

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

**RECEIVED**

By Office of General Counsel at 12:22 pm, May 16, 2018

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.

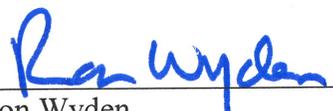
Last summer, in response to a request from the House of Representatives' Sergeant at Arms, the FEC issued an advisory opinion determining that Members of Congress may use excess campaign funds to bolster home security in response to physical threats. Through this opinion, the FEC recognized that Members 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



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:

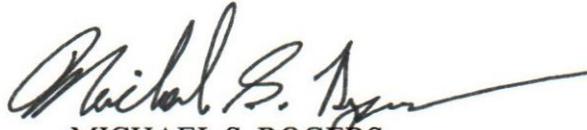
Thank you for your 27 October 2017 letter on the security of personal devices and accounts belonging to senior U.S. Government officials. I certainly agree with your concerns that these devices and accounts remain prime targets for exploitation, and we must raise awareness so all Government employees 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](http://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.

A handwritten signature in black ink, appearing to read "Michael S. Rogers", with a long horizontal flourish extending to the right.

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

## Joanna Waldstreicher

---

**From:** Soghoian, Chris (Wyden) <Chris\_Soghoian@wyden.senate.gov>  
**Sent:** Wednesday, June 06, 2018 1:13 PM  
**To:** Joanna Waldstreicher  
**Subject:** RE: advisory opinion request

I just wanted to make sure you saw page 4 of this document, which is a series of answers to questions for the record, from the Director of National Intelligence

<https://www.intelligence.senate.gov/sites/default/files/documents/Response%20to%20SSCI%20QFRs%20-%20Unclassified%20Subset.pdf>

I could chat anytime between 4:30-6 today, or tomorrow from 3-5.

---

**From:** Joanna Waldstreicher <JWaldstreicher@fec.gov>  
**Sent:** Wednesday, June 6, 2018 12:51 PM  
**To:** Soghoian, Chris (Wyden) <Chris\_Soghoian@wyden.senate.gov>  
**Subject:** advisory opinion request

Dear Chris:

I got your message about sending us some additional materials, so please feel free to use this email address for anything you would like to send our way. In addition, a colleague and I would like to give you a call to discuss next steps. Is there a good time to call you this afternoon or tomorrow?

Best,  
Joanna S. Waldstreicher  
Office of the General Counsel, Policy Division  
Federal Election Commission  
1050 First Street, NE  
Washington, DC 20463  
(202) 694-1650

**UNCLASSIFIED RESPONSES TO QUESTIONS FOR THE RECORD  
SENATE SELECT COMMITTEE ON INTELLIGENCE  
HEARING FEBRUARY 13, 2018**

**Hearing Date:** February 13, 2018  
**Committee:** SSCI  
**Member:** Sen. Rubio  
**Witnesses:** Director Coats  
**Info Current as of:** April 2, 2018

**Question:** The National Security Strategy of the United States emphasizes, “The United States also remains committed to supporting and advancing religious freedom.”

**What kind of violations and threats to religious freedom do you assess are threats to our national security? Which countries are the greatest offenders?**

**Answer:**

Most foreign government violations of religious freedom—from the persecution of small communities of Baha’is and Jehovah’s Witnesses in many countries to North Korean prohibitions against all faiths—can be categorized as human rights concerns that might create conditions for future harm to U.S. national security interests. More direct threats to U.S. interests primarily arise when religious repression fuels either the growth of anti-Western violent extremism or instability in a country, such as majority-Buddhist Burma’s crackdown on its population of 2 million Muslim Rohingyas, which the United Nations and others have described as ethnic cleansing. Violations by governments against Muslims, for example, can bolster Islam-under-attack narratives that jihadist groups use to attract recruits and advance their agendas against the West and its partners. Government violations of religious freedom also can fuel societal intolerance against the targeted faiths, which in turn can lead to societal tensions, protests, political turmoil, or other forms of instability in a wide variety of places around the globe, including China and Western Europe.

- Among the governments that violate religious freedoms—Burma, China, Eritrea, Iran, North Korea, Saudi Arabia, Sudan, Tajikistan, Turkmenistan, and Uzbekistan—are designated by the Department of State as Countries of Particular Concern (CPC) for engaging in or tolerating “systematic, ongoing, and egregious” violations. In 2017, the U.S. Commission on International Religious Freedom (USCIRF) recommended designating Russia and Syria as CPCs and placed Egypt, Indonesia, and Malaysia on the second-highest tier of concern.
- Of the non-CPC countries, Egypt, Indonesia, Malaysia, Russia, and Syria ranked highest on the Pew Research Center’s most recent index of government violators compiled in December 2015. Sunni terrorist groups are internationally notorious for being among the more egregious violators of religious freedom globally.

