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

May 16, 2018

The Honorable Caroline C. Hunter
Chair
Federal Election Commission
1050 First Street, NE Washington, DC 20463

Dear Ms. Hunter:

I am writing to request that the Federal Election Commission (FEC) issue an advisory opinion on whether Members of Congress may use excess campaign funds to protect themselves and their personal devices and accounts from the enhanced cyber threats they face in their roles as elected officials.

Last summer, in response to a request from the House of Representatives' Sergeant at Arms, the FEC issued an advisory opinion determining that Members of Congress may use excess campaign funds to bolster home security in response to physical threats. Through this opinion, the FEC recognized that Members face threats greater than those to the general public due to their high-profile roles as elected officials.

Some of the threats members face are physical, but many more are digital. The 2016 election season highlighted the dangers elected officials face in the cyber realm, including attacks by sophisticated state-sponsored hackers and intelligence agencies against personal devices and accounts. Indeed, in a recent letter, Admiral Michael Rogers, then the Director of the National Security Agency, confirmed that personal devices and accounts of senior U.S. government officials "remain prime targets for exploitation." I have enclosed a copy of that letter.

Effectively defending against these threats imposes prohibitive costs and should not be the sole personal financial responsibility of members. Therefore, I ask that the FEC issue an advisory opinion on whether Members of Congress may use excess campaign funds to protect themselves from cyber threats they face during their time as public officials.

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

Sincerely,

Ron Wyden
United States Senator

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

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