RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

September 19, 2018

The Honorable Mitch McConnell
Majority Leader
United States Senate
Washington, DC 20510

The Honorable Charles E. Schumer
Minority Leader
United States Senate
Washington, DC 20510

The Honorable Roy Blunt
Chairman
Committee on Rules and Administration
United States Senate
Washington, DC 20510

The Honorable Amy Klobuchar
Ranking Member
Committee on Rules and Administration
United States Senate
Washington, DC 20510

Dear Majority Leader McConnell, Minority Leader Schumer, Chairman Blunt, and Ranking Member Klobuchar:

I write to express my serious concern that the U.S. Senate Sergeant at Arms (SAA) apparently lacks the authority to protect U.S. Senators and Senate staff from sophisticated cyber attacks directed at their personal devices and accounts. I am introducing legislation to address this problem and invite you to support it.

The 2016 election made it clear that foreign governments, including Russia, are leveraging cyberspace to target the fundamental pillars of American democracy. Even more concerning, administration officials confirm that Russia is continuing its campaign of hacking and influence operations. But our adversaries do not limit their cyber attacks to elections infrastructure or even to official government accounts and devices; they are also targeting U.S. officials' personal accounts and devices. Indeed, Admiral Michael Rogers confirmed earlier this year that personal devices and accounts of senior U.S. government officials "remain prime targets for exploitation." I have enclosed a copy of Admiral Rogers' letter.

These attacks are not limited to members of the executive branch. Press reports from January of this year indicate that Fancy Bear–the notorious Russian hacking group–targeted senior congressional staff in 2015 and 2016. My office has since discovered that Fancy Bear targeted personal email accounts, not official government accounts. And the Fancy Bear attacks may be the tip of a much larger iceberg. My office has also discovered that at least one major technology company has informed a number of Senators and Senate staff members that their personal email accounts were targeted by foreign government hackers.

Given the significance of this threat, I was alarmed to learn that SAA cybersecurity personnel apparently refused to help Senators and Senate staff after these attacks. The SAA informed each

Senator and staff member who asked for help that it may not offer cybersecurity assistance for personal accounts. The SAA confirmed to my office that it believes it may only use appropriated funds to protect official government devices and accounts.

This approach must change to keep up with changing world realities.

Congress has recognized a need to protect executive branch officials' personal devices and accounts, authorizing the Department of Defense in the past few years to provide personal-device cyber protection to Pentagon officials likely to be high-value targets. The U.S. Senate Select Committee on Intelligence approved an intelligence authorization bill earlier this year with language that would similarly protect intelligence community personnel if enacted.

The Senate, meanwhile, has only established a working group to "identify, develop, and recommend options to provide enhanced cybersecurity for Senators' personal communications devices and accounts."

The November election grows ever closer, Russia continues its attacks on our democracy, and the Senate simply does not have the luxury of further delays. Already there is a growing chorus for action: The Appropriations Committee recently noted in its report accompanying the 2019 Legislative Branch Appropriations bill that it "continues to be concerned that Senators are being targeted for hacking and cyber attacks, especially via their personal devices and accounts."

In light of this ever-growing threat, I invite you to support legislation that I am introducing to permit the SAA to provide cybersecurity assistance to Senators and staff, on an opt-in basis, for their personal devices and accounts. I also ask that you poll Senators and staff in your respective caucuses to determine how many of them have been notified by major technology companies that their accounts were targeted by foreign government hackers.

If you have any questions regarding this request, please contact Chris Soghoian in my office.

Sincerely,

Ron Wyden

Ron Wyden
United States Senator

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

12 April 2018

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Wyden:

Thank you for your 27 October 2017 letter on the security of personal devices and accounts belonging to senior U.S. Government officials. I certainly agree with your concerns that these devices and accounts remain prime targets for exploitation, and we must raise awareness so all Government employees employ proper cybersecurity hygiene. A process to detect and remediate exploitation would complement such preventative security measures. Only through a whole-of-Government approach can we as a nation begin to address these growing threats, and we look forward to your continued support in this regard.

For its part, the National Security Agency (NSA) will continue our mission of securing National Security Systems. We collaborate with and support the Department of Homeland Security (DHS) and other Executive Branch agencies regarding cybersecurity threats, vulnerabilities, and mitigations. NSA subject matter experts deliver cybersecurity briefings and demonstrations to audiences throughout the Federal Government, including the Legislative Branch. In order to better inform the public, NSA also publishes unclassified guidance on how users can secure their communications devices, computing equipment, and networks.

Specifically, NSA has provided classified briefings to DHS on cybersecurity threats and vulnerabilities, including briefings on best practices for securing mobile devices. Additionally, NSA has made guidance publicly available at www.iad.gov for application to Government and personal devices. This includes best practices for keeping home networks secure (https://www.iad.gov/iad/library/ia-guidance/security-tips/best-practices-for-keeping-your-home-network-secure-updated.cfm).

The measures described above help manage, but do not eliminate, the risk of compromise. Should senior leaders' personal devices and accounts be compromised, a process to detect and remediate the threats would reduce the risk of sensitive information being obtained by our adversaries. I will direct NSA's cybersecurity technical experts to raise this issue with their DHS counterparts as part of their continuing discussions.

Thank you again for your correspondence and interest in this important issue. NSA is prepared to support DHS as needed and upon request.

MICHAEL S. ROGERS
Admiral, U.S. Navy
Director, NSA

Copies Furnished:
Honorable Kirstjen M. Nielsen,
Secretary of Homeland Security
Mr. Rob Joyce
White House Cybersecurity Coordinator