**Hearing Date:** February 13, 2018  
**Committee:** SSCI  
**Member:** Sen. Rubio  
**Witnesses:** Director Coats  
**Info Current as of:** April 2, 2018

**Question:** The National Security Strategy of the United States emphasizes, “The United States also remains committed to supporting and advancing religious freedom.”

**What trends do you see regarding religious freedom violations, especially from governments justifying violations in the name of security or countering extremism?**

**Answer:**

The depth and breadth of religious freedom violations around the world varies from country to country but is historically elevated, according to diplomatic, UN, and other open-source reporting. The level of violations in the early and mid-1990s that spurred passage of the 1998 International Religious Freedom Act has since worsened, according to the USCIRF and other open-source reporting. Government restrictions on religious practice increased in all major regions of the world between 2007 and 2015, according to the Pew Research Center, while social hostilities and violations by nonstate actors also steadily increased in most regions. Department of State and USCIRF reporting highlights the growth in recent years of government violations of religious freedom tied to laws intended to counter terrorism or extremism.

**Hearing Date:** February 13, 2018  
**Committee:** SSCI  
**Member:** Sen. Wyden  
**Witnesses:** Director Coats  
**Info Current as of:** April 23, 2018

**Question:** Recent news reports indicate that the same Russian hackers who infiltrated the Democratic National Committee in 2016 and the German Bundestag in 2014 repeatedly targeted senior US government officials, defense contractors, and scientists through their personal email accounts. (AP, “‘Fancy Bear’ hackers took aim at US defense contractors,” February 7, 2018.)

**Do you believe there is a legitimate government interest in protecting the personal accounts and devices of government officials?**

**Answer:**

The personal accounts and devices of government officials can contain information that is useful for our adversaries to target, either directly or indirectly, these officials and the organizations with which they are affiliated.

**Hearing Date:** February 13, 2018  
**Committee:** SSCI  
**Member:** Sen. Wyden  
**Witnesses:** Director Coats  
**Info Current as of:** April 23, 2018

**Question:** Recent news reports indicate that the same Russian hackers who infiltrated the Democratic National Committee in 2016 and the German Bundestag in 2014 repeatedly targeted senior U.S. government officials, defense contractors, and scientists through their personal email accounts. (AP, “‘Fancy Bear’ hackers took aim at U.S. defense contractors,” February 7, 2018.)

**What resources do you need in order to ensure that these personal accounts and devices are not a vulnerable target for foreign intelligence services?**

**Answer:**

We have the resources we need to continue our respective education and awareness programs, which are the most important weapons in the cyber-battlefield when it comes to personal devices and accounts. We also need to continue to harden our government systems, both classified and unclassified, to prevent the potential compromise of a Government-issued personal device or account from becoming a major cyber-intrusion or cyber-success against our government networks or programs; I have made this a priority for the IC. If these programs require additional resources, I will inform this committee.

**Hearing Date:** February 13, 2018  
**Committee:** SSCI  
**Member:** Sen. Cotton  
**Witnesses:** Director Coats  
**Info Current as of:** March 29, 2018

**Question:** In 2017, the Director of the Central Intelligence Agency referred to WikiLeaks as a “non-state hostile intelligence service” that often aids U.S. adversaries like Russia and China. At my request, Chairman Burr and Vice-Chairman Warner included language to that effect in the FY17 Intelligence Authorization Act.

**Do you agree with Director Pompeo and this Committee that WikiLeaks is a non-state hostile intelligence service that often aids U.S. adversaries like Russia?**

**Answer:**

Yes, WikiLeaks should be viewed as a non-state hostile foreign intelligence entity whose actions, both individually and in collaboration with others, have caused harm to U.S. national security and interests.

**Hearing Date:** February 13, 2018  
**Committee:** SSCI  
**Member:** Sen. Heinrich  
**Witnesses:** Director Coats  
**Info Current as of:** April 23, 2018

**Question: How long can personnel from the Executive Office of the President (EOP) hold an interim clearance before the clearance process is terminated and access suspended?**

**Answer:**

Under Executive Order 12968 (EO 12968), where official functions must be performed prior to the completion of the investigation and adjudication process, temporary eligibility for access to classified information may be granted. EO 12968 imposes no time limit on temporary access.

