of cyber incidents. But given the relatively short timeframe that will be available under the Act for reporting certain incidents, this legislation provides additional reason for companies to take the time now to review their cybersecurity response plans and disclosure controls to ensure that they are appropriately designed to enable prompt evaluation and timely disclosure of cyber incidents where required.

Effective Date and Scope of Covered Entities

Under the Act, CISA is required to issue a proposed implementing rule by March 15, 2024 and a final rule 18 months thereafter, which will establish the effective date for the Act.

The Act defines "covered entity" as "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21 that satisfies the definition established by [CISA] in the final rule issued pursuant to section 2242(b)."

[1] *See* Consolidated Appropriations Act, 2022 Division Y- Cyber Incident Reporting For Critical Infrastructure Act of 2022.

[2] *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure as well as Public Company Cybersecurity Fact Sheet.

The Act requires CISA's definition of "covered entity" to be "based on (A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety; (B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country and (C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure" as well as the definition set forth in the Homeland Security Act of 2002, codified at 6 U.S.C. 651.[3] However, in light of Presidential Policy Directive 21, a company in any of the following sectors, at a minimum, will be included as a covered entity: 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.[4]

Reporting Requirements

The Act will require covered entities to report a "covered cyber incident" within 72 hours.

The Act directs CISA to define a "covered cyber incident." At a minimum, the definition is required to include an incident that (1) results in a "substantial loss of confidentiality, integrity or availability of the information system or the information the system processes, stores, or transmits"; (2) results in "disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability" or (3) involves "unauthorized access or disruption of business or industrial operations" due to a "compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise." When defining a covered cyber incident, CISA is also required to consider the sophistication of the attack, the type and volume of information affected, the number of individuals potentially affected, and the impact to systems.

Notably, the Act recognizes that a covered cyber incident "does not include an occurrence that imminently, but not actually, jeopardizes (i) information on information systems or (ii) information systems."

A covered entity is required to report a covered cyber incident when it "reasonably believes that a covered cyber incident has occurred." However, the Act is silent with respect to what constitutes a "reasonable" belief, but such clarity may be included in the forthcoming CISA implementing rule. If there is a reasonable belief such event has occurred, the initial disclosure to CISA must include the following information:

[3] *See* Homeland Security Act 2002, 6 U.S.C. 651 (The term "incident" means "an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system").

[4] *See* President Policy Directive 21.

- A description of the covered cyber incident, which identifies and describes the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been affected by such cyber incident; describes the unauthorized access, estimated date range of such incident and 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 the cyber incident; and
- The category or categories of information that were, or are reasonably believed to have been, subject to unauthorized access or acquisition.

In terms of supplemental disclosures, the Act requires that covered entities "promptly submit to the Agency an update or supplement to a previously submitted covered cyber incident report if substantial new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report . . . until such date that such covered entity notifies the Agency that the covered cyber incident at issue has concluded and has been fully mitigated and resolved."

Reporting Requirements for Ransomware

The Act separately includes reporting requirements for ransomware payments specifically that are far broader than its reporting requirements for cyber incidents more generally. Under the Act, covered entities will be required to report a "ransom payment" within 24 hours of payment, and include the date, demand and amount of payment, as well as the payment instructions. In other words, ransom payments must be reported to the CISA even if the incident does not meet the definition of a covered cyber incident. (We note that special considerations and risks apply if the ransomware demand comes from a sanctioned country or individual. Please consult the authors of this memorandum with any questions.)

The Act defines "ransom payment" 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." A "ransomware attack" is defined 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 a 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." It 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."

For further information regarding this memorandum, please contact one of the following authors:

NEW YORK CITY

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Bobbie Burrows
+1-212-455-2333
bobbie.burrows@stblaw.com

Shanice D. Hinckson
+1-212-455-2113
shanice.hinckson@stblaw.com

Melanie D. Jolson
+1-212-455-3346
melanie.jolson@stblaw.com

Jonathan S. Kaplan
+1-212-455-3028
jonathan.kaplan@stblaw.com

Jacob Lundqvist
+1-212-455-3348
jacob.lundqvist@stblaw.com

Kate E. Mirino
+1-212-455-2055
kate.mirino@stblaw.com

Alysha J. Sekhon
+1-212-455-3762
alysha.sekhon@stblaw.com

PALO ALTO

Harrison J. (Buzz) Frahn
+1-650-251-5065
hfrahn@stblaw.com

For further information regarding ransomware and sanctions, please contact one of the following:

WASHINGTON, D.C.

Abram J. Ellis
+1-202-636-5579
aellis@stblaw.com

Malcolm J. (Mick) Tuesley
+1-202-636-5561
mick.tuesley@stblaw.com