

RECEIVED

By Office of the Commission Secretary at 1:15 pm, Dec 12, 2018



FEDERAL ELECTION COMMISSION
Washington, DC 20463

AGENDA DOCUMENT NO. 18-46-B
AGENDA ITEM
For meeting of December 13, 2018
Submitted Late

December 12, 2018

MEMORANDUM

TO: The Commission

FROM: Lisa J. Stevenson *LJS by CDG*
Acting General Counsel

Neven F. Stipanovic *NFS by CDG*
Acting Associate General Counsel

Robert M. Knop *RMK by CDG*
Assistant General Counsel

Joanna S. Waldstreicher *JSW*
Attorney

Subject: AO 2018-15 (Wyden) Draft B

Attached is a proposed draft of the subject advisory opinion.

Members of the public may submit written comments on the draft advisory opinion. We are making this draft available for comment until 9:00 am (Eastern Time) on December 13, 2018.

For more information about how to submit comments or attend the Commission meeting, go to <https://www.fec.gov/legal-resources/advisory-opinions-process/>

Attachment

1 ADVISORY OPINION 2018-15
2
3 The Honorable Ron Wyden
4 221 Dirksen Senate Office Building
5 Washington, DC 20510

DRAFT B

6
7 Dear Sen. Wyden:

8 We are responding to your advisory opinion request concerning the application of the
9 Federal Election Campaign Act, 52 U.S.C. §§ 30101-45 (the “Act”), and Commission
10 regulations to your proposal to use campaign funds to protect your personal electronic devices
11 and accounts from cyber threats you face in your role as an elected official.¹ The Commission
12 concludes that you may use campaign funds to pay for the costs of security measures to protect
13 your personal devices and accounts without such payments constituting an impermissible
14 conversion of campaign funds to personal use, under the Act and Commission regulations.

15 **Background**

16 The facts presented in this advisory opinion are based on your letter received on May 16,
17 2018, and emails and attachments received from your office on June 6, September 14, September
18 20, and October 3, 2018.

19 You are a United States Senator from Oregon. While you do not report any specific
20 threats against your personal electronic devices or accounts,² you note “the dangers elected
21 officials face in the cyber realm, including attacks by sophisticated state-sponsored hackers and
22 intelligence agencies against personal devices and accounts.” Advisory Opinion Request at

¹ Although your advisory opinion request is framed on behalf of Members of Congress generally, the Commission may only address your individual circumstances and proposed activities. *See* 52 U.S.C. § 30108; 11 C.F.R. § 112.1(b). However, the Commission notes that any person similarly situated may rely on this advisory opinion’s conclusion. 52 U.S.C. § 30108(c)(1)(B); 11 C.F.R. § 112.5(a)(2).

² In a letter to Senate leaders included with your advisory opinion request, you stated that your office has “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” but you do not indicate whether you or your staff received such a notification. AOR025.

1 AOR001. Michael Rogers, then director of the National Security Agency, agreed that the
2 personal devices and accounts of senior U.S. government officials “remain prime targets for
3 exploitation,” AOR002, and Dan Coats, Director of National Intelligence, has testified that “[t]he
4 personal accounts and devices of government officials can contain information that is useful for
5 our adversaries to target.” AOR008. The Senate Appropriations Committee has also expressed
6 its concern “that Senators are being targeted for hacking and cyberattacks, especially via their
7 personal devices and accounts.” AOR017.

8 In your request, you cite to Professor Thomas Rid, a cybersecurity expert at Johns
9 Hopkins University’s School of Advanced International Studies, who analyzed the cybersecurity
10 risk to federal officeholders as distinguished from the risk to other individuals. He notes that
11 although for-profit criminals target many individuals with identity theft, ransomware, spyware,
12 phishing attacks and other cyber threats, “senior executive branch officials and Members of
13 Congress face additional, targeted threats from sophisticated, persistent, and often well-funded
14 adversaries” who seek sensitive information or weaknesses in our defenses. AOR019.

