WILMERHALE

Senate Omnibus Cybersecurity Bill Emphasizes Critical Infrastructure Protection, Information-Sharing

2012-02-14

Senators Joseph Lieberman (D-CT), Susan Collins (R-ME), Jay Rockefeller (D-WV), and Diane Feinstein (D-CA) today introduced a long-awaited omnibus cybersecurity bill promised last fall by Senate Majority Leader Harry Reid. The bill (S. 2105) would authorize the Department of Homeland Security (DHS) to identify and establish cybersecurity performance standards for "covered critical infrastructure," such as important energy, financial, telecommunications, and transportation systems or assets (Title I); would clarify the authority of owners of information systems to monitor and undertake "countermeasures" on their own systems and would create institutions and legal incentives for the sharing of cyber threat and response information among businesses and between businesses and the federal government (Title VII); and would strengthen the ability of the federal government to protect its own networks and centralize enhanced authority in DHS (Titles II and III). The Senate Homeland Security and Government Affairs Committee, led by Senator Lieberman as Chair and Senator Collins as Ranking Member, will hold a hearing on the bill on Thursday, Feb. 16 at 2:30 PM.[1]

Below we provide a title-by-title summary of the bill. The text of the bill and the section-by-section analysis provided by the committee can be found here and here. Committee-created flow charts explaining the process for designation of and establishment of cybersecurity standards for covered critical infrastructure can be found here and here. Our earlier report describing other cybersecurity bills being considered can be found here.

TITLE I: CRITICAL INFRASTRUCTURE

- Owners, not operators, of "covered critical infrastructure" would be responsible for complying with the new requirements (§ 101(b))
- DHS, after consultation with other federal agencies and private-sector actors, would have 90 days to assess the degree of cyber risks in different economic sectors containing critical infrastructure and establish a priority list of sectors requiring most urgent attention (§ 102)
- DHS would then be required, through a consultative process with other agencies and private-sector stakeholders, to designate "covered critical infrastructure" at the system and

asset level (§ 103(a))

- Systems or assets could be designated as "covered critical infrastructure" only if damage or unauthorized access to that system or asset could reasonably result in

  (i) the interruption of life-sustaining services, including energy, water, transportation, emergency services, or food, sufficient to cause –

  (aa) a mass casualty event that includes an extraordinary number of fatalities; or

  (bb) mass evacuations with prolonged absence;

  (ii) catastrophic economic damage to the United States including—

  (aa) failure or substantial disruption of a United States financial market;

  (bb) incapacitation or sustained disruption of a transportation system; or

  (cc) other systemic, long-term damage to the United States economy or

  (iii) severe degradation of national security or national security capabilities, including intelligence and defense functions (§ 103(b))

- Commercial information technology products, including both hardware and software, along with services provided in support of those products, could not themselves be designated as covered critical infrastructure, but assets or systems using such products could be designated (§ 103(b))
- DHS would be required to issue rules, within one year, establishing sector-specific cybersecurity performance requirements (§ 104); the requirements could not directly specify how particular hardware or software should run or require inclusion or exclusion of particular IT products. Owners of covered systems or assets would have to certify compliance annually or get third-party assessments of their compliance, and establish response plans and report on cybersecurity incidents. (§ 105) But

  - DHS would be required to establish a process by which an owner of a covered system or asset could show its cybersecurity was good enough to warrant exemption from the new requirements (§ 105)
  - DHS could determine that no new regulations are required if existing sector-specific regulations set sufficiently high requirements (§ 104(c))
  - The President could exempt parts of covered critical infrastructure if he determined that a sector-specific agency's requirements and enforcement mechanisms were sufficient to mitigate cyber risks (§ 104(f))
- Compliance with the new federal cybersecurity requirements would protect owners of

covered critical infrastructure from punitive damages in "any civil action for damages directly caused by an incident related to a cyber risk identified, so long as they are in compliance with the various cybersecurity requirements established under the Act" (§ 105(e))

- The new federal standards would preempt state or local laws or rules "that expressly require[] comparable cybersecurity practices to covered critical infrastructure" (§ 111)
- DHS would be permitted, in its discretion, to provide "technical assistance" to owners of covered critical infrastructure (§ 108)

TITLE II: FISMA REFORM

- Would shift responsibility for setting compulsory information security policies for non-national security federal systems, including information systems used or operated by a contractor on behalf of an agency, from OMB to DHS (amended 44 U.S.C. § 3553)
- Would shift authority to issue binding "information security standards" for non-national security federal systems from OMB to the Department of Commerce (amended 40 U.S.C. § 11331)
- Would authorize DHS, notwithstanding any other law and in response to a known or reasonably suspected information security threat, to monitor, retain and disclose information from non-national security federal systems and to deploy "associated countermeasures" to protect those systems; if information acquired through this program reveals evidence that a crime has been, is being, or is about to be committed, it could, with the approval of the Attorney General, be shared with law enforcement (amended 44 U.S.C. § 3553(d))
- Would authorize DHS, in response to a known or reasonably suspected information security threat, to order agency officials to take lawful protective measures on non-national security federal systems, including on contractors' systems owned or operated on behalf of the agency (amended 44 U.S.C. § 3553(e))
- Would require agencies to develop and implement cybersecurity programs "for the information and information systems that support the operations and assets of the agency, including those provided or managed by . . . [a] contractor or other source" (amended 44 U.S.C. § 3554(b))

