ML STRATEGIES

August Cybersecurity Update: Congress Finishes Up NDAA and Continues Work on Cybersecurity Bills

August 12, 2019 | | By **Christian Tamotsu Fjeld**, **Alexander Hecht**

As August recess gets underway for the House and the Senate, ML Strategies has prepared a summary of the status of this summer's key cybersecurity issues. ML Strategies will continue to track these and other cybersecurity priorities before Congress and the Administration through August and beyond.

House and Senate Language in the National Defense Authorization Act

The House and Senate have finalized their respective versions of the National Defense Authorization Act for Fiscal Year 2020 (NDAA). The NDAA now goes to conference, where final language will be hammered out. There are several key differences between the House and Senate versions on cybersecurity issues, but both the House and Senate bills would provide significant investments in cybersecurity and cyber operations, including funding to the U.S. Cyber Command.

The Senate bill, S. 1790, would require the Department of Defense's (DoD) Chief Information Officer and Chief Data Officer to develop and issue enterprise-wide strategy and implementing instructions for the transition of DoD data to the cloud, in accordance with the DoD-wide cloud strategy. The Senate bill would also require the Secretary of Defense to "reorient the Big Data Platform" to align with the DoD's Cyber Strategy by establishing a common baseline and security classification scheme for the collection, querying, analysis, and accessibility of metadata across the DoD's Information Network, in order to discover, track, and remediate cybersecurity threats.

The Senate version would also require the DoD to "streamline and digitize" its approach towards mitigating risks to the defense industrial base across the acquisition process. This would require a framework to mitigate the DoD's acquisition risk, including supply chain risks related to material sources and fragility, counterfeit parts, and cybersecurity of contractors. The Senate bill also authorizes three test networks for the testing and accreditation of cybersecurity products and services which feature cybersecurity processes, tools, and technologies that are appropriate for test purposes and representative of the processes, tools, and technologies that are widely used throughout the Department.

Section 853 of the House's version of NDAA, H.R. 2500, directs the Secretary to include security as a stated primary purpose of DoD acquisition and to appropriately revise all instructions, regulations, and directives to include this new purpose. Furthermore, this section establishes a risk certification protocol that requires the Vice Chief of an Armed Force to issue a written assessment of a DOD procurement that describes actions taken to mitigate potential vulnerabilities and certifies that the procurement will not interfere with military operations. DoD is required to report on its cybersecurity synchronization efforts across the defense industrial base, including a list of its cybersecurity compliance programs, the status of standards and cybersecurity policy creation, and deconfliction of policies. Section 853 addresses cybersecurity risks and supply chain vulnerability issues within the military by emphasizing the role of defense contractors when providing hardware, software, and supply chain services.

Both the House and Senate bills contain language to rein in foreign cybersecurity threats. The Senate version requires detailed reporting from the DoD to prevent transfers of sensitive technology to China or Russia, as well as reports on access to the Arctic. It also requires tighter screening of foreign scholars seeking visas to the United States. The House version requires an assessment of China's expansion of its surveillance state to protect American intellectual property.

House and Senate Committees Advance IoT Cybersecurity Bills

On June 12, the House Oversight and Reform Committee favorably reported by voice vote H.R. 1668, the IoT Cybersecurity Improvement Act of 2019. A week later, the Senate Homeland Security and Government Affairs Committee (HSGAC) favorably reported the Senate companion bill, S. 734. The bills are bipartisan: Reps. Kelly (D-IL) and Hurd (R-TX) introduced the House bill; Senators Warner (D-VA) and

Gardner (R-CO) introduced the Senate bill. Both H.R. 1668 and S. 734 were amended as they were reported out of their committees. While the texts of the underlying bills are identical, the amended versions reported out of each committee differ in their drafting. Nonetheless, the two bills retain their policy objectives.

The IoT Cybersecurity Improvement Act would promulgate standards for all IoT devices procured by the federal government. Specifically, the bills would direct the National Institute of Standards and Technology (NIST) to issue a report and issue guidelines on the secure development, identity management, patching, and configuration management of IoT devices. The bills would, in turn, further direct the Office of Management and Budget (OMB) to issue requirements consistent with NIST's work to all federal government agencies. OMB would review these requirements at least every five years, and all federally procured IoT devices would be required to comply with such standards. NIST would also be directed to work with cybersecurity researchers and private industry experts to develop and publish guidelines on coordinated vulnerability disclosure protocols to address vulnerabilities in federally procured IoT devices. OMB would, in turn, issue standards based on these guidelines and would require private contractors and vendors abide by these standards.

The IoT Cybersecurity Act has a good chance at becoming law. The full House is likely to take up the bill when Members return from the August recess. The fate of S. 734 in the Senate also looks promising given that the bill was reported out of HSGAC by voice vote en bloc with a slew of other non-controversial bills, including S. 1846, the State and Local Government Cybersecurity Act (see below). HSGAC's Chairman, Senator Johnson, is considered one of the more conservative Members of the Senate, as is Senator Paul (R-KY) who is also a Member of the committee and did not voice any objections. If prospects for passage in the Senate prove to be positive, the House and Senate will likely reconcile drafting differences between their versions of the amended bills in a "pre conference" setting in order to allow both the House and Senate to pass identical final bills for the President's desk.

