March 18, 2022

New 72-Hour Cyber Incident Notice Requirement for Critical Infrastructure Entities

On March 15, as part of the Consolidated Appropriations Act, 2022, 2022 P.L. 117-103, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the Act). The Act, which passed with bipartisan support, comes amid repeated warnings of potential cyberattacks against the United States by Russia as the conflict with Ukraine escalates, and follows several high-profile cyber incidents.

With the goal of centralizing reporting, coordination, and response for cyber-related incidents within the Cybersecurity and Infrastructure Security Agency (CISA), an operational component under Department of Homeland Security oversight, the Act requires entities meeting its definition of "covered entity" to, among other things, (1) report to CISA within 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred and (2) report to CISA within 24 hours of any ransom payment made by the covered entity as the result of a ransomware attack against the covered entity. With these new rapid reporting requirements, Congress hopes to avoid confusion among victims as to which federal government entity has primary responsibility for incident response and to enhance the federal government's ability to spot attack patterns and prevent attacks from spreading. In addition to reporting requirements, the Act requires compliance with procedures, to be developed by CISA, to ensure the preservation and integrity of data related to any covered cyber incident or ransom payment.

A covered entity, as defined by the Act, falls within one of the 16 critical infrastructure sectors, set forth in Presidential Policy Directive 21, whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, economic security, national public health or safety, or any combination thereof, including the Chemical, Energy, Financial Services, Healthcare and Public Health, and Information Technology sectors, just to name a few.[1] The entities within these sectors that fall within the definition of covered entity will be dependent on the final rules promulgated by CISA. The Act, however, directs CISA to consider the following in defining a covered entity: (1) the consequences that disruption or compromise of an entity would have on national security, economic security, or public health and safety; (2) the likelihood that such an entity may be targeted by a cyberattack; and (3) the extent to which compromise of an entity will enable disruption in the operation of critical infrastructure.

CISA is also tasked with defining a "covered cyber incident" within its rulemaking authority. At a minimum, a cyber incident must be substantial and involve the occurrence of (1) "a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes"; (2) "a disruption of business or industrial operations" as a result of certain attacks against an information system or network or a technology system or process; or (3) "unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise." CISA is also directed to consider, in defining a covered cyber incident, (1) the tactics used to facilitate the cyber incident; (2) the amount, type, and sensitivity of the data subject to the incident; (3) the volume of individuals potentially affected by the incident; and (4) the "potential impacts on industrial control systems."

A covered entity that is impacted by a covered cyber incident will be required to submit a report within 72 hours of having reasonable belief that such an incident has occurred. The report will need to include, at a minimum, (1) a detailed description of the incident, including its impacts on operations; (2) a description of the security measures that were in place at the time of

the incident, the exploited vulnerabilities, and the techniques used by the attacker; (3) any contact information related to the actors believed to be responsible for the incident; (4) the categories of information accessed or obtained by the attacker; (5) details about the entity; and (6) contact information of the entity.

Although the Act grants CISA 24 months to publish a notice of proposed rulemaking and 18 months thereafter to issue a final rule, it may move more quickly given the threat of cybersecurity incidents in today's geopolitical unrest. Given this and the very short period of time for reporting cyber incidents, potentially covered entities are well advised to review their existing incident response plans to ensure timely response and reporting under the new Act. If you anticipate that your business may qualify as a covered entity under the Act, you should track CISA's proposed rules closely as they unfold. Comments you may wish to provide CISA should consider whether your processes are nimble enough to comply with the Act's tight reporting deadlines. Is information reporting within your incident response team sufficiently centralized to ensure an efficient flow of information to the persons in charge of preparing the Act's required reports? Looking at the report elements specified in the Act, is your incident response plan structure appropriate for quickly gathering the required information? Are the definitions of incidents to be reported and information to report sufficiently clear? Those businesses that anticipate being covered by the Act should also consider preparing a template report, attached as an exhibit to your incident response plan, that can be used as a guide for initial information collection.

If you have questions about how to determine whether your company qualifies as a covered entity under the Act, how to participate in the CISA rulemaking efforts, how to prepare for compliance with the Act's reporting and other requirements, or any other questions related to the Act, please reach out to any of the attorneys in Day Pitney's Cybersecurity and Data Protection group.

---

[1] The complete list of critical infrastructure sectors is Chemical Sector, Commercial Facilities Sector, Communications Sector, Critical Manufacturing Sector, Dams Sector, Defense Industrial Base Sector, Emergency Services Sector, Energy Sector, Financial Services Sector, Food and Agriculture Sector, Government Facilities Sector, Healthcare and Public Health Sector, Information Technology Sector, Nuclear Reactors, Materials, and Waste Sector, Transportation Systems Sector, and Water and Wastewater Systems Sector.

Authors

David T. Doot
Of Counsel

Hartford, CT | (860) 275-0102

dtdoot@daypitney.com

John F. Kaschak
Associate

Parsippany, NJ | (973) 966-8034

jkaschak@daypitney.com

Kritika Bharadwaj
Partner

New York, NY | (212) 297-2477

kbharadwaj@daypitney.com

Richard D. Harris
Of Counsel

Hartford, CT | (860) 275-0294

New Haven, CT | (203) 752-5094

rdharris@daypitney.com

William J. Roberts
Partner

Hartford, CT | (860) 275-0184

wroberts@daypitney.com