ECKERT SEAMANS ATTORNEYS AT LAW

October 5, 2022

Data Privacy & Security Alert

DHS's Cybersecurity and Infrastructure Security Agency Seeking Guidance on Critical Infrastructure Cyber Reporting

By Matthew H. Meade and Emma M. Lombard

On September 12, 2022, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued a Request for Information (RFI) in an effort to obtain feedback from the public on aspects of proposed regulations for cyber incident reporting by critical infrastructure entities.

This ongoing endeavor stems largely from a wave of cyberattacks on critical infrastructure entities in 2021, including those that made national news against SolarWinds and Colonial Pipeline. As a result, in May 2021, President Biden signed Executive Order 14028, titled "Improving the Nation's Cybersecurity," which outlines ways to protect federal networks, remove barriers to sharing threat information, and establish stronger incident detection and response tactics.

In March of this year, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which primarily requires "covered entities" to report "substantial" cyber incidents to CISA within 72 hours of their occurrence, and to report any ransom paid to a threat actor within 24 hours of payment. It also directs CISA to implement rules that further define certain provisions.

The primary question that CIRCIA leaves unanswered is who qualifies as a "covered entity," as its definition within the Act is "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 2242(b)." Presidential Policy Directive 21 identifies the following sixteen critical infrastructure sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food & Agriculture; Government Facilities; Healthcare & Public Health; Information Technology; Nuclear Reactors, Materials, & Waste; Transportation Systems; and Waste & Wastewater Systems. Because CIRCIA's definition incorporates by reference a rule that CISA has yet to propose or finalize, whether an entity within any of the foregoing critical infrastructure sectors will be subject to CIRCIA's mandatory reporting requirements cannot be determined. The current definition is broad enough to include entities of all types in both the public and private sectors.

CIRCIA further requires CISA to consider the following three factors in formulating its definition of "covered entity":

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.

H.R. 2471 § 2242(c)(1).

© Eckert Seamans Cherin & Mellott, LLC, 2022, all rights reserved.

Regarding the substantive provisions of the proposed regulations, the RFI seeks feedback on the meanings of "covered cyber incident," "substantial cyber incident," "supply chain compromise," and any other terms that "would improve the regulations and proposed definitions for those terms." The RFI also asks what constitutes a "reasonable belief" that a covered cyber incident has occurred to trigger the 72-hour reporting deadline. Seemingly in an attempt to gauge the impact of any proposed regulation, CISA has requested feedback on the number of entities likely to be covered by the reporting, as well as the number of covered cyber incidents likely to occur either in total, or by industry, along with the number of ransom payments likely to be made on annual basis.

As to the procedural provisions, the RFI seeks comments on the policies, procedures, and requirements for incident reporting. Specifically, the RFI poses several questions regarding how costly compliance with existing reporting requirements is, how reporting under the new regulations should work, and what method should be employed for calculating the reporting timeline.

This RFI is an ideal opportunity for organizations to offer feedback and potentially shape the scope of the proposed regulations. CISA is hosting a series of public listening sessions, including one newly-announced session in Washington, D.C., and accepting responses to the RFI until November 14, 2022. Despite the potential length of the public rulemaking process, companies should begin preparing for these regulations now by reviewing and updating their incident response plans. Potentially covered entities should monitor the rulemaking process to ensure that they are equipped technically and organizationally to meet CIRCIA'S obligations. Eckert Seamans will continue to monitor the rulemaking process.

ECKERT SEAMANS ATTORNEYS AT LAW

This Data Security & Privacy Alert is intended to keep readers current on developments in the law, and is not intended to be legal advice. If you have any questions, please contact Matthew H. Meade at 412.566.6983 or mmeade@eckertseamans.com, Emma M. Lombard at 609.989.5024 or elombard@eckertseamans.com,or any other attorney at Eckert Seamans with whom you have been working.

© Eckert Seamans Cherin & Mellott, LLC, 2022, all rights reserved.