**Hearing Date:** February 13, 2018  
**Committee:** SSCI  
**Member:** Sen. Heinrich  
**Witnesses:** Director Coats  
**Info Current as of:** April 23, 2018

**Question: What accountability is there to the DNI, as the government's security executive agent, for the granting of interim security clearances generally, and the interim SCI clearances, specifically?**

**Answer:**

While the DNI has policy and oversight responsibilities for Government personnel security programs and access to SCI, under authorities set forth in statute and Executive Order, Agency Heads are responsible for establishing and maintaining an effective program to ensure that temporary access to classified information by personnel is clearly consistent with the interest of national security. Agency Heads are responsible for following the DNI's policy guidance when granting such clearances.

**Hearing Date:** February 13, 2018  
**Committee:** SSCI  
**Member:** Sen. Heinrich  
**Witnesses:** Director Coats  
**Info Current as of:** April 23, 2018

**Question: Has the DNI reviewed all the cases of interim access to SCI, both in the EOP and across the government?**

**Answer:**

The DNI does not routinely review cases of interim access to SCI in the government. The DNI does not recommend temporary accesses be granted or denied in specific cases unless an Agency Head specifically requests guidance.

**Hearing Date:** February 13, 2018  
**Committee:** SSCI  
**Member:** Sen. Heinrich  
**Witnesses:** Director Coats  
**Info Current as of:** April 23, 2018

**Question: Are personnel with interim access to SCI under a Continuous Evaluation protocol, and if so, who manages that?**

**Answer:**

Personnel with interim access may be under Continuous Evaluation. Identification of the population covered by Continuous Evaluation is the responsibility of the Agency Head.

**Hearing Date:** February 13, 2018  
**Committee:** SSCI  
**Member:** Sen. Heinrich  
**Witnesses:** Director Coats  
**Info Current as of:** April 23, 2018

**Question:** Are there executive branch and EOP personnel who have held interim access to SCI for longer than one year, and if so, how many such personnel and in what agencies do they work?

**Answer:**

In terms of EOP interim SCI access, the best source of information would be EOP, and I would defer to them to address questions regarding EOP personnel with interim access to SCI.

**Hearing Date:** February 13, 2018  
**Committee:** SSCI  
**Member:** Sen. Harris  
**Witnesses:** Director Coats  
**Info Current as of:** April 16, 2018

**Question: You have the authority to issue Intelligence Community Directives that establish policy across the IC. Your predecessor used that authority to establish specific duties to warn victims?**

**Will you commit to using that same authority to establish a specific duty to warn states about election related cybersecurity threats? If not, why not?**

**Answer:**

We appreciate the importance of this issue, and the IC remains committed to warning our intelligence consumers about the wide range of serious threats facing the United States that are prioritized and disseminated commensurate with oversight by select committees for intelligence. We do not intend to issue a policy specifically establishing a duty to warn states about election-related cybersecurity threats. The referenced policy, ICD 191, *Duty to Warn*, was issued in 2015 directing IC elements to warn U.S. and non-U.S. persons of impending threats of intentional killing, serious bodily injury, or kidnapping. The Duty to Warn Directive was established to account for intelligence that, when encountered, would be acted upon in a time-sensitive manner directly by IC elements. We do have policies in place that were established to ensure the IC is providing intelligence information, at an appropriate clearance level, to support the Department of Homeland Security (DHS) and other Executive Branch agencies, as appropriate, in their ability to provide useful information to state, local, and tribal governments in a timely manner. The first of these policies, ICD 209, *Tearline Production and Dissemination*, was issued at the request of DHS to expand the utility of intelligence to a broad range of customers. The second Directive, ICD 208, *Write for Maximum Utility*, was issued to ensure intelligence products were written and disseminated in a manner that provides the greatest use for our customers. The IC will continue to support our customers by providing useful and timely intelligence information as appropriate.

## Joanna Waldstreicher

---

**From:** Soghoian, Chris (Wyden) <Chris\_Soghoian@wyden.senate.gov>  
**Sent:** Monday, June 18, 2018 12:28 PM  
**To:** Joanna Waldstreicher  
**Subject:** RE: advisory opinion request

Joanna,

Flagging this language for you, from the new FY2019 Legislative Branch Appropriations Act, Committee Report.  
<https://www.appropriations.senate.gov/download/fy19-legislative-branch-appropriations-act-report-115-274&download=1>

**Senators' Personal Cybersecurity.—The Committee continues to be concerned that Senators are being targeted for hacking and cyberattacks, especially via their personal devices and accounts.** The Committee appreciates the efforts of the bipartisan Senators' Personal Cybersecurity Working Group established by the Legislative Branch Appropriations Act, 2018 to identify, develop, and recommend options to provide enhanced cybersecurity for Senators' personal communications devices and accounts. The Committee encourages the working group to continue collaborating across offices in a bipartisan manner and consulting with the Senate community and external experts to provide a comprehensive report on options to improve Senators' personal cybersecurity by the required deadline of September 19, 2018. The Committee also reiterates that such report must include an analysis of an option or options that would provide for a direct provision of services by the Senate Sergeant At Arms upon voluntary election by an individual Senator and that privacy protections must be a component of each option.

