PUBLICATION

New Legislation Will Require Critical Sector Entities to Report Certain Cyber Incidents

Authors: Monica J. Manzella
March 21, 2022

On March 15, 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act (the Act) as part of the Consolidated Appropriations Act of 2022. The Act requires "critical sector" entities to promptly report to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) certain cyber incidents and ransomware payments. Critical sector entities are those considered vital to the U.S. economy and public health and safety, but were not specifically identified by the Act. CISA will conduct an education campaign in connection with the issuance of the final rule to inform applicable entities of the Act's reporting requirements.

Reporting Requirements and Guidelines. Entities subject to the Act must report all cyber incidents within 72 hours of either the discovery of the incident or the reasonable belief that a covered cyber incident took place. Entities must further report all ransomware related payments within 24 hours of payment. This requirement applies even if payments are made as a result of a ransomware attack that is not defined by the Act as a covered cyber incident. If an entity experiences a covered cyber incident and makes a ransom payment prior to the deadline for the 72-hour report, it may submit a single report to satisfy the requirements of both deadlines. However, an entity is required to supplement a cyber incident report to CISA if it makes a ransom payment after submitting that initial report. In addition, entities must promptly submit updates and supplements to CISA as substantially new or different information becomes available. Entities have a continuing obligation to submit report updates and supplements until they have notified CISA that the covered cyber incident at issue has been resolved.

An entity may use a third party, such as an incident response company, insurance provider, service provider, or law firm to fulfill its report submission requirements under the Act. Entities are further required to preserve any and all data relevant to the cyber incident or ransom payment in accordance with the procedures to be established in the final rules. This should not change much of what already transpires when handling such incidents in a practical sense; however, it could necessitate more formal tracking and retention of information gathered during such incidents.

All submitted reports will be treated as commercial, financial, and proprietary information of the entity when designated as such and will not constitute a waiver of any applicable privilege or protection provided by law. Furthermore, no cause of action can be maintained based on the submission of a report unless it is action taken by the federal government.

Exemption. These reporting requirements do not apply if an entity is already required to report substantially similar information to another federal agency within a substantially similar timeframe, but only if that federal agency has an agency agreement sharing mechanism CISA. Notwithstanding this exemption, entities may voluntarily report cyber incidents or ransom payments to CISA that are not required under the rules, but which may enhance the situational awareness of cyber threats. Entities may also voluntarily include information not required in mandatory reports.

Reporting Analysis. The Act requires CISA's National Cybersecurity and Communications Integration Center (the Center) to promptly review and analyze all reports made to determine whether the cyber incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability, to assess the effectiveness of security controls, to identify tactics and techniques to overcome the cybersecurity threat, and for other cybersecurity purposes, including to assess potential impact of cyber incidents on public health and safety and to enhance situational awareness of cyber threats across critical infrastructure sectors. Entities should anticipate more direct communication from the government as a result and will need to plan for those communications and related expectations.

Within 24 hours of receiving a submitted report, the Center will be required to make this information available to the appropriate Sector Risk Management Agencies and other appropriate federal agencies to enhance collaboration and coordination efforts, provided such data sharing is constricted to the following purposes:

1. A cybersecurity purpose;
2. A response to a cyber threat;
3. A response to a security vulnerability;
4. A response to a specific threat of death or serious bodily harm, or serious economic harm;
5. A response to a serious threat to a minor; and
6. Prevention of an offense arising out of a cyber-incident.

The Center will also be tasked with:

7. Establishing mechanisms to receive feedback from stakeholders on its processes;
8. Facilitating timely sharing of cyber incident information with critical infrastructure owners and operators; and
9. Publishing quarterly unclassified, public reports that aggregate cyber incident observations and recommendations.

Enforcement. If CISA has reasonable grounds to believe that an entity has experienced a reportable cyber incident or made a reportable ransom payment, and that entity fails to submit its required report, CISA may obtain information about the cyber incident or ransom payment by engaging the entity directly to request information. If CISA does not receive a response from the initial information request within 72 hours, it may issue a subpoena. If the entity fails to comply with the subpoena, or if CISA otherwise determines that grounds exist to support the referral of the matter to the U.S. Attorney General, the Act allows for such a referral and for the Attorney General to bring a regulatory enforcement action or criminal prosecution against the offending entity.

Additional Provisions. The Act also includes several provisions to further enhance cybersecurity protective efforts and public-private information sharing including the creation of a Cyber Incident Reporting Council, the development of a Ransomware Vulnerability Warning Pilot Program, the establishment of a Joint Ransomware Task Force, and greater data and reporting sharing requirements among federal agencies.

Effectiveness of the Act. It is important to note that the reporting requirements described in this Alert will not be effective until the final rules are effective and published, which we estimate to take at least two years. CISA must first issue a Notice of Proposed Rulemaking (NPRM) within two years proposing the final rules to implement the requirements included in the Act and then, not later than 18 months after publication of the NPRM, the final rule will be issued. The final rule will more clearly define the scope of these reporting requirements and also specify incident report content requirements, ransom report content requirements and the scope of data preservation requirements.

Nonetheless, critical infrastructure entities would be well-served to begin considering whether they will be subject to the new reporting requirements and whether any immediate adjustments should be made to their cyber programs to meet the Act's goals. Entities should also consider participation in the forthcoming rulemaking process, either directly or through industry groups, in conjunction with their internal business assessments.

Baker Donelson stands ready to support you as you navigate these considerations and the potential impact of the Act on your business operations. If you have any questions about this or any other aspect of your cybersecurity practices, please contact Monica J. Manzella, CIPP/US or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Practice Team.