Akin®

Cybersecurity Activity During Last Gasp of Lame-Duck Congress

Dec 12, 2014

Reading Time : **3 min**

By: Francine E. Friedman, Matthew Thomas (Senior Public Policy Specialist), David S. Turetsky, Visiting Professor, College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University of Albany

On Wednesday, the Senate passed the National Cybersecurity Protection Act (S. 2519, also sponsored by Sen. Carper), which is the Senate's version of a House-passed bill, the National Cybersecurity and Critical Infrastructure Protection Act (NCCIP). The bill officially authorizes the already-existing cybersecurity information-sharing hub at DHS. Known as the National Cybersecurity and Communications Integration Center, the hub receives cyber information from multiple government and industry sources, then disseminates information on specific cyber threats back to those partners. The Senate's measure is a slimmed-down version of the House bill, leaving out many of the specifics on the information exchange between the public and private sector. The House passed the bill on Thursday, and it now also heads to the president's desk for signature.

Further, the Senate also passed H.R. 2952 on December 10, 2014. Originally titled and passed by the House as the Critical Infrastructure Research and Development Advancement Act of 2014, the Senate approved an amendment by Sen. Carper to require the Secretary of Homeland Security to assess the cybersecurity workforce of DHS and develop a comprehensive workforce strategy. The bill was also passed by the House on Thursday and now heads to the president's desk, along with the other two previously mentioned above.

Additionally, the Homeland Security Cybersecurity Workforce Assessment Act, which was included in the Border Patrol Agent Pay Reform Act of 2014 (S. 1691), was passed by the House on Wednesday. Though the bill is primarily about compensating border patrol agents, when it passed the Senate in September, lawmakers added provisions to the bill incorporating Sen.

Carper's DHS Cybersecurity Workforce Recruitment and Retention Act of 2014. The provisions would give DHS special flexibility to recruit and pay cyberprofessionals. That bill also now awaits President Obama's signature.

On Thursday evening, the House and Senate passed S. 1353, the Cybersecurity Act of 2013. The bill, sponsored by outgoing Senate Commerce Committee Chairman Rockefeller Jay Rockefeller (D-WV), amends the National Institute of Standards and Technology Act to permit the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), to facilitate and support the development of a voluntary, industry-led set of standards and procedures to reduce cyberrisks to critical infrastructure. Under the standards, NIST would be directed to "include methodologies to mitigate impacts on business confidentiality, protect individual privacy and civil liberties" when coordinating and sharing information with private owners and operators of critical infrastructure. It should be noted that the term "critical infrastructure" is not defined within the context of the bill. Further, the bill would require the development of a national cybersecurity research and development plan, direct the departments of Commerce and Homeland Security to sponsor competitions and other challenges to recruit cybersecurity workers, and direct NIST to continue efforts to improve public awareness of cybersecurity risks.

Finally, the Senate Banking Committee held a hearing Wednesday about how to prevent cyber-attacks and handle data breaches facing the financial-services industry. In submitted testimony, the Securities Industry and Financial Markets Association urged lawmakers to pass the Cybersecurity Information Sharing Act of 2014 (knowas CISA, or CISPA in the House), since the bill would be the best way "for Congress to engage more productively in this effort to improve our cybersecurity." The hearing featured testimony from representatives of the Treasury, DHS, Office of the Comptroller of Currency, the Secret Service and the Federal Bureau of Investigation. The Senate is not expected to pass CISA before the end of the lame-duck session.

In sum, it is likely that five bills pertaining to federal information security (S. 2521), limited cyber information sharing (S. 2519), critical infrastructure cybersecurity, R&D and workforce development, and the hiring of federal cybersecurity professionals will all become law before the end of the year. However, Congress has yet to reach an agreement on how to create a framework for comprehensive cooperation and collaboration on cybersecurity information sharing with the private sector, and such legislation is unlikely to pass in the waning days of the 113th Congress.

Categories

Cybersecurity, Privacy & Data Protection

Policy & Regulation