15 Professor Rid further states that officeholders’ personal accounts and devices are at
16 particular risk because their personal accounts “are outside the official security perimeter of the
17 U.S. government, yet contain highly sensitive information about officials’ activities, private
18 communications, family life, finances, and movements. Personal accounts are often much softer
19 targets because the user determines the security settings, not cybersecurity professionals.”
20 AOR021. In other words, “the personal accounts of Senators and their staff are high-value, low-
21 hanging targets.” *Id.*

1 You propose to use campaign funds for several types of expenses you might reasonably
2 incur in order to protect your personal devices and accounts or to recover from cyberattacks.
3 These include but are not limited to: (1) hardware, such as dedicated secure cell phones and
4 computers, secure home routers and networking equipment, and security tokens and “keys”; (2)
5 personal software and apps, such as endpoint protection, firewall, and antivirus software,
6 password management tools, secure and encrypted backup and cloud services, and secure and
7 encrypted chat, email, and project management tools; (3) consulting services from cybersecurity
8 professionals, and professionally-managed security services such as endpoint detection and
9 response, anti-malware, anti-phishing, firewall, and exploit protection; and (4) emergency
10 assistance, such as professional incident response, mitigation, and remediation services.

11 AOR036.

12 **Question Presented**

13 *May a United States Senator use campaign funds to pay for the costs of cybersecurity*
14 *measures to protect his personal electronic devices and accounts?*

15 **Legal Analysis and Conclusions**

16 Yes, you may use campaign funds to pay for cybersecurity protection for your personal
17 devices and accounts. Such expenses fall within the uses defined as permissible under the Act:
18 ordinary and necessary expenses incurred in connection with the duties of the individual as a
19 holder of federal office. 52 U.S.C. § 30114(a)(2).

20 The Act and Commission regulations permit a federal officeholder to use campaign funds
21 for a variety of enumerated purposes, including “ordinary and necessary expenses incurred in
22 connection with duties of the individual as a holder of Federal office,” and for “any other lawful

1 purpose” that does not constitute conversion of campaign funds to “personal use.” 52 U.S.C.
2 § 30114(b)(1); 11 C.F.R. § 113.2(e). Conversion to personal use occurs when a contribution or
3 amount is used “to fulfill any commitment, obligation, or expense” of a federal officeholder “that
4 would exist irrespective” of the officeholder’s duties. 52 U.S.C. § 30114(b)(2); *see also* 11
5 C.F.R. § 113.1(g).

6 The Act and Commission regulations provide a non-exhaustive list of items that would
7 constitute a prohibited personal use *per se*, none of which applies here. *See* 52 U.S.C.
8 § 30114(b)(2)(A)-(I); 11 C.F.R. § 113.1(g)(1)(i)(A)-(J). For items not on this list, such as
9 payments for cybersecurity measures for personal electronic devices and accounts, the
10 Commission determines on a case-by-case basis whether such expenses would fall within the
11 definition of “personal use.” 11 C.F.R. § 113.1(g)(1)(ii). The Commission has long recognized
12 that if a candidate or federal officeholder “can reasonably show that the expenses at issue
13 resulted from campaign or officeholder activities, the Commission will not consider the use to be
14 personal use.” Personal Use of Campaign Funds, 60 Fed. Reg. 7682, 7867 (Feb. 9, 1995).

15 The Commission has not previously considered whether payments for cybersecurity
16 measures would constitute personal use of campaign funds under the Act and Commission
17 regulations. The Commission has, however, previously concluded that payments for physical
18 protection of a federal officeholder or candidate’s residence do not constitute personal use when
19 such protection is needed due to threats driven by the individuals’ roles as officeholders. In
20 Advisory Opinion 2011-17 (Giffords), Advisory Opinion 2011-05 (Terry), and Advisory
21 Opinion 2009-08 (Gallegly), federal officeholders faced “specific and ongoing threats to the
22 safety of themselves and their families,” and the information provided suggested that “the threats

1 were motivated by the Members' public roles as federal officeholders and/or candidates."
2 Advisory Opinion 2017-07 (Sergeant at Arms) at 3. The Commission concluded in those
3 instances that "the threats would not have occurred had the Members not been federal
4 officeholders and/or candidates, and that the expenses for the proposed residential security
5 upgrades would not exist irrespective of their duties as federal officeholders and/or candidates."