## Joanna Waldstreicher

---

**From:** Soghoian, Chris (Wyden) <Chris\_Soghoian@wyden.senate.gov>  
**Sent:** Friday, September 14, 2018 3:06 PM  
**To:** Joanna Waldstreicher  
**Subject:** FW: Letter  
**Attachments:** ridt-letter-wyden.pdf

Joanna,

Senator Wyden received this letter today from Professor Thomas Rid of Johns Hopkins University, addressing the question of whether Senators face unique cybersecurity threats due to their roles as elected officials.

Professor Rid previously testified at an open hearing before the Senate Intelligence Committee in March, 2017 on the topic of Russian Active Measures. A copy of his testimony can be accessed here:  
<https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf>

Would you please add Dr. Rid's letter to the folder associated with Senator Wyden's original FEC request and then docket the request and accompanying materials, so that they can be considered soon by the Commission?

Thanks,

Chris



T Rid, SAIS, 1619 Massachusetts Ave NW, Washington, DC 20036

The Honorable Ron Wyden  
United States Senate  
Washington, DC 20510-3703

9/14/18

Subject: Congressional Cybersecurity

Dear Senator Wyden:

I understand the Federal Election Commission (FEC) is looking for expert analysis on the threat foreign hackers pose to Members of Congress and senior United States Government officials. I write to provide you my professional assessment in hopes that you will pass it on to the FEC.

By way of background, I am a Professor at Johns Hopkins University's School of Advanced International Studies and an expert on cybersecurity. Before moving to Washington D.C. last year, I was a Professor of Security Studies at King's College in the United Kingdom. My recent work focuses on identifying and analyzing the threats posed by cyberattacks. My piece "How Russia Pulled off the Biggest Election Hack in US History," from October 2016, has received widespread media attention. In March 2017 I testified in front of the Senate Select Committee on Intelligence on election interference.

For-profit criminals go after Americans with identity theft, ransomware, spyware, phishing attacks, impersonal fraud, or other scams. But senior executive branch officials and Members of Congress face additional, targeted threats from sophisticated, persistent, and often well-funded adversaries. The motivations of these hostile actors vary widely. Some seek sensitive information to embarrass or disrupt the workings of our government, while others are probing for weaknesses in our nation's defenses. Tactics vary widely, too, from using highly sophisticated technical intrusion capabilities, to borrowing tactics from criminals (e.g. phishing and spyware). Whatever the technical route, and whatever the motivation, no country has a larger target surface than the United States.

**Thomas Rid**  
**Professor of Strategic Studies**

The Paul H. Nitze School of Advanced International Studies  
1619 Massachusetts Avenue NW Washington, DC 20036  
rid@jhu.edu <https://ridt.co>  
<https://sais-jhu.edu>

## Tip of the Iceberg

In 2016, hackers working for the Russian government broke into a range of targets, including the network of the Democratic National Committee, the email account of Senator Hillary Clinton's presidential campaign manager John Podesta, and former chairman of the Joint Chiefs Colin Powell. These widely publicized breaches are only the tip of a vast iceberg. These hacks are widely known today because the emails stolen from these accounts were subsequently weaponized and used as part of a campaign to influence the outcome of several elections — most publicly, the Presidential race between Donald Trump and Hillary Clinton, but also House races in Illinois, New Hampshire, New Mexico, North Carolina, Ohio, and Pennsylvania.<sup>1</sup> Senator Lindsey Graham also reported that his campaign's email was successfully compromised.<sup>2</sup>

While the 2016 hacks were a watershed moment, they are only the most visible and disruptive instances of this wider threat to American democracy. In 2008, the Obama and McCain presidential campaigns were both reportedly compromised by hackers working for the Chinese government. These cyber operations had all the hallmarks of traditional espionage. The hackers reportedly stole “massive amounts of internal data from both campaigns — including internal position papers and private emails of key advisers in both camps,” which were quietly exfiltrated.<sup>3</sup>

Critically, we know about these attacks because the hacked information was deliberately leaked, or because the hackers were sloppy, or unlucky, and got caught. For example the hacking against White House Chief of Staff John Kelly's phone appears to have only been discovered because it caused his device to malfunction. It is likely that we only know a fraction of the total number of successful hacks. Without a systematic effort to track cyberattacks against American officials, many of the most sophisticated digital operations, particularly those conducted for espionage rather than in aid of influence operations, are likely to remain hidden.

