GIBSON DUNN

March 22, 2022

PRESIDENT BIDEN SIGNS INTO LAW THE CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT, EXPANDING CYBER REPORTING OBLIGATIONS FOR A WIDE RANGE OF PUBLIC AND PRIVATE ENTITIES

To Our Clients and Friends:

On March 15, 2022, President Joe Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act, which was included in an omnibus appropriations bill.[1] Against the backdrop of high-profile cyberattacks on critical infrastructure providers and growing concerns of retaliatory cyberattacks relating to Russia's invasion of Ukraine, the House approved the bipartisan legislation on March 9 and the Senate unanimously approved the legislation on March 11 after failing to pass similar legislation in recent years.

The Act creates two new reporting obligations on owners and operators of critical infrastructure:

- An obligation to report certain cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) within 72 hours, and
- An obligation to report ransomware payments within 24 hours.

The new reporting obligations will not take effect until the Director of CISA promulgates implementing regulations, including "clear description[s] of the types of entities that constitute covered entities."[2] The Act does provide guideposts for which entities may be covered and refers to the Presidential Policy Directive 21 from 2013, which deems the following sectors as critical infrastructure: 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.[3]

The Act considerably expands the reporting obligations of covered entities and CISA's role with respect to cyber reporting initiatives, the rulemaking process, and information sharing among federal agencies. Below is a summary of the legislation, as well as key takeaways.

I. The Act's Impact on Covered Entities

A. Reporting Obligations

Under the Act, covered entities that experience a "covered cyber incident" are required to report the incident to CISA no later than 72 hours after the entity "reasonably believes" that such an incident has

occurred.[4] The Act defines a "covered cyber incident" as one that is "substantial" and meets the "definition and criteria" to be set by the CISA Director in the forthcoming rulemaking process.[5] In addition, covered entities are also required to report any ransom payments made as a result of a ransomware attack to CISA no later than 24 hours after making the payment.[6] Entities are required to report ransom payments even if the underlying ransomware attack is not a covered cyber incident."[7] If a covered entity experiences a covered incident and remits a ransom before the 72-hour deadline, it may submit a single report to satisfy both reporting requirements.[8] Covered entities that are required to report cyber incidents or ransom payments also will be required to preserve relevant data.[9] Although the Act specifies some of the content that reports should contain,[10] the CISA Director will further prescribe report contents through the rulemaking process.

After reporting a covered incident, covered entities will be required to submit updates as "substantial new or different information becomes available" until the covered entity notifies CISA that the incident has been fully mitigated and resolved.[11] Such supplemental reports will need to address whether a covered entity made a ransom payment after submitting the initial report.

To "enhance the situational awareness of cyber threats," the legislation provides for voluntary reporting of incidents and ransom payments by non-covered entities, as well as the voluntary provision of additional information beyond what is mandatory by covered entities.[12] Required and voluntary reporting will receive the same protections, further described below.

Notably, the Act creates an exception whereby its reporting requirements will not apply to covered entities that, "by law, regulation, or contract," are already required to report "substantially similar information to another Federal agency within a substantially similar timeframe."[13] However, this exception will be available only if the relevant federal agency has an "agency agreement and sharing mechanism" in place with CISA.

B. Protections for Reporting Entities

Recognizing some of the concerns relating to reporting, the Act protects reporting entities from certain liability associated with the submission of required or voluntary reports. Under the Act, submitted cyber incident and ransom payment reports cannot be used by CISA, other federal agencies, or any state or local government to regulate, including through enforcement action, the activities of the covered entity that submitted the report.[14]

In addition, submitted reports must:

- Be considered commercial, financial, and proprietary information if so designated;
- Be exempt from disclosure under freedom of information laws and similar disclosure laws;
- Not constitute a waiver of any applicable privilege or protection provided by law; and
- Not be subject to a federal rule or judicial doctrine regarding *ex parte* communications.[15]

Certain additional protections further encourage compliance and recognize the concerns that victim companies may face in providing notifications. Notably, the required reports, and material used to prepare the reports, cannot be received as evidence, subject to discovery, or used in any proceeding in federal or state court or before a regulatory body.[16] Also, no cause of action can be maintained based on the submission of a report unless it is an action taken by the federal government to enforce a subpoena against a covered entity. These liability protections only apply to litigation based on the submission of a cyber incident or ransom payment report to CISA, not the underlying cyber incident or ransom payment.[17]

II. CISA's Oversight and Responsibilities under the Act

By considerably expanding CISA's role, the Act essentially establishes CISA as the central federal agency responsible for cyber reporting for companies operating within a critical infrastructure sector, advancing the forthcoming rulemaking process, and coordinating with other agencies with respect to information sharing and new initiatives.

