Akin Gump
STRAUSS HAUER & FELD LLP

Cybersecurity, Privacy & Data Protection Alert

December 21, 2017

Key Points

- The U.S. House of Representatives passed a major cybersecurity bill last week that could cause widespread changes in one of the nation's key cybersecurity agencies if a similar bill is adopted by the Senate. The bill is the latest sign of growing congressional concern with, and attention to, cybersecurity issues.
- If adopted, the bill would centralize authority and responsibility for cybersecurity at DHS within a single operational agency. The bill would elevate NPPD at DHS to an operational agency and rename it CISA. CISA would become a stand-alone agency within DHS. The bill would centralize various cybersecurity-related responsibilities that are now dispersed throughout the DHS hierarchy under the control of CISA, streamlining decisionmaking.
- The bill is the latest in a string of congressional efforts to legislate reforms to the agencies and departments responsible for protecting the nation's cybersecurity and critical infrastructure. That the bill passed the House may be a sign of a growing willingness among lawmakers to turn to legislative fixes in the face of increasing numbers ofcyberattacks. Whether the Senate agrees remains to be seen.

New House Bill Signals Potential for Major Changes in DHS Cybersecurity Efforts

Overview

On December 11, the House passed the Cybersecurity and Infrastructure Security Agency Act of 2017 (the "Bill") (H.R. 3359), which amends the Homeland Security Act of 2002 to create a new operational agency, the Cybersecurity and Infrastructure Security Agency (CISA), with responsibility for protecting the nation's cybersecurity and critical infrastructure. The Bill was introduced by Rep. Michael McCaul (R-TX), Chairman of the House Committee on Homeland Security, and passed with bipartisan support. It is intended to streamline the U.S. Department of Homeland Security's (DHS) ability to respond to, and protect against, the increasing number of cyberattacks taking place within the United States. By making CISA an operational agency, the Bill would put it on the same footing as other major federal protection and response agencies, such as the Federal Emergency Management Agency. It would also consolidate under one roof an array of cybersecurity and infrastructure protection responsibilities that are now

scattered throughout DHS. Proponents of the Bill say that, by doing so, it would enable CISA to more effectively execute cybersecurity- and critical-infrastructure-related authorities than the current National Protection and Programs Directorate (NPPD). There is no Senate counterpart to the Bill yet.

Background

NPPD was established in 2007 and is led by the Under Secretary for National Protection and Programs. It does not have the status as a full operational agency within DHS. There are five sections in the NPPD: (1) the Federal Protective Service, (2) the Office of Biometric Identity Management, (3) the Office of Cybersecurity and Communications, (4) the Office of Cyber and Infrastructure Analysis, and (5) the Office of Infrastructure Protection.

NPPD and DHS more generally have been criticized in the past for failing to properly protect the nation's cybersecurity. Some of this criticism arose from the scattering of cybersecurity oversight and responsibilities throughout DHS. At certain points, this resulted in different sections of DHS being responsible for overlapping tasks, or for some tasks being missed altogether. Because different agencies within DHS are accountable to different congressional oversight committees, this scattering also made it more difficult for congressional leaders to get the full picture on cybersecurity efforts.

The Bill is intended to better equip DHS and CISA to be flexible and responsive, and to centralize responsibility for quick decisionmaking and clear oversight. NPPD is said to support the new Bill and to have encouraged its passage.

Key Provisions of the Bill

If adopted, the bill would affect, among others, the following changes:

- Rename NPPD as CISA and make CISA its own operational agency. Within DHS, operational agencies are those stand-alone entities that together make up DHS (e.g., the U.S. Citizenship and Immigration Services or the Transportation Security Administration). This would provide CISA with increased independence and power.
- Direct that CISA be led by a Director of Cybersecurity and Infrastructure Security (the "Director") who would report directly to the Secretary of DHS. This would put the Director on par with other intra-DHS agency leaders. Proponents suggest that elevating leadership within CISA in this manner will help streamline decisionmaking and empower the Director to quickly escalate events and requests for assistance as needed.
- Task CISA and its Director with responsibility for, among other things, (1) leading cybersecurity and critical infrastructure security programs, including national cybersecurity asset response activities; (2) coordinating with federal and nonfederal entities (including internationally) to carry out cybersecurity and critical infrastructure activities; (3) carrying out the Secretary of DHS's responsibilities to secure federal information and information systems; (4) coordinating a national effort to secure and protect against critical infrastructure risks; (5) providing, upon request, analyses, expertise and technical assistance to critical infrastructure owners and operators; (6) developing, coordinating and

implementing comprehensive strategic plans for CISA and risk assessments by and for CISA; and (6) developing and utilizing mechanisms for collaboration within CISA's divisions and between CISA and other agencies.

- Mandate that the Director have a responsibility to report back to Congress on various issues and the overall work of CISA. This is intended to create greater accountability. The current head of NPPD is not required to report to Congress in the same manner.
- Include within CISA the following divisions: (1) the Cybersecurity Division, which would carry out activities related to the security of federal information and information systems; (2) the Infrastructure Security Division, which would direct the critical infrastructure security efforts at CISA, including carrying the Chemical Facilities Anti-Terrorism Standards Program and securing the handling of ammonium nitrate; and (3) the Emergency Communications Division, which would have the responsibilities of the prior Office of Emergency Communications. Each division would be led by an assistant director with powers specific to his or her role.
- Order that a Privacy Officer be employed by CISA to (1) ensure that the use of technologies by CISA supports, and does not erode, privacy protections; (2) ensure that personal information is handled properly; (3) evaluate legislative and regulatory proposals involving the collection, use or disclosure of personal information by CISA; and (4) conduct a privacy impact assessment of proposed CISA rules.

Moving Forward

On December 12, the Bill was received in the Senate and referred to the Committee on Homeland Security and Governmental Affairs. DHS Secretary Nielsen recently "urge[d] the Senate to pass similar legislation." (DHS Press Release (12/11/17) It remains to be seen whether the Senate will take up Secretary Nielsen's call. The recently passed Bill is similar to another piece of legislation pushed by Rep. McCaul during the last Congress. That bill was not taken up by the Senate. There is some fear that the current Bill will meet the same fate.

Even if the Senate does not act on the Bill, its passage marks an important development in the increasing willingness of Congress to try legislative fixes to the growing tide of cyber threats. DHS plays a critical role in protecting the nation's digital infrastructure, from digital election records to our digital health care systems. Given Rep. McCaul is Chairman of the House Committee on Homeland Security and his dedication to this issue, it is likely that another piece of similar legislation will be promoted next Congress if the Senate fails to act on this Bill.

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
nkohne@akingump.com
415.765.9505
San Francisco

Michelle A. Reed
mreed@akingump.com
214.969.2713
Dallas

Robert K. Huffman
rhuffman@akingump.com
202.887.4530
Washington, D.C.

James Romney Tucker Jr.
jtucker@akingump.com
202.887.4279
Washington, D.C.

Tom W. Davidson
tdavidson@akingump.com
202.887.4011
Washington, D.C.

Francine E. Friedman
ffriedman@akingump.com
202.887.4143
Washington, D.C.

Greg W. Guice
gguice@akingump.com
202.887.4565
Washington, D.C.

Diana E. Schaffner
dschaffner@akingump.com
415.765.9507
San Francisco