## Personal Devices and Accounts: Unprotected but Highly Targeted

The wave of hacking and hacking attempts against United States officials are not limited to agency servers and official, government email accounts. **Every major hacked-and-leaked email account during the 2016**

---

<sup>1</sup> “Democratic House Candidates Were Also Targets of Russian Hacking,” *The New York Times*, Dec. 13, 2016

<sup>2</sup> “Graham: Russians hacked my campaign email account,” CNN, Dec. 14, 2016

<sup>3</sup> “Chinese hacked Obama, McCain campaigns, took internal documents, officials say,” NBC News, Jun 6, 2013.

**election interference campaign was a non-government (personal or campaign) account** — many of the documents that Russian fronts claimed came “from the DNC” in fact did not come from the DNC, but from personal email accounts. These accounts are outside the official security perimeter of the U.S. government, yet contain highly sensitive information about officials’ activities, private communications, family life, finances, and movements. Personal accounts are often much softer targets because the user determines the security settings, not cybersecurity professionals.

As a result, hackers working for foreign powers (as well as so-called ‘hacktivists’) have zeroed on the non-official accounts of current and former officials. These include: White House Chief of Staff John Kelly (personal phone), former CIA Director John Brennan (personal email), former DNI James Clapper (personal email, phone accounts), and former FBI Deputy Director Mark Giuliano (personal email).

### Protecting Senators at Work and at Home

Private-sector intelligence reports show that several Senators and their staff have been targeted by advanced, persistent cyber attacks beginning in June of 2017.<sup>4</sup> Critically, adversaries targeted probably more personal accounts than official accounts.

It is my expert opinion that these reports only scratch the surface of the advanced cyber threats faced by Senators, House members, senior executive branch officials and important political staff. Further, it is clear that our most aggressive and dangerous adversaries do not limit their targeting to official accounts and devices and why anybody would think so is beyond me. But because personal accounts and devices are at an even greater risk.

The personal accounts of Senators and their staff are high-value, low-hanging targets. No rules, no regulations, no funding streams, no mandatory training, no systematic security support is available to secure these resources. With no one forcing them to improve their personal cybersecurity and little expert assistance available, it’s unsurprising that many elected officials have bad personal cybersecurity. In this regard, elected politicians indeed represent average Americans — like most people, they reuse passwords, don’t bother with two-factor authentication, and regularly open attachments they receive via email on their own devices. That may not sound bad, but it is. Poor personal cybersecurity habits may not create serious problems for the average American, or indeed endanger

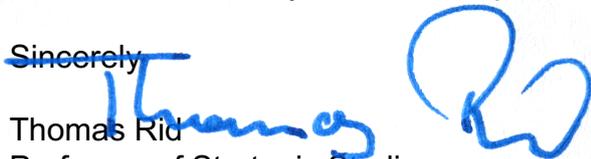
---

<sup>4</sup> “Update on Pawn Storm: New Targets and Politically Motivated Campaigns,” Trend Micro, 12 January 2018.

national security. The average American, after all, does not have foreign intelligence services trying to break into their email account and smartphone.

Tragically, we all now recognize that physical threats against Members of Congress follow them beyond the grounds of the Capitol. So too cyber threats follow Members to whichever accounts and devices they use. If anything, hackers are likely to target the digital resources that are the least protected, which will frequently be a personal account or device. It would therefore be prudent as well as urgent to encourage and support efforts to increase the security of Senators' personal devices and accounts.

Sincerely,



Thomas Rid  
Professor of Strategic Studies  
Johns Hopkins University/SAIS

## Joanna Waldstreicher

---

**From:** Soghoian, Chris (Wyden) <Chris\_Soghoian@wyden.senate.gov>  
**Sent:** Thursday, September 20, 2018 3:02 PM  
**To:** Joanna Waldstreicher  
**Cc:** Robert Knop  
**Subject:** RE: Letter

Joanna,

I wanted to flag this letter and accompanying article for you:

<https://www.wyden.senate.gov/imo/media/doc/wyden-member-personal-email-cybersecurity-letter-to-leadership-rules-sept-19.pdf>

<https://apnews.com/bfeedaeedbe9473eacd6ee20d06e832d>

---

**From:** Joanna Waldstreicher <JWaldstreicher@fec.gov>  
**Sent:** Friday, September 14, 2018 4:18 PM  
**To:** Soghoian, Chris (Wyden) <Chris\_Soghoian@wyden.senate.gov>  
**Cc:** Robert Knop <rknop@fec.gov>  
**Subject:** RE: Letter

Chris, thanks for this additional information. We will review it and add it to Sen. Wyden's request.