A. Forthcoming Rulemaking

The Act provides some parameters for key definitions and processes, but ultimately requires CISA to spell out various requirements via rulemaking. The legislation requires the CISA Director—in consultation with Sector Risk Management Agencies, the Department of Justice, and other federal agencies—to issue a notice of proposed rulemaking within 24 months.[18] The Director must issue a final rule within 18 months of issuing the proposed rule.[19] Among other items, the Director will need to issue regulations concerning which entities are covered by the requirements, the types of substantial cyber incidents that the Act covers, data preservation, and the manner, timing, and form of reports.

Once the final rule is issued, CISA will conduct an outreach and education campaign to inform likely covered entities and supporting cybersecurity providers of the Act's requirements.[20]

B. Information Assessment and Sharing

The Act requires CISA to aggregate, analyze, and share information learned from submitted reports to provide government agencies, Congress, companies, and the public with an assessment of the constantly evolving cyber threat landscape. (When sharing information with non-federal entities and the public, CISA is required to anonymize the victim entities that filed report(s).[21])

Some of the responsibilities of CISA's National Cybersecurity and Communications Integration Center ("the Center") include immediately reviewing submitted reports to determine whether the incident relates to an ongoing cyber threat or security vulnerability.[22] Moreover, the legislation enhances federal cyber incident sharing. The Center is required to make reports available to relevant Sector Risk Management Agencies and appropriate federal agencies within 24 hours of receipt.[23] Similarly, federal agencies that receive incident reports (including from non-covered entities) must submit them to CISA no later than 24 hours following receipt.[24]

The Act sets forth authorized uses and sharing of submitted reports. Information may be disclosed to, retained by, and used by federal agencies solely for: a cybersecurity purpose; to identify a cyber threat or security vulnerability; to respond to, prevent or mitigate specific threats of death, serious bodily harm, or serious economic harm; to respond to or prevent a serious threat to a minor; or to respond to an offense arising out of a reported incident.[25]

Among other items, the Center is tasked with establishing mechanisms to receive feedback from stakeholders, facilitating timely information sharing with critical infrastructure companies, and publishing quarterly unclassified reports on cyber incident trends and recommendations.[26] The Act also imposes on CISA several congressional reporting requirements, including briefings to describe stakeholder engagement with rulemaking and enforcement mechanism effectiveness.[27]

C. Enforcement

The Act provides several enforcement mechanisms. If a covered entity fails to submit a required report, the CISA Director may obtain information about the cyber incident or ransom payment by directly engaging with the covered entity "to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred."[28] If the covered entity does not respond to the initial information request within 72 hours, the CISA Director may issue a subpoena. Failure to comply with the subpoena – or information furnished in response to a subpoena – may result in the referral of the matter to the Department of Justice for enforcement.[29]

Additionally, the Act denies covered entities some of the protections detailed above if they do not comply with its reporting requirements.

Under the Act, the CISA Director must provide an annual report to Congress that conveys anonymized information about the number of initial requests for information, issued subpoenas, and referred enforcement matters.[30] This report will be published on CISA's website.

D. Forthcoming Initiatives

Finally, the Act sets forth several initiatives to enhance cybersecurity coordination efforts:

- *Cyber Incident Reporting Council*: The Act calls for DHS to lead an intergovernmental Cyber Incident Reporting Council to "coordinate, deconflict, and harmonize Federal incident reporting requirements[.]"[31]

- *Ransomware Vulnerability Warning Pilot Program*: No later than one year after the Act's enactment, CISA is required to establish a new Ransomware Vulnerability Warning Pilot Program.[32] Leveraging existing authorities and technology, this program is tasked with identifying the most common security vulnerabilities used in ransomware attacks and techniques on how to mitigate and contain the security vulnerabilities.

- *Joint Ransomware Task Force*: The Act instructs the CISA Director to establish and chair the Joint Ransomware Task Force "to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation."[33]

III. Takeaways

Once in effect, the Act will considerably expand reporting considerations for some entities. Accordingly, companies should consider the following next steps:

- ***Companies in Many Sectors Are Potentially Subject to the New Reporting Requirements.*** Companies in the many industry sectors cited in Presidential Policy Directive 21 should closely monitor the proposed rulemaking and evaluate whether the Act's requirements are likely to apply to their businesses. Entities that may be covered by the Act may wish to comment during the rulemaking process, as the final rule will impose more detailed requirements.

