CISA Seeks Public Input on Cyber Incident Reporting

By Susan Lindberg
September 12, 2022

The Cybersecurity and Infrastructure Security Agency (CISA) recently issued a Request for Information (RFI) seeking public input on cyber incident reporting requirements. The RFI marks an initial step by CISA in formulating regulations as required under the new Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), enacted March 15, 2022. Comments must be submitted by November 14, 2022.

CISA will also hear comments from the public in listening sessions in 11 cities, beginning in September. Dates, times, and locations can be found in the Federal Register notice. Sessions will be four hours and presentations are limited to three minutes each, and capacity is limited, with priority given to attendees who pre-register.

The new legislation requires critical infrastructure companies to report cybersecurity incidents to CISA within 72 hours, and ransom payments within 24 hours. The requirements will become effective when CISA issues new regulations implementing the statute. CISA has until March 2024 to propose rules and another 18 months after that to finalize them. Affected companies will have the opportunity to comment during the CISA rulemaking process. More information on CIRCIA can be found here.

In the RFI, CISA lists the specific topics on which it seeks feedback, although the list is not exhaustive. The four key topics are:

1. definitions and terminology – for example, the meaning of "covered entity" subject to reporting requirements, and the meaning of "covered cyber incident";

2. report contents and submission procedures, including the specific information required to be included in the reports, what constitutes a "reasonable belief" that a covered cyber incident has occurred, clarification on the timing of reports and supplemental information submissions, and requirements for submission of reports by third parties;

3. existing incident reporting requirements and security vulnerability information sharing – for example, areas of overlap, duplication, or conflicts between existing requirements and CIRCIA requirements, and information on the cost of compliance;

4. additional policies, procedures, and requirements, including information on protections for reporting entities.

CISA encourages commenters to identify specific approaches for the agency to consider and to "provide information supporting why the approach would foster a cost-effective and balanced

approach to cyber incident and ransom payment reporting requirements." Specific information, data, or recommendations are encouraged as opposed to "generic feedback."

Until fairly recently, reporting of cybersecurity incidents has been largely voluntary. Prescriptive requirements for disclosure to the government have been industry specific, or, in the case of government contractors, specified by contract. Successive administrations have attempted to encourage voluntary information sharing by private industry, with limited success. The Cybersecurity Information Sharing Act of 2015 required the Department of Homeland Security to establish a capability and process for sharing cyber threat indicators with both the federal government and private sector entities. The statute includes protections for private companies that share information with the government through DHS, including liability protections, privilege maintenance, protection of proprietary information, a safe harbor from disclosure in response to Freedom of Information Act requests, and other protections. These aspects are further detailed in guidance documents. In practice, the language of the statute creating these protections is not particularly clear, and relatively few companies have chosen to voluntarily share information.

CISA's RFI offers critical infrastructure owners the opportunity to shape the new information sharing requirements so that a company's information and infrastructure is sufficiently protected, and to create a reporting process that acknowledges the practical realities of responding to an incident.

For more information regarding GableGotwals' Cybersecurity and Data Privacy practice, please click here.

Susan Lindberg
Energy | Cybersecurity | Governance
918-595-4826
slindberg@gablelaw.com