

United States Senate

WASHINGTON, DC 20510

October 9, 2019

The Honorable Mick Mulvaney
Director
Office of Management and Budget
725 17th Street NW
Washington, DC 20503

Dear Director Mulvaney,

We write urging the Federal Acquisition Security Council (FASC) to develop a strategic plan for sharing supply chain security information with Congress and the judiciary to better protect U.S. government systems and enhance our national security. Both Congress and the Executive branch have devoted considerable time identifying ways to enhance the supply chain security of information and communications technology (ICT) on U. S. government systems. As a result, the U.S. has started putting mechanisms in place to improve supply chain risk management (SCRM), primarily as it relates to executive agencies. That work is vitally important, but executive agency solutions do not always mean whole of government solutions. The government must ensure that information used to secure executive agency computer systems and networks is shared with ICT professionals in Congress and the judiciary.

Last Congress, President Trump signed into law a measure creating the FASC.¹ The FASC is responsible for identifying and recommending supply chain risk management standards, guidelines, and practices for “executive agencies, other Federal entities, and non-Federal entities with respect to supply chain risk.”² Specifically, the FASC is charged with facilitating information sharing within the federal government. As the Intelligence Community (IC) analyzes the ICT SCRM threats and shares that information, through the FASC, with civilian agencies making security and acquisition decisions, it is important that this information also be provided to the other two branches of government.

Neither Congress nor the judiciary has the resources, expertise, or mission to replicate the IC’s SCRM work, meaning that the comprehensive “whole of government” approach the FASC was intended to achieve will likely only benefit one branch of the federal government. This leaves Congress and the courts at risk of introducing insecure ICT that is vulnerable to the national security threats assessed by the IC and FASC.

The threat is not hypothetical. Americans may accept the principle of the separation of branches of government, but our adversaries don’t abide by that principle. The 2018 National Cyber Strategy notes that “adversaries have increased the frequency and sophistication of their malicious cyber activities.”³ For the past three years, the U.S. Courts Information Systems and Cybersecurity Annual Report has highlighted the need to “counter a range of threats posed by hacking, computer viruses, and other malicious acts.”⁴ A recent Center for Strategic and International Studies report on Russian targeting of the judiciary’s system notes, “[t]here is an

¹ SECURE Technology Act, Pub. L. No. 115-390, 132 Stat. 5173 (2018).

² 41 U.S.C. § 1322(a), 1323(a) (2018).

³ White House, Nat’l Cyber Strategy of the U.S. of Am. I (2018), <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

⁴ Info. Sys. & Cybersecurity – Annual Report 2018, U.S. Courts, <https://www.uscourts.gov/statistics-reports/information-systems-and-cybersecurity-annual-report-2018>.


immediate need to expand both the content and the reach of threat awareness among practitioners in the justice system so that they are cognizant of the threat and can be ready to respond.”⁵

Adversaries abroad have similarly targeted Congress, most recently documented in a number of attempted hacks of Senate offices.⁶ This threat goes back over a decade, with one notable incident in 2008 impacting a number of Congressional computers.⁷ These adversaries are likely are using every tool at their disposal to compromise the ICT used every day by Congressional offices, committees, and staff.

Congress created the FASC to advance a critical information-sharing mission that includes identifying criteria for sharing information with both federal agencies and non-federal entities. To ensure that the federal government maintains a true whole-of-government SCRM policy in line with Congressional intent, we urge the FASC to develop a strategic plan that will specifically incorporate information sharing with the judiciary and Congress. As such, we request that FASC provide information to the Senate Sergeant at Arms, the House of Representatives Chief Information Officer, and their appropriate counterparts in the Judiciary that includes, but is not limited to, threat briefings on ICT.

Thank you for your attention to this serious matter. We look forward to receiving a written response detailing how FASC will implement its new strategic plan by October 23, 2019.

Sincerely,



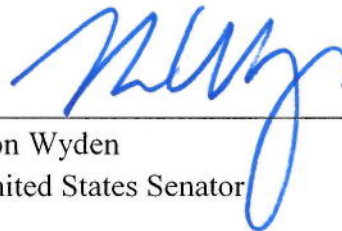
Ron Johnson
Chairman
Senate Homeland Security and
Governmental Affairs Committee



Gary C. Peters
Ranking Member
Senate Homeland Security and
Governmental Affairs Committee



Tom Cotton
United States Senator



Ron Wyden
United States Senator

⁵ Suzanne Spalding, et al., Ctr. for Strategic and Int’l Studies, *Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System* 34 (2019), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190430_RussiaUSJusticeSystem_v3_WEB_FULL.pdf.

⁶ Donnie O’Sullivan, *Russians targeted Senate and conservative think tanks, Microsoft says*, CNN (Aug. 22, 2018), <https://www.cnn.com/2018/08/21/politics/microsoft-russia-american-politicians/index.html>.

⁷ Sean Lyngaas, *Lawmakers want data on the number of times Senate computers have been hacked*, CyberScoop (Mar. 13, 2019), <https://www.cyberscoop.com/senate-hacked-ron-wyden-tom-cotton-sergeant-at-arms/>.