As a reminder, we post each advisory opinion request to our website and trigger the 60-day deadline for the Commission to respond once the request is complete; that is, once it includes all the information we need to answer the question asked. We will review Prof. Rid's letter to determine whether it provides the necessary information as to the unique cybersecurity threats faced by senators, and if you recall we also asked you to provide some further information about the kinds of expenses Sen. Wyden proposes to use campaign funds for. Please let me know if you have any questions about this.

Best,  
Joanna S. Waldstreicher  
Office of the General Counsel, Policy Division  
Federal Election Commission  
1050 First Street, NE  
Washington, DC 20463  
(202) 694-1650

---

**From:** Soghoian, Chris (Wyden) [[mailto:Chris\\_Soghoian@wyden.senate.gov](mailto:Chris_Soghoian@wyden.senate.gov)]  
**Sent:** Friday, September 14, 2018 3:06 PM  
**To:** Joanna Waldstreicher <[JWaldstreicher@fec.gov](mailto:JWaldstreicher@fec.gov)>  
**Subject:** FW: Letter

Joanna,

Senator Wyden received this letter today from Professor Thomas Rid of Johns Hopkins University, addressing the question of whether Senators face unique cybersecurity threats due to their roles as elected officials.

Professor Rid previously testified at an open hearing before the Senate Intelligence Committee in March, 2017 on the topic of Russian Active Measures. A copy of his testimony can be accessed here:

<https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf>

Would you please add Dr. Rid's letter to the folder associated with Senator Wyden's original FEC request and then docket the request and accompanying materials, so that they can be considered soon by the Commission?

Thanks,

Chris

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

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](http://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

AOR025

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.

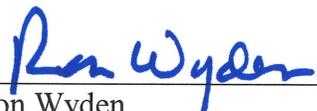
The Senate, meanwhile, has only established a working group to "identify, develop, and recommend options to provide enhanced cybersecurity for Senators' personal communications devices and accounts."

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  
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](http://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.

A handwritten signature in black ink, appearing to read "Michael S. Rogers", with a long horizontal flourish extending to the right.

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



# State-backed hackers target Gmail of US senators, aides

AP NEWS | Sign up

AP Top News Sports Entertainment Explore ▼

By FRANK BAJAK and  
RAPHAEL SATTER

Sep. 20, 2018



<https://apn>

## RELATED TOPICS

[Ron Wyden](#)

[Technology](#)

[Politics](#)

[Oregon](#)

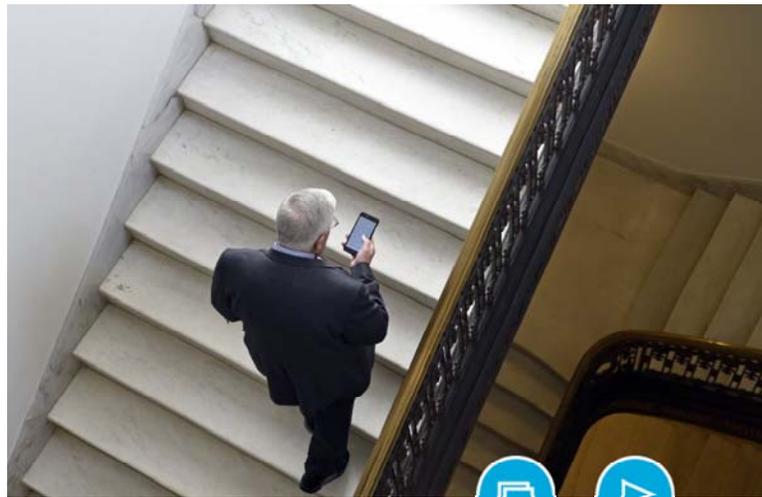
[North America](#)

[Business](#)

[Email](#)

More from

[AP Top News](#)



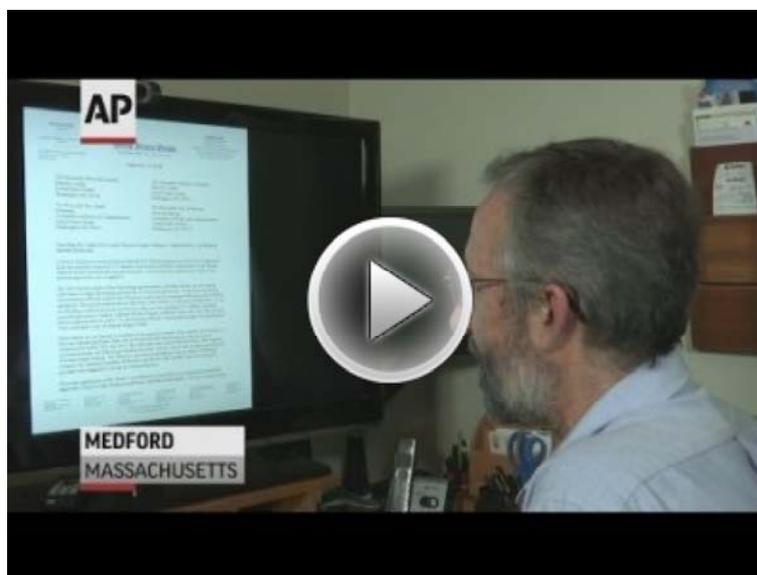
State-backed hackers are still trying to break into the personal email accounts of U.S. senators and their aides — and a lawmaker focused on cybersecurity says the Senate’s security office should stop refusing to help defend them.

