US Senate unanimously passes the Strengthening American Cybersecurity Act

Cybersecurity Law Alert

14 March 2022

By: Andrew Serwin | Deborah R. Meshulam | Edward J. McAndrew | Leila Javanshir

In a sign of how quickly the policy environment around cybersecurity is changing, the US Senate unanimously passed legislation on March 1, 2022 that would usher in sweeping changes to the federal legal landscape relating to cybersecurity and cyber incident response. Prior versions of this and related legislation failed to win passage in recent years.

The Strengthening American Cybersecurity Act combines pieces of three bills: Title I, the Federal Information Security Modernization Act; Title II, the Cyber Incident Reporting Act; and Title III, the Federal Secure Cloud Improvement and Jobs Act. This alert focuses on the proposed cyber incident reporting obligations under Title II.

Title II – named the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the Act) – would require critical infrastructure entities and civilian federal agencies to report any "substantial cyber incident" within 72 hours and any ransomware payment within 24 hours to the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA). Entities would be required to preserve – and, in certain cases, to produce to CISA – data relevant to the cyber incident or ransom payment. Supplemental reports would be required until the incident is resolved if substantially new or different information becomes available or if a covered entity makes a ransom payment after it has already submitted its initial report.

The Act would apply to entities "in a critical infrastructure sector, as defined in Presidential Policy Directive 21," that fall within the definition of "covered entity," to be established by CISA rulemaking. As detailed on CISA's website, there are 16 federally designated sectors of critical infrastructure, including the financial, communications, information technology, energy, healthcare, food, water and transportation sectors.

Though specific reporting requirements will be established by CISA rulemaking, the Act would establish certain minimum reporting requirements:

- A description of the cyber incident, including:
  - Identification and description of the function of affected systems, networks and devices
  - Description of the unauthorized access
  - Estimated date range of the incident
  - Impact to operations
- A description of the vulnerabilities exploited and the security defenses that were in place, as well as the tactics, techniques and procedures used to perpetrate the cyber incident
- Any identifying or contact information related to each actor reasonably believed to be responsible for such cyber incident
- The categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person
- The name and other information that clearly identifies the covered entity impacted by the cyber incident and
- Contact information for the covered entity.

In the case of a ransomware payment, to the extent applicable and available, reports must include:

- A description of the ransomware attack, including the estimated date range of the attack
- A description of the vulnerabilities, tactics, techniques and procedures used to perpetrate the ransomware attack
- Any identifying or contact information related to the actor(s) reasonably believed to be responsible for the attack
- The name and other information that identifies the covered entity that made the ransom payment
- Contact information for the covered entity
- The date of the ransom payment
- The ransom payment demand, including the type of virtual currency or commodity requested
- The ransom payment instructions and
- The amount of the ransom payment.

The Act includes significant enforcement mechanisms and penalties for non-compliance with reporting obligations. CISA would be empowered to request or subpoena information from covered entities, with civil enforcement of subpoenas by the Justice Department. Non-compliance with a subpoena would be punishable by contempt of court, and CISA would be statutorily authorized to share information and make referrals to the Department of Justice or appropriate federal agencies for criminal prosecution and/or regulatory enforcement action.

A covered entity that submits compliant reports to CISA would be entitled to certain protections under the Act, including those available under the Cybersecurity Information Sharing Act of 2015. Covered entities would be immune from any civil suit based on the CISA reporting. Regulatory agencies could not use information obtained solely through CISA reporting in enforcement actions against the covered entity. Such information also would be protected as "commercial, financial and proprietary information of the covered entity," would not be subject to public access laws and would maintain any legally privileged status.

Other portions of the Strengthening American Cybersecurity Act would significantly update existing federal cybersecurity laws relating to federal agencies and government contractors. Title I would modernize the Federal Information Security Modernization Act to improve the coordination and communication between federal agencies. The new legislation would also require those agencies to share cyber incident information with the CISA, which would play a central statutory role in inter-agency cybersecurity coordination.

Lastly, Title III of the bill would authorize the Federal Risk and Authorization Management Program (FedRAMP) to ensure federal agencies can efficiently and securely adopt cloud-based technologies to improve government operations. Such authorization would last for five years.

The bill now goes to the House for consideration, and some significant issues – most notably, the opposition of the Justice Department and FBI to the bill – remain to be resolved. However, it is likelier than ever that a broad federal cyber incident notification requirement will be enacted into law in the near future. If this is the case, critical infrastructure entities will need to adjust their incident response plans to an early and substantial disclosure process that will likely have a significant impact on their overall response to cyber incidents and ransomware attacks.

AUTHORS

Andrew Serwin
Partner
San Diego (Golden Triangle) | T: +1 858 677 1400
andrew.serwin@dlapiper.com

Deborah R. Meshulam
Partner
Washington, DC | T: +1 202 799 4000
deborah.meshulam@dlapiper.com

Edward J. McAndrew
Partner
Wilmington | T: +1 302 468 5700
Washington, DC | T: +1 202 799 4000
ed.mcandrew@dlapiper.com

Leila Javanshir
Associate
Seattle | T: +1 206 839 4800
Leila.Javanshir@dlapiper.com