- ***Companies Should Identify Existing Reporting Obligations and Monitor Interagency Sharing Agreements.*** Although the Act's reporting obligations will not become effective for some time, critical infrastructure entities should take steps now to prepare for potentially overlapping disclosure obligations. As detailed above, the Act creates an exception whereby its reporting requirements will not apply to covered entities that file a substantially similar report with another federal agency. However, this exception will be available only if the relevant federal agency has an agreement and sharing mechanism in place with CISA. The law also authorizes federal (but not state) agencies to coordinate, deconflict and harmonize federal incident reporting obligations.In order to monitor developments in the harmonization of federal incident reporting obligations, as well as track agency sharing mechanisms, potentially impacted entities should first assess their other federal cybersecurity disclosure obligations. Some of these obligations may stem from reporting obligations imposed on federal government contractors and recent executive orders. For instance, the Biden administration's Executive Order in May 2021, "Improving the Nation's Cybersecurity," requires federal contractors to share information regarding incidents.[34] In 2021, the Transportation Security Administration also issued a directive which requires pipeline entities to report confirmed and potential incidents.[35]Public companies should also consider whether reports submitted under the Act may prompt disclosures under the SEC's newly proposed rule, which requires public disclosure of material cybersecurity incidents within four business days.[36]Finally, the recent reporting developments should be assessed against a heightened enforcement backdrop—namely, the DOJ's Civil Cyber-Fraud Initiative, which seeks to leverage the False Claims Act to hold accountable contractors and recipients of federal funds and grants that knowingly violate contractual obligations to monitor and report cybersecurity incidents and breaches.[37]

- ***Companies May Need to Revisit their Cybersecurity Policies, Procedures, and Programs.*** In light of the Act's requirements, potentially impacted entities should determine whether changes to their cyber programs may be required, examine their internal policies and procedures to reflect the Act's requirements, and address and prepare for overlapping disclosure obligations under state, federal and international laws.

[1] *See* Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 116th Cong. (2022).

[2] H.R. 2471 § 2242(c)(1). This provision provides that when promulging the final rule to define "covered entities," the CISA Director must consider the national security, economic security, and public health and safety consequences of a potential cyberattack on the entity, the likelihood that such an entity could be targeted, and the extent to which a cyberattack will enable disruption of the reliable operation of critical infrastructure.

[3] H.R. 2471 § 2240(5). *See also* White House, Office of the Press Secretary, *Presidential Policy Directive -- 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; CISA, *Critical Infrastructure Sectors*, available at https://www.cisa.gov/critical-infrastructure-sectors.

[4] H.R. 2471 § 2242(a)(1)(A).

[5] *Id.* at § 2240(4). The legislation does not define "substantial."

[6] H.R. 2471 § 2242(a)(2)(A).

[7] H.R. 2471 § 2242(a)(2)(B).

[8] H.R. 2471 § 2242(a)(5)(A).

[9] H.R. 2471 § 2242(a)(4).

[10] At a minimum, covered incident reports must convey certain information about the incident, including:

- a description of the covered incident;
- a description of the vulnerabilities exploited, security defenses in place, and tactics, techniques, and procedures used to perpetrate the incident;
- information about the actor(s) reasonably believed to be responsible for the incident;
- and the identification of categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person.*See* H.R. 2471 § 2242(c)(4). The Act also details minimum reporting requirements for ransom payments. *See id.* at § 2242(c)(5).

[11] H.R. 2471 § 2242(a)(3).

[12] H.R. 2471 § 2243.

[13] H.R. 2471 § 2242(a)(5).

[14] H.R. 2471 § 2245(a)(5)(A).

[15] H.R. 2471 § 2245(b).

[16] H.R. 2471 § 2245(c)(3).

[17] H.R. 2471 § 2245(c).

[18] H.R. 2471 § 2242(b)(1).

[19] H.R. 2471 § 2242(b)(2).

[20] H.R. 2471 § 2242(e)

[21] H.R. 2471 § 2245(d).

[22] H.R. 2471 § 2245(a)(2)(A).

[23] H.R. 2471 § 2241(a)(10).

[24] H.R. 2471 § 104(a)(1).

[25] H.R. 2471 § 2245(a)(1).

[26] H.R. 2471 § 2241(a).

[27] H.R. 2471 §§ 107; 2244(g).

[28] H.R. 2471 § 2244(a).

[29] H.R. 2471 § 2244(c)-(d).

[30] H.R. 2471 § 2244(g).

[31] H.R. 2471 § 2246(a).

[32] H.R. 2471 § 105.

[33] H.R. 2471 § 106(a)(1).

[34] *See* Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 12, 2021).

[35] *See* Press Release, Dep't of Homeland Security, *DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators* (May 27, 2021),

https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

[36] *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release, No. 34-94382 (Mar. 9, 2022), available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf; *see also* Gibson Dunn's client alert on the SEC's proposed rule, available at https://www.gibsondunn.com/sec-proposes-rules-on-cybersecurity-disclosure/.

[37] *See* Press Release, U.S. Dep't of Justice, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

This alert was prepared by Ashlie Beringer, Alexander H. Southwell, Ryan T. Bergsieker, and Snezhana Stadnik Tapia.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity and Data Innovation practice group:

United States

Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Robert K. Hur – Washington, D.C. (+1 202-887-3674, rhur@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)

GIBSON DUNN

Europe

Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com)
Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Bernard Grinspan – Paris (+33 (0) 1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen – London (+44 (0) 20 7071 4203, swazen@gibsondunn.com)

Asia

Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)