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

October 27, 2017

The Honorable Elaine C. Duke
Acting Secretary of Homeland Security
Washington, D.C. 20528

Admiral Michael S. Rogers
Director, National Security Agency
9800 Savage Road
Ft. George G. Meade, MD 20755-6000

Dear Acting Secretary Duke and Admiral Rogers:

I write to ask that you take prompt action to protect the personal devices and online accounts of senior government officials from attack by hackers and foreign governments.

According to media reports, malware was recently discovered on the personal smartphone of White House Chief of Staff John Kelly. General Kelly joins a long list of senior government official whose accounts or devices have been compromised in recent years, including CIA Director John Brennan, Colin Powell, John Podesta, and Sarah Palin.

It is clear why government officials such as General Kelly would be prime targets for hackers or foreign intelligence services. Of far greater concern is that the malware was reportedly only discovered because his smartphone was malfunctioning. This raises deeply troubling questions about whether the White House regularly screens personal devices for foreign malware and how long the malware might have remained on General Kelly's phone undetected had the device not obviously malfunctioned.

Foreign governments could target government officials' personal devices and accounts because they have significant intelligence value and are often poorly secured. For example, hackers can easily co-opt personal smartphones, turning the phone's microphone into a listening device that can record nearby conversations even when the phone isn't being used. Likewise, if hackers gain access to an official's personal email account, they will gain access to contact lists and other personal information that enables them to launch even more effective spear-phishing attacks.

In light of this serious cyber threat to U.S. national security, I urge you to immediately direct your respective agencies to collaborate on a comprehensive effort to secure the personal devices and accounts of senior government officials. At a minimum, this effort must include:

- A voluntary program to regularly screen the personal computers and smartphones of senior officials for malware, utilizing threat signatures identifying nation-state malware;

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

HTTP://WYDEN.SENATE.GOV

- A cybersecurity "check-up" of personal accounts, ensuring senior government officials are using strong passwords and have enabled two-factor authentication; and
- Collaboration with major phone and internet companies to flag the accounts of senior government officials so that high-risk transactions such as password resets and SIM card swaps require manual approval.

If you have any questions about this request, please contact Chris Soghoian on my staff at (202) 224-5244.

Sincerely,

Ron Wyden

Ron Wyden
United States Senator

CC: Mr. Rob Joyce, White House Cybersecurity Coordinator