Sen. Ron Wyden, an Oregon Democrat, said in a [Wednesday letter to Senate leaders](#) that his office discovered that “at least one major technology company” has warned an unspecified number of senators and aides that their personal email accounts were “targeted by foreign government hackers.”

On Thursday, Google spokesman Aaron Stein confirmed that his company had notified the Senate targets.

Neither Stein nor Wyden provided any indication as to who might be behind the attempted break-ins, whether they targeted lawmakers from both political parties or their timing, though a Senate staffer said they occurred “in the last few weeks or months.” The aide spoke on condition of anonymity because he was not authorized to discuss the issue publicly.

Email theft is favored by hackers the world over, including the Russian military agents accused of leaking the content of Democrats’ inboxes ahead of the 2016 elections, and personal accounts have proven to be the easiest targets.



A U.S. lawmaker says foreign government hackers continue to target the personal accounts of U.S. senators and their aides – and that the Senate’s security office won’t help defend them. (Sept. 19)

Wyden noted that the [Office of the Sergeant at Arms](#) , which oversees Senate security, had [informed legislators and staffers](#) that it has no authority to help secure personal, rather than official, accounts.

“This must change,” Wyden wrote in the letter. “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.”

A spokeswoman for the security office said it would have no comment.

Wyden has proposed legislation that would [allow the security office to offer digital protection](#) for personal accounts and devices, the same way it does with official ones.

The Wyden letter cites previous Associated Press reporting on the Russian hacking group known as Fancy Bear and how it targeted the personal accounts of congressional aides between 2015 and 2016. The group's prolific cyberspying targeted the Gmail accounts of current and former Senate staffers, including Robert Zarate, now national security adviser to Florida Sen. Marco Rubio, and Jason Thielman, chief of staff to Montana Sen. Steve Daines, the AP found.

The same group also spent the second half of [2017 laying digital traps](#) intended to look like portals where Senate officials enter their work email credentials, the Tokyo-based cybersecurity firm TrendMicro has reported.

Microsoft seized some of those traps, and in September 2017 apparently thwarted an attempt to [steal login credentials of a policy aide to Missouri Sen. Claire McCaskill](#), the Daily Beast discovered in July. Last month, Microsoft made news again when it [seized several internet domains](#) linked to Fancy Bear, including two apparently aimed at conservative think tanks in Washington.

Such incidents “only scratch the surface” of advanced cyberthreats faced by U.S. officials in the administration and Congress, according to Thomas Rid, a cybersecurity expert at Johns Hopkins University. Rid made the statement [in a letter to Wyden last week](#).

“The personal accounts of senators and their staff are high-value, low-hanging targets,” Rid wrote. “No rules, no regulations, no funding streams, no mandatory training,

no systematic security support is available to secure these resources.”

Attempts to breach such accounts were a major feature of the yearlong AP investigation into Fancy Bear that identified hundreds of senior officials and politicians — including former secretaries of state, top generals and intelligence chiefs — whose Gmail accounts were targeted.

The Kremlin is by no means the only source of worry, said Matt Tait, a University of Texas cybersecurity fellow and former British intelligence official.

“There are lots of countries that are interested in what legislators are thinking, what they’re doing, how to influence them, and it’s not just for purposes of dumping their information online,” Tait said.

In an April 12 letter released by Wyden’s office, Adm. Michael Rogers — then director of the National Security Agency — acknowledged that personal accounts of senior government officials “remain prime targets for exploitation” and said that officials at the NSA and Department for Homeland Security were discussing ways to better protect them. The NSA and DHS declined to offer further details.

Wyden said Thursday that state-backed hackers “are like burglars who are knocking on windows and doors. They are out knocking on a lot of them right now just looking for an opportunity to get through.”

Guarding personal accounts is a complex, many-layered challenge.

Boosting protection in the Senate could begin with the distribution of small chip-based security devices such as the YubiKey, which are already used in many secure corporate and government environments, Tait said. Such

keys supplement passwords to authenticate legitimate users, potentially frustrating distant hackers.