S. 1846, the State and Local Government Cybersecurity Act of 2019

As noted above, at its June 19 mark-up, HSGAC also favorably reported S. 1846, the State and Local Government Cybersecurity Act of 2019, introduced by the Ranking Member, Senator Peters, and Senator Portman (R-OH). The bill would facilitate coordination between the Department of Homeland Security (DHS) and state and local governments to protect critical infrastructure. The bill would authorize DHS's National Cybersecurity and Communications Integration Center (NCCIC) to provide assistance to states and localities in the form of guidance and training, as well as access to improved security tools, policies, and procedures. S. 1846 also directs NCCIC to coordinate with DHS's Multi-State Information Sharing and Analysis Center (MS-ISAC), which operates in all 50 states and 6 territories and constantly monitors cyber threats for local governments. While S. 1846 passed en bloc with S. 1668 and other non-controversial bills without any objections, its passage in the full Senate may be more difficult.

Stakeholders should keep a close eye on bigger-picture politics related to the aforementioned bills. For example, S. 734 was introduced by Senator Gardner, who is considered one of the most vulnerable GOP Members up for reelection in 2020, and the Republican Conference will likely be eager to provide him with a legislative victory to boost his campaign. Conversely, Senator Peters is also up for a tough reelection in 2020, and so a multi-bill negotiation might be needed to ensure passage of these measure.

DoD Inspector General Report on Cybersecurity Risks for Commercial Off the Shelf (COTS) Purchases

On July 26, 2019, DoD's Office of the Inspector General (OIG) released a report revealing that in FY 2018, the Department spent more than $38.2 million to purchase more than 9,000 commercial off-the-shelf (COTS) technology products with known security risks that could be used to spy on or hack U.S. military personnel and facilities. As the report states, "[i]f the DoD continues to purchase and use COTS information technology items without identifying, assessing, and mitigating the known vulnerabilities associated with COTS information technology items, missions critical to national security could be compromised." The OIG report notes that the recent increase in DoD's micro-purchase threshold to $10,000 may serve to increase the scale of purchases of potentially risky information technology devices. The report recommended, among other things, that DoD direct an organization to develop a risk-based strategy for COTS cybersecurity and review acquisition policies to add cybersecurity evaluations for purchase cards.

Government Accountability Office Cybersecurity Report

On July 25, 2019, the Government Accountability Office (GAO) issued a progress report on 23 agencies' enterprise risk management programs, designed to reduce agency level cybersecurity risks. GAO found that agencies identified multiple challenges in establishing and implementing cybersecurity risk management programs, most critically in recruiting and retaining key cybersecurity risk management personnel. Other issues include maintaining and executing consistent security policies and procedures

and receiving quality risk data. GAO concluded that most agencies did not develop an adequate agency-wide cybersecurity risk management strategy to guide their risk decisions.

House Energy & Commerce Committee Advances Cybersecurity Bills

Although news headlines are dominated by partisanship, lawmakers on both sides of the aisle have continued to find common ground in strengthening the nation's cybersecurity. On July 17, the House Energy & Commerce Committee favorably reported four cybersecurity bills focused on the country's energy sector. The committee approved all four bills by voice vote, and the full House will likely take them up on the floor under suspension of the rules when Members return from the August Recess.

The first bill considered was H.R. 359, Enhancing Grid Security through Public-Private Partnerships Act, which encourages the Department of Energy (DOE) to facilitate public-private partnerships in order to address and mitigate the physical security and cybersecurity risks to the U.S. electric grid. Rep. Jerry McNerney (D-CA) and Rep. Bob Latta (R-OH) introduced H.R. 359 on July 9.

Next, the committee considered H.R. 360, the Cyber Sense Act of 2019, which would create a voluntary "Cyber Sense" program under DOE that would establish a process to test and report on the cybersecurity vulnerabilities of products and technologies necessary for operating an interconnected electric energy transmission network. Rep. Latta introduced H.R. 360 as the lead author on January 9 along with Rep. McNerney.

The committee also considered H.R. 362, the Energy Emergency Leadership Act, introduced by Energy Subcommittee Chairman Bobby Rush (D-IL) and Rep. Tim Walberg (R-MI). The bill would require the Secretary of DOE to assign energy emergency and energy security functions to an Assistant Secretary, including responsibilities with respect to infrastructure and cybersecurity.

Lastly, the committee considered H.R. 370, the Pipeline and LNG Facility Cybersecurity Preparedness Act, which would require 'DOE to implement a program to ensure the security, resiliency, and survivability of natural gas pipelines, hazardous liquid pipelines, and liquefied natural gas facilities. The bill was introduced by the Ranking Member of the Energy Subcommittee, Rep. Fred Upton (R-MI) and Rep. Dave Loebsack (D-IA).

Authors

Christian Tamotsu Fjeld, Senior Vice President

Christian Tamotsu Fjeld is a Vice President of ML Strategies in the firm's Washington, DC office. He assists a variety of clients in their interactions with the federal government.

Alexander Hecht, Executive Vice President & Director of Operations

Alexander Hecht is Executive Vice President & Director of Operations of ML Strategies, Washington, DC. He's an attorney with over a decade of senior-level experience in Congress and trade associations. Alex helps clients with regulatory and legislative issues, including health care and technology.