TITLE III: CONSOLIDATION OF FEDERAL CYBERSECURITY FUNCTIONS

- Would establish within DHS a National Center for Cybersecurity and Communications, with a presidentially appointed Director, which would take over the functions of the National Cyber Security Division, the Office of Emergency Communications, and the National Communications System and would be responsible for coordinating cyber threat and response information-sharing among federal agencies and for overseeing the national security and emergency communications infrastructure

TITLE IV: EDUCATION, RECRUITMENT, AND WORKFORCE DEVELOPMENT

- Would authorize agencies, including DHS, National Science Foundation, Office of

Personnel Management (OPM), and National Institute of Standards and Technology, to establish programs related to cybersecurity education, hiring, scholarships, and awareness (§§ 402-408)

- Would require DHS, in coordination with the Commerce Department, to develop programs to recognize products, services, and companies that meet the highest cybersecurity standards (§ 402)
- Would require OPM to establish a cybersecurity curriculum for all federal employees and contractors engaged in "design, development, or operation" of federal information infrastructure (§ 407)

TITLE V: RESEARCH AND DEVELOPMENT

- Would authorize development of cybersecurity research and development programs by the Office of Science and Technology Policy and DHS (§§ 501 and 502)

TITLE VI: FEDERAL ACQUISITION RISK MANAGEMENT STRATEGY

- Would require DHS to develop an acquisition risk management strategy "to ensure, based on mission criticality and cost effectiveness, the security of the Federal information infrastructure" (§ 601)
- Would amend laws governing federal acquisition of information technology (Clinger-Cohen Act) to enhance consideration of information security in federal acquisition programs (§ 602)

TITLE VII: INFORMATION-SHARING, MONITORING AND COUNTERMEASURES

Monitoring and Countermeasures:

- Notwithstanding a variety of federal surveillance laws, would authorize private-sector entities to monitor their own information systems or, upon request, information systems belonging to third parties (§ 701(1),(2))
- Notwithstanding a variety of federal surveillance laws, would authorize private-sector entities to deploy countermeasures to protect their information systems or, upon request, information systems belonging to third parties (§§ 701(3),(4))

Voluntary Information Sharing Among Private Entities:

- Would empower private entities, notwithstanding any other provision of law, to share and receive indicators of cybersecurity threats, provided the entities do not use the information to gain a competitive advantage and take reasonable steps to protect personally identifying information about individual persons (§ 702)

Cybersecurity Exchanges:

- Would create "cybersecurity exchanges" as clearinghouses for government and private-sector entities to share cybersecurity threat information (§ 703)
- Would requires DHS to create procedures for (a) designating cybersecurity exchanges, (b)

facilitating sharing of classified and non-classified information, and (c) certifying private entities capable of receiving classified cybersecurity information (§ 703)

- Notwithstanding any other provision of law, would authorize private-sector entities to share cybersecurity threat information with a cybersecurity exchange (§ 704)
- Would make cybersecurity exchanges that receive information from the private sector subject to privacy and civil liberties guidelines and would permit them to use or retain the information only to protect information systems (§ 704)

Liability Protection:

- Would bar state or federal causes of action based on (a) cybersecurity monitoring activities authorized by the Act, or (b) sharing of cybersecurity threat information with a cybersecurity exchange, certain critical infrastructure entities, or any private entity so long as the information was also shared with a cybersecurity exchange (§ 706)
- Would make good-faith belief that monitoring or information-sharing activities were authorized by the Act a complete bar to civil or criminal liability (§ 706)

Preemption:

- Would preempt all state or local laws that regulate cybersecurity activities authorized by the Act or that regulate the acquisition, use, dissemination or disclosure of communications in a manner that is inconsistent with the Act (§ 706)

TITLE VIII: PUBLIC AWARENESS REPORTS

- To increase public awareness of the scope of cyber threats facing the country and the ways in which our national and economic security are threatened, would require a number of annual reports to Congress:
  - *Federal Cyber Intrusions*. DHS to issue report summarizing major cyber incidents against civilian government networks, while the Defense Department is to issue a report summarizing such incidents on military networks (§ 802)
  - *Cyber Crime*. The Attorney General and FBI Director to issue a report describing investigations and prosecutions relating to cybercrime (§ 803)
  - *Improving Critical Infrastructure Security*. DHS and the National Research Council to issue a report on constitutionally sound technical options available for improving critical infrastructure network security (§ 804)
  - *Federal Courts*. The Attorney General to issue a report on whether the federal courts are able to provide timely relief in matters relating to cybercrime (§ 805)
  - *Public Awareness*. DHS to issue a report on impediments to better informing the public about cybersecurity (§ 806)
  - *Electric Grid*. DHS, in consultation with the Secretary of Defense and the Director of National Intelligence, to issue a report on options to prevent and respond to a cyber attack on the U.S. electric grid (§ 807)

TITLE IX: INTERNATIONAL COOPERATION

- Would express the sense of Congress that achieving U.S. objectives relative to cyberspace should be an integral part of U.S. diplomatic efforts (§ 903)
- Would authorize the Secretary of State to designate a senior official to coordinate U.S. diplomatic engagement relative to cybersecurity, and would call on the Secretary to provide an annual briefing on trends in cybercrime (§§ 904-905)

---

[1] The hearing can be watched live at: www.hsgac.senate.gov/hearings/securing-americas-future-the-cybersecurity-act-of-2012.

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

David W. Ogden

PARTNER

Chair, Government and Regulatory Litigation Practice Group

david.ogden@wilmerhale.com

+1 202 663 6440

David J. Ross

PARTNER

Chair, International Trade, Investment and Market Access Practice Group

david.ross@wilmerhale.com

+1 202 663 6515

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195