Cybersecurity experts also recommend them for high-value cyber-espionage targets including human rights workers and journalists.

“In an ideal world, the Sergeant at Arms could just have a pile of YubiKeys,” said Tait. “When legislators or staff come in they can (get) a quick cybersecurity briefing and pick up a couple of these for their personal accounts and their official accounts.”

---

Bajak reported from Boston. Satter reported from London. AP video journalist Gillian Flaccus contributed from Portland, Oregon.



## GOP looking more confident on Kavanaugh after FBI report

an hour ago



## Joanna Waldstreicher

---

**From:** Soghoian, Chris (Wyden) <Chris\_Soghoian@wyden.senate.gov>  
**Sent:** Wednesday, October 03, 2018 11:48 AM  
**To:** Joanna Waldstreicher  
**Subject:** Cybersecurity supplement letter from Senator Wyden  
**Attachments:** wyden-fec-cybersecurity-example-expenses-letter.pdf

Joanna,

Please see the attached letter from Senator Wyden. Let me know if you have any problems opening it.

Regards,

Chris

Christopher Soghoian, Ph.D.  
Senior Technologist, Senior Advisor for Privacy & Cybersecurity  
Senator Ron Wyden  
221 Dirksen Senate Building  
(202) 224-5244

United States Senate  
WASHINGTON, DC 20510-3703

October 3, 2018

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

Dear Ms. Hunter:

I write to supplement my May 16, 2018 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.

After I submitted my request, the FEC's Office of General Counsel informed my staff that the FEC required specific examples of the kinds of cybersecurity-related expenses that Members of Congress might reasonably incur in order to protect themselves from or recover from cyber-attacks by sophisticated foreign government hackers.

After consulting with a number of cybersecurity experts, I have put together the table below. This is by no means an exhaustive list, but is instead intended to provide illustrative examples in response to the FEC Office of General Counsel's request.

What type of investment	How this increases security
<p><b>Hardware</b></p> <ol style="list-style-type: none"> <li>1. Dedicated secure cell phones, computers, and hotspots</li> <li>2. Secure home routers and networking equipment</li> <li>3. Security tokens and 'keys'</li> </ol>	<ol style="list-style-type: none"> <li>1. Dedicated devices are an important cybersecurity measure, by enabling their owner to compartmentalize information and therefore limit information loss when a device is compromised. Some devices, such as specific cellphones and computers, have additional security features.</li> <li>2. Home routers are a known target for hackers. A home router that receives automatic updates can help to mitigate this risk.</li> <li>3. Physical security tokens are a more secure method of two-factor authentication and are more resistant to phishing attacks than using cellular text messages or email for authentication. Given the frequency and effectiveness of Russia's phishing attacks</li> </ol>

	<p>against U.S. political targets in 2016, it is strongly advisable for individuals who are likely targets of foreign government cyber attacks to use two-factor authentication with a physical security token.</p>
<p><b>Personal software and apps</b></p> <ol style="list-style-type: none"> <li>1. Endpoint protection, firewall, and antivirus software</li> <li>2. Password management tools</li> <li>3. Secure, encrypted backup and cloud services</li> <li>4. Secure, encrypted chat, group chat, e-mail, and project management tools</li> </ol>	<ol style="list-style-type: none"> <li>1. Security software can help reduce the threat of malware and phishing attacks, as well as network-based hacking.</li> <li>2. Password managers enable users to easily create and manage unique passwords for each website.</li> <li>3. Insecure cloud services are frequent targets of hackers. Securing these services and ensuring reliable backups can protect against hacks, including reducing the harm caused by a ransomware infection.</li> <li>4. Coupling dedicated secure communications devices (cell phones, computers) with trusted and secure messaging applications can enable more secure communication.</li> </ol>
<p><b>Consulting services</b></p> <ol style="list-style-type: none"> <li>1. Services from cybersecurity professionals and consultants</li> <li>2. Professionally-managed security services, such as endpoint detection &amp; response, anti-malware, anti-phishing, firewall, and exploit protection</li> </ol>	<ol style="list-style-type: none"> <li>1. High-value targets, like elected officials, should use technology that has been subjected to regular audits, and is protected by network devices, security appliances, and services that are managed professionally. Security experts should regularly review security alerts and logs.</li> <li>2. Enterprise security services can more effectively identify and block sophisticated or persistent attackers.</li> </ol>
<p><b>Emergency assistance</b> Professional incident response, mitigation, and remediation services</p>	<p>Once a cyber attack has been identified, services like these are essential to identify the damage, stop the threat, and remediate the impact.</p>

If you require any further information as you consider my May 16, 2018 request, please contact Chris Soghoian in my office.

Sincerely,

  
 Ron Wyden  
 United States Senator