6 *Id.*

7 In Advisory Opinion 2017-07 (Sergeant at Arms), the Commission considered similar
8 residential security issues pertaining to all Members of Congress. Based on information
9 regarding "the current threat environment facing Members of Congress due to their status as
10 federal officeholders" as well as a threat assessment completed by the United States Capitol
11 Police recommending that all Members of Congress upgrade their residential security, the
12 Commission concluded that the need for such increased security would not have existed
13 irrespective of the Members' roles as federal officeholders. Advisory Opinion 2017-07
14 (Sergeant at Arms) at 3. Therefore the use of campaign funds to pay for the recommended
15 residential security installation or upgrades would not constitute an impermissible personal use
16 of campaign contributions under the Act and Commission regulations. *Id.*

17 Similarly, you have provided information regarding the heightened threat of cyberattacks
18 you face with respect to your personal electronic devices and accounts by virtue of your role as a
19 federal officeholder. As Professor Rid opined, "the personal accounts of Senators and their staff
20 are high-value . . . targets" because they "contain highly sensitive information about officials'
21 activities, private communications, family life, finances, and movements." AOR021. The value
22 of such information means that the personal electronic devices and accounts of Senators are more

1 likely to be the targets of hackers and foreign actors than are those of other individuals, and both
2 the heightened risk to Senators' personal electronic devices and accounts and the magnitude of
3 the potential harm would not exist if not for their roles as federal officeholders. Accordingly, the
4 reasonable expenses incurred in protecting your personal electronic devices and accounts from,
5 and responding to, cybersecurity threats, as described in your advisory opinion request,
6 constitute ordinary and necessary expenses incurred in connection with your duties as a holder of
7 federal office, which are a permissible use of campaign funds. These expenses must be
8 reported as "cybersecurity expenses" on campaign-finance reports; simultaneously with the
9 approval of this Advisory Opinion, the Commission will add "cybersecurity expenses" to its
10 list of reporting purposes deemed "adequate" for campaign disbursements.³

11 The Commission emphasizes that this conclusion is based on the information provided
12 about the current heightened threat environment of cyberattacks faced by Senators, and that if
13 that threat environment should diminish significantly at some point in the future, this conclusion
14 may no longer apply. In addition, the Commission emphasizes that the use of campaign funds
15 for the expenses described in your request is limited to your own personal devices and accounts
16 and not available for devices and accounts of family members, staff or other persons.

17 This response constitutes an advisory opinion concerning the application of the Act and
18 Commission regulations to the specific transaction or activity set forth in your request. *See*
19 52 U.S.C. § 30108. The Commission emphasizes that, if there is a change in any of the facts or
20 assumptions presented, and such facts or assumptions are material to a conclusion presented in

³ The Commission assumes that your campaign committee will pay the fair market value of any such cybersecurity hardware, software, or services to prevent the acceptance of potentially impermissible in-kind contributions from vendors.

1 this advisory opinion, then the requestor may not rely on that conclusion as support for its
2 proposed activity. Any person involved in any specific transaction or activity which is
3 indistinguishable in all its material aspects from the transaction or activity with respect to which
4 this advisory opinion is rendered may rely on this advisory opinion. *See* 52 U.S.C.
5 § 30108(c)(1)(B). Please note that the analysis or conclusions in this advisory opinion may be
6 affected by subsequent developments in the law including, but not limited to, statutes,
7 regulations, advisory opinions, and case law. Any advisory opinions cited herein are available
8 on the Commission's website.

9

10
11
12
13
14
15

On behalf of the Commission,

Caroline C. Hunter,
Chair