Data Privacy and Cybersecurity

United States Senate and Transportation Security Administration Take Steps Toward Expanding Cybersecurity Requirements

By: Shoba Pillay, David Bitkower, Aaron R. Cooper, and Ashwini Bharatkumar

Last week, the United States Senate and the Transportation Security Administration (TSA) each took steps toward expanding cybersecurity requirements for private sector entities. In the US Senate, a bipartisan group of 15 Senators led by Mark Warner (D-VA), Marco Rubio (R-FL), Susan Collins (R-ME)—respectively the Chairman, Vice Chairman, and a senior member of the Select Committee on Intelligence—introduced the Cyber Incident Notification Act of 2021. Meanwhile, TSA issued its second Security Directive since the Colonial Pipeline ransomware attack, setting forth cybersecurity requirements for critical pipelines. These developments signal continuing appetite in Congress and in the Executive Branch to move beyond voluntary guidelines and establish new rules of the road on cybersecurity and incident reporting in key sectors.

Cyber Incident Notification Act of 2021

The proposed Cyber Incident Notification Act of 2021 would create new mandatory reporting obligations for private sector and federal government entities that experience a cybersecurity intrusion. It directs the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to develop "Cyber Intrusion Reporting Capabilities," or capabilities to securely and confidentially collect notifications about cybersecurity intrusions from federal agencies and private sector entities covered by the statute.

Under the proposed legislation, a covered entity or federal agency that discovers a cybersecurity intrusion or potential cybersecurity intrusion must notify CISA within 24 hours of confirming the intrusion or potential intrusion. If the discovering entity or agency is subject to other, more stringent federal reporting requirements, then it may have less than 24 hours to report the intrusion. Until an incident is mitigated or fully investigated, the discovering entity or agency must provide cybersecurity threat information updates to CISA within 72 hours of any discovery of new information. The bill contemplates—but leaves to CISA—the establishment of notification obligations for cybersecurity intrusions of which a federal agency or covered entity is *aware*, but which do not directly impact that agency's or entity's information systems. While the legislation, as drafted, leaves much to DHS rulemaking, including specification of the entities covered by the proposed statutory provisions, it establishes certain minimum requirements for any rules to be promulgated by DHS.

For instance, unlike the May 12, 2021 Executive Order on Improving the Nation's Cybersecurity (see Jenner & Block's client alert issued on the Executive Order), the proposed legislation calls upon CISA to establish cyber intrusion reporting requirements applicable, at minimum, to federal contractors, owners or operators of critical infrastructure, and nongovernmental entities providing cybersecurity incident response services. The bill also calls upon CISA to establish capabilities to accept cybersecurity notifications from *any* entity, not only those covered by the Act. The bill requires CISA to define criteria according to which Sector Risk Management Agencies or other federal agencies must submit cybersecurity notifications pertaining to covered entities in their sectors. [1]

While the bill focuses on cybersecurity intrusions carried out by nation-states or transnational crime groups, or which otherwise have national implications, it also covers any cybersecurity intrusion involving ransomware.

In addition to enabling "timely Federal Government awareness of cyber intrusions that pose a threat to national security," the bill seeks to "make appropriate, actionable cyber threat information available to the relevant government and private sector entities, as well as the public." [2] The bill directs CISA to define the scope and parameters of such information sharing.

At the same time, the bill includes liability protections and restrictions on the use of information shared in cybersecurity notifications. In particular, shared information is exempt from FOIA disclosure and state, tribal, and local disclosure requirements. Further, shared information is inadmissible as evidence in civil or criminal actions, and only Congress can subpoena such information.

The proposed legislation features enforcement mechanisms that vary by entity type: federal contractors may face removal from contracting schedules, other entities may face financial penalties, and federal agencies may face referral to their respective inspectors general for failure to comply with the statute.

TSA Pipeline Security Directive

TSA continues to leverage its authority over national pipeline security to advance new cybersecurity requirements. Under that authority, TSA issued last week's Security Directive requiring owners and operators of TSA-designated critical pipelines that transport hazardous liquids and natural gas to implement measures protecting against cyber intrusions. While the Directive remains largely confidential, likely in order to prevent disclosure to threat actors, TSA announced that the Directive mandates implementation of protections against ransomware attacks and other known threats, mandates development and implementation of cybersecurity contingency and recovery plans, and requires pipeline operators to complete cybersecurity architecture design reviews.

Last week's Security Directive follows on the heels of TSA's May 2021 Security Directive. The May 2021 Directive requires owners and operators of critical pipelines to report confirmed and potential cybersecurity incidents to CISA, designate a Cybersecurity Coordinator, and identify and report gaps in pipeline cybersecurity practices.

---

[1] A Sector Risk Management Agency (SRMA) is a federal agency identified by *Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience* as the federal government liaison for each of the 16 critical infrastructure sectors.

[2] Cyber Incident Notification Act of 2021, S.___, 117th Cong. (2021).

Contact Us

Shoba Pillay

spillay@jenner.com | Download V-Card

David Bitkower

dbitkower@jenner.com | Download V-Card

Aaron R. Cooper

acooper@jenner.com | Download V-Card

Ashwini Bharatkumar

abharatkumar@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower
Co-Chair
dbitkower@jenner.com
Download V-Card

Madeleine V. Findley
Co-Chair
mfindley@jenner.com
Download V-Card