HUNTON& WILLIAMS

Byline

December 18, 2014

Congress Surprisingly Passes Several Cybersecurity Bills

by Paul M. Tiao and Eric M. Hutchins

Published in Law360

In a flurry of activity on cybersecurity in the waning days of the 113th Congress, Congress unexpectedly approved, largely without debate and by voice vote, a series of cybersecurity bills that: (1) clarify the role of the U.S.Department of Homeland Security in private-sector information sharing, (2) codify the National Institute of Standards and Technology's cybersecurity framework, (3) reform oversight of federal information systems, (4) enhance the federal government's cyber-security workforce recruitment and retention, and (5) assess the federal government's cybersecurity workforce. Congress also included cybersecurity-related provisions in the omnibus appropriations bill.

The president has or is expected to sign each of these bills. This legislation — summarized and outlined below — is somewhat limited as it largely codifies agency activity already underway or requires reports to Congress. Notably, Congress did not pass the information-sharing liability protections that were included in other recent unsuccessful cybersecurity bills like the House Cyber Intelligence Sharing and Protection Act ("CISPA") or Senate Cyber Information Sharing Act ("CISA"). However, with many observers expecting little legislative activity on cybersecurity before the end of the year, that Congress has passed and sent major cybersecurity legislation to the White House for the first time in 12 years may signal Congress' intent to address systems protection issues more thoroughly in the next Congress.

S. 2519, "National Cybersecurity Protection Act of 2014"

Highlights

- Codifies DHS's National Cybersecurity and Communications Integration Center ("NCCIC") as a "federal civilian interface" to provide federal and non-federal entities "shared situational awareness" to address cybersecurity risks, coordinate the sharing of cybersecurity information, conduct and share analysis, and provide technical assistance and recommendations on network security.

- Directs that NCCIC should include members of: sector-specific agencies, law enforcement, the intelligence community, state and local governments, information-sharing and analysis organizations, and owners and operators of critical information systems.

- Directs DHS to make available the process to apply for security clearances to those involved in public-private information sharing.

- Makes clear that nothing in the act shall be construed as providing new regulatory authority.

Analysis

On Dec. 11, the House passed Senate legislation codifying DHS' NCCIC and making it the federal government's central hub for public-private cybersecurity information sharing. That bill, the National Cybersecurity Protection Act of 2014, is the Senate version of similar legislation passed by the House this past summer. The legislation now heading to the president is a pared-down version of the original House bill.

Notably, industry has been calling for legal protections for companies engaged in sharing information with the government, similar to provisions that were included in CISPA and CISA. Nevertheless, the legislation passed by Congress lacks an extensive legal safe harbor for information sharing. In addition, this version of the legislation lacks language from the original House bill that would explicitly allow application of the SAFETY Act — which provides liability protections through DHS for anti-terrorism technologies — to cybersecurity products and services (it should be noted that DHS already applies the SAFETY Act to cybersecurity products and services).

In sum, while passage of this legislation is an important, even stunning, step forward on cybersecurity policy, liability concerns will continue to hamper cybersecurity information sharing.

S. 1353, "Cybersecurity Enhancement Act of 2014"

Highlights

- Specifies that act does not confer any new regulatory authority.

- Formally codifies the ongoing NIST process for developing industry-driven, consensus-based, voluntary cybersecurity standards for critical infrastructure.

- Directs NIST and the National Science Foundation ("NSF") to plan for and encourage research into cybersecurity.

- Directs NIST, NSF, DHS, the U.S. Department of Commerce, and Office of Management and Budget to encourage programs to develop and retain cybersecurity professionals.

- Directs NIST to develop programs to raise public awareness of cybersecurity.

- Directs NIST to ensure coordination of federal agencies in the development of international technical standards relating to cybersecurity.

Analysis

Late in the evening on Dec. 11, the House and Senate passed the Cybersecurity Enhancement Act of 2014, which authorizes NIST to facilitate and support the development of voluntary, industry-led cyber standards and best practices for critical infrastructure. The bill essentially codifies the ongoing process begun earlier this year through which the NIST cybersecurity framework was developed. That process remains voluntary under the bill, with no new regulatory authority added to the framework. The bill also authorizes the federal government to support research, raise public awareness of cyber risks, and improve the nation's cybersecurity workforce.

S. 2521, "Federal Information Security Modernization Act of 2014"

Highlights

- Codifies action by the White House to elevate DHS' role in administering the implementation of information security policies and practices in civilian federal information systems, while retaining OMB's role in overseeing the security of federal government information systems in general.

- Describes the information security responsibilities of OMB, DHS and all other federal agencies.

