Senate To Consider Compromise Cybersecurity Legislation

2012-07-23

In what may prove to be a final attempt to secure passage of substantial cybersecurity legislation in the current session of Congress, Senators Joe Lieberman (D-CT) and Susan Collins (R-ME) introduced a revised version of their omnibus cybersecurity bill last Thursday.[1] The bill (S. 3414), which could be brought before the Senate as early as this week, includes the following main elements.

- **Critical Infrastructure** (Title I): Instead of authorizing the Department of Homeland Security (DHS) to establish mandatory cybersecurity performance requirements for systems in critical infrastructure sectors, the new bill would establish a National Cybersecurity Council of federal agencies chaired by DHS that, in collaboration with private sector owners and operators, would “coordinate the adoption of private-sector recommended voluntary outcome-based cybersecurity practices” with an array of public and private stakeholders. (§ 101(a)(3)) But sector-specific agencies would be permitted to adopt the recommended practices as mandatory requirements if their pre-existing authorities would authorize them to do so. (§ 103(g)) Companies receiving certification of compliance with the cybersecurity practice standards would gain various benefits, including protection from punitive damages in claims arising from cyber incidents. (§ 104(c))
- **Information-Sharing, Monitoring, and Countermeasures** (Title VII): Like the comparable portions of the earlier bill, these sections of the new bill would clarify the authority of owners of information systems to monitor and undertake "countermeasures" on their own systems (or to authorize others to do so) 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. But in response to concerns raised by privacy advocates, the new bill imposes clearer and tighter restrictions on the use of shared information: it provides expressly that private entities may use, retain, or further disclose shared cyber threat information solely for cybersecurity purposes (§ 702); while cybersecurity exchanges and federal entities would still be permitted to disclose shared information for certain law-enforcement purposes as well, those permissible law-enforcement grounds have been limited to information pertaining to cybersecurity crimes, imminent threats of death or serious bodily injury, and serious threats to minors (§ 703(g)(2)(A)); the lead federal cybersecurity exchange would have to be based in a civilian agency

(§ 703(c)); and individuals harmed by an intentional violation of these restrictions by a federal agency may sue the offending agency for damages (§ 704(g)7)).

- **FISMA Reform and Procurement** (Titles II and V): These portions of the bill are nearly unchanged from the earlier version. They would strengthen the ability of the federal government to protect its own networks and centralize enhanced authority in DHS. They would also enhance the ability of federal agencies to impose cybersecurity requirements on government contractors.

More Detailed Description[2]

The bill has seven titles. It does not include a federal data breach notification requirement.

Critical Infrastructure (Title I).

- The newly established National Cybersecurity Council would be chaired by Secretary of DHS and would include presidentially-appointed representatives from the Departments of Commerce, Defense, and Justice, the intelligence community, and sector-specific Federal agencies, which would likely include, for example, the Departments of the Treasury and Transportation, the Nuclear Regulatory Commission, and others. (§ 101)
- Within 180 days of enactment, "a member agency"—likely DHS—would be required to undertake an inventory of cyber risks to identify infrastructure sectors where enhanced security measures are most urgently needed. (§ 102) Within 180 days of enactment, the Council, in consultation with the private sector, would be required to identify categories of critical cyber infrastructure warranting issuance of cybersecurity performance standards. Those standards would draw on the work of the existing Critical Infrastructure Partnership Advisory Council and its sector-specific committees.[3] The Council would have to notify both Congress and owners and operators of potentially affected assets. Congress would have 60 days to review and disapprove any of the Council's determinations. (§ 102)
- Within one year of enactment, the Council would be required to adopt recommended cybersecurity practices by sector, based on recommendations from sector-specific councils of private companies and security experts. (§ 103) The standards must be technology neutral and must not require use of any particular IT product or service. (§ 103(f))
- Companies that are certified as complying with the cybersecurity practices adopted by the Council
  - shall be immune from punitive damages in any action for damages "directly caused by an incident related to a cyber risk" identified by the Council in its inventory of cyber risks

- shall be entitled to expedited security clearances for employees
- shall be entitled to prioritized technical assistance
- shall receive, to the extent practicable, real-time cyber threat information
- shall receive public recognition

The Council and the Federal Acquisition Regulatory Council shall conduct a study considering whether a federal procurement preference should be established for certified companies. (§ 104)

Information-Sharing, Monitoring, and Countermeasures (Title VII).

Monitoring and Countermeasures:

- Notwithstanding certain federal surveillance laws, would authorize private-sector entities to monitor their own information systems or, upon request, information systems belonging to third parties (§ 701)
- 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)

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 use the information only for cybersecurity purposes and 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; that protection would be eliminated if the party knowingly or acting in gross negligence violated the title or regulations issued under it (§ 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)

FISMA Reform and Procurement (Titles II, V). This part of the bill is nearly unchanged from the earlier version.

- 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))
- 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)

- 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

R & D, Workforce, International Cooperation (Titles III, IV, VI). These sections are unchanged from the earlier version of the bill.[4]

Prospects

The fate of the bill remains uncertain. The Obama Administration continues to press for action based on national security concerns, most strikingly in a recent *Wall Street Journal* op-ed piece by the President himself.[5]The improved privacy protections in the new bill have won favorable comments from some groups that had raised concerns about other bills.[6] But it remains unclear whether the shift in the direction of voluntary rather than mandatory cybersecurity standards for critical infrastructure will be sufficient to win the support of enough Republican Senators to get past the 60-vote hurdle now placed in front of every action in the Senate.[7] If the cybersecurity title still proves controversial, there might also be an attempt to move forward just on information-sharing and FISMA reform, two areas where the House has already passed its own bills.[8] Final passage would then require reconciling the House and Senate versions.

---

[1] For our description of the earlier bill go to: http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=10038. The other lead sponsors are Senators Tom Carper (D-DE), Jay Rockefeller (D-WV), and Diane Feinstein (D-CA).

[2] The bill text as well as the summary and section-by-section analysis prepared by the Senate Homeland Security and Government Affairs Committee can be found here: http://www.hsgac.senate.gov/issues/cybersecurity.

[3] A description of the Critical Infrastructure Partnership Advisory Council and its work can be found here: http://www.dhs.gov/files/committees/editorial_0843.shtm.

[4] For a description of these provisions see our earlier alert: http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=10038.

[5] The op-ed can be found here: http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html?KEYWORDS=Obama+cybersecurity.

[6] For a discussion see: http://thehill.com/blogs/hillicon-valley/technology/239295-privacy-advocates-

satisfied-with-liebermans-cybersecurity-rewrite.

[7] For an earlier account of the legislative debate go to: http://www.wilmerhale.com/-/media/files/WilmerHale_Shared_Content/Files/Editorial/Publication/Can Cybersecurity Legislation Overcome Partisan Divide.pdf.

[8] The House-passed bills, H.R. 3523, the Cyber Intelligence Sharing and Protection Act, and H.R. 4257, the Federal Information Security Amendments Act of 2012, can be found here and here.

Authors

Jamie Gorelick

PARTNER

Chair, Regulatory and Government Affairs Department

jamie.gorelick@wilmerhale.com

+1 202 663 6500

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195