- Eliminates requirement that federal agencies file annual checklists that show steps they have taken to secure systems and instead requires that agencies "continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement."

- Requires agencies to notify Congress of security incidents within seven days of discovery.

Analysis

On Dec. 8, the Senate passed by voice vote and without debate the Federal Information Security Modernization Act of 2014, which overhauls the 12-year-old Federal Information Security Management Act ("FISMA"). This legislation replaces FISMA's current requirement that agencies file annual checklists that show the steps they have taken to secure their information technology systems and puts DHS in charge of "compiling and analyzing data on agency information security" and helping agencies install tools "to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement."

DHS had been increasingly taking such a role already and similar legislation passed the House of Representatives in April 2013. However, that bill was subject to jurisdictional disagreements between the House Homeland Security and Oversight and Government Reform Committees.

Surprisingly, Oversight and Government Reform Chairman Rep. Darrell Issa, R-Calif., whose chairmanship of the committee will end in the next Congress, dropped objections to the Senate's FISMA reform bill and the House passed it on Wednesday evening by voice vote.

S. 1691, "DHS Cybersecurity Workforce Recruitment and Retention Act of 2014" and "Homeland Security Cybersecurity Workforce Assessment Act" (Attached to the Border Patrol Agent Pay Reform Act)

DHS Cybersecurity Workforce Recruitment and Retention Act of 2014 Highlights

- Authorizes DHS to establish cybersecurity positions in DHS as positions in the excepted service (not subject to the regular federal pay scale), and sets forth DHS' authority to make appointments, fix pay rates, and provide incentives and allowances for such positions.

- Requires a report to Congress concerning such positions.

Homeland Security Cybersecurity Workforce Assessment Act Highlights

- Requires federal agencies to identify and code cybersecurity workforce positions within the agency.

- Directs each agency head, to submit a report identifying critical needs in the agency's cybersecurity workforce.

- Requires OMB to provide guidance to agencies on identifying critical cybersecurity workforce needs.

H.R. 2952, "Cybersecurity Workforce Assessment Act"

Highlights

- Directs DHS to assess the department's cybersecurity workforce including the readiness of DHS, where such positions are located in DHS and throughout the federal government, job training in the government cybersecurity workforce, and cybersecurity workforce vacancies.

- Directs DHS to develop comprehensive workforce strategy to enhance the readiness, capacity, training, recruitment and retention of the cybersecurity workforce of DHS.

- Requires DHS to develop a plan for a Cybersecurity Fellowship Program to offer tuition payment for cybersecurity specialists who agree to work for DHS.

H.R. 83, Consolidated and Further Continuing Appropriations Act, 2015

Highlights

- Sec. 515: Prohibits Departments of Commerce and Justice, the National Aeronautics and Space, Administration, or the NSF from acquiring high-impact or moderate-impact information systems unless an assessment is conducted of any risk of cyberespionage or sabotage associated with the acquisition of such system from any country posing a cyber threat, including China.

- Explanatory Statement (Division E): Directs the U.S. Securities and Exchange Commission to submit a report to Congress on efforts to modernize disclosure requirements, including an update on cybersecurity.

Analysis

The omnibus bill generally eases supply-chain reporting requirements on technology and software linked to the Chinese government. However, the bill requires that high-impact or moderate-impact information systems acquired by the federal government undergo analysis to identify risks of cyberespionage.

General Analysis of Legislative Activity

This spate of cybersecurity legislation is more limited in scope than the measures that have been sought by the private sector. Indeed, rather than provide new cybersecurity tools, the bills approved by Congress largely make pre-existing actions official. Still, with the 113th Congress effectively ending last week, passage of any cybersecurity bills unexpectedly no less, at the same time that Congress feverishly worked to avert another government shutdown unexpectedly is very surprising, particularly given the general inability of Congress over the past two years to move bills to the president.

This legislative activity on cybersecurity indicates a seriousness by policymakers to confront issues vital to information systems protection. Having been largely inactive for the past four years, the Senate now appears to be scrambling to set its mark on future cybersecurity policy. For its part, the House's sudden action on Senate cybersecurity bills may point to a willingness by House committees to overcome internal jurisdictional disagreements that have hampered similar legislation in the past.

The significance here is the recognition by Congress that legislative success now builds momentum for systems-protection policies in the next Congress, such as information-sharing liability protection or even data breach legislation. How the 114th Congress confronts those issues is important to businesses seeking to enter public-private partnerships and information-sharing agreements; but, that Congress has done anything at all here greatly increases the possibility that it will take action on cybersecurity in the next two years.

