FEDERAL ELECTION COMMISSION
WASHINGTON, D.C. 20463

December 13, 2018

CERTIFIED MAIL
RETURN RECEIPT REQUESTED

ADVISORY OPINION 2018-15

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

Dear Sen. Wyden:

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

Background

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

You are a United States Senator from Oregon. While you do not report any specific threats against your personal electronic devices or accounts,[2] you note "the dangers elected officials face in the cyber realm, including attacks by sophisticated state-sponsored hackers and

[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.

intelligence agencies against personal devices and accounts." Advisory Opinion Request at AOR001. Michael Rogers, then director of the National Security Agency, agreed that the personal devices and accounts of senior U.S. government officials "remain prime targets for exploitation," AOR002, and Dan Coats, Director of National Intelligence, has testified that "[t]he personal accounts and devices of government officials can contain information that is useful for our adversaries to target." AOR008. The Senate Appropriations Committee has also expressed its concern "that Senators are being targeted for hacking and cyberattacks, especially via their personal devices and accounts." AOR017.

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

Professor Rid further states that officeholders' personal accounts and devices are at particular risk because their personal 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." AOR021. In other words, "the personal accounts of Senators and their staff are high-value, low-hanging targets." *Id.*

You propose to use campaign funds for several types of expenses you might reasonably incur in order to protect your personal devices and accounts or to recover from cyberattacks. These include but are not limited to: (1) hardware, such as dedicated secure cell phones and computers, secure home routers and networking equipment, and security tokens and "keys"; (2) personal software and apps, such as endpoint protection, firewall, and antivirus software, password management tools, secure and encrypted backup and cloud services, and secure and encrypted chat, email, and project management tools; (3) consulting services from cybersecurity professionals, and professionally managed security services such as endpoint detection and response, anti-malware, anti-phishing, firewall, and exploit protection; and (4) emergency assistance, such as professional incident response, mitigation, and remediation services. AOR036.

Question Presented

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

Legal Analysis and Conclusions

Yes, you may use campaign funds to pay for cybersecurity protection for your personal

devices and accounts. Such expenses fall within the uses defined as permissible under the Act: ordinary and necessary expenses incurred in connection with the duties of the individual as a holder of federal office. 52 U.S.C. § 30114(a)(2).

The Act and Commission regulations permit a federal officeholder to use campaign funds for a variety of enumerated purposes, including "ordinary and necessary expenses incurred in connection with duties of the individual as a holder of Federal office," and for "any other lawful purpose" that does not constitute conversion of campaign funds to "personal use." 52 U.S.C. § 30114(b)(1); 11 C.F.R. § 113.2(e). Conversion to personal use occurs when a contribution or amount is used "to fulfill any commitment, obligation, or expense" of a federal officeholder "that would exist irrespective" of the officeholder's duties. 52 U.S.C. § 30114(b)(2); *see also* 11 C.F.R. § 113.1(g).

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

The Commission has not previously considered whether payments for cybersecurity measures would constitute personal use of campaign funds under the Act and Commission regulations. The Commission has, however, previously concluded that payments for physical protection of a federal officeholder or candidate's residence do not constitute personal use when such protection is needed due to threats driven by the individuals' roles as officeholders. In Advisory Opinion 2011-17 (Giffords), Advisory Opinion 2011-05 (Terry), and Advisory Opinion 2009-08 (Gallegly), federal officeholders faced "specific and ongoing threats to the safety of themselves and their families," and the information provided suggested that "the threats were motivated by the Members' public roles as federal officeholders and/or candidates." Advisory Opinion 2017-07 (Sergeant at Arms) at 3. The Commission concluded in those instances that "the threats would not have occurred had the Members not been federal officeholders and/or candidates, and that the expenses for the proposed residential security upgrades would not exist irrespective of their duties as federal officeholders and/or candidates." *Id.*

In Advisory Opinion 2017-07 (Sergeant at Arms), the Commission considered similar residential security issues pertaining to all Members of Congress. Based on information regarding "the current threat environment facing Members of Congress due to their status as federal officeholders" as well as a threat assessment completed by the United States Capitol Police recommending that all Members of Congress upgrade their residential security, the Commission concluded that the need for such increased security would not have existed irrespective of the Members' roles as federal officeholders. Advisory Opinion 2017-07

(Sergeant at Arms) at 3. Therefore the use of campaign funds to pay for the recommended residential security installation or upgrades would not constitute an impermissible personal use of campaign contributions under the Act and Commission regulations. *Id.*

Similarly, you have provided information regarding the heightened threat of cyberattacks you face with respect to your personal electronic devices and accounts by virtue of your role as a federal officeholder. As Professor Rid opined, "the personal accounts of Senators and their staff are high-value . . . targets" because they "contain highly sensitive information about officials' activities, private communications, family life, finances, and movements." AOR021. The value of such information means that the personal electronic devices and accounts of Senators are more likely to be the targets of hackers and foreign actors than are those of other individuals, and both the heightened risk to Senators' personal electronic devices and accounts and the magnitude of the potential harm would not exist if not for their roles as federal officeholders. Accordingly, the reasonable expenses incurred in protecting your personal electronic devices and accounts from, and responding to, cybersecurity threats, as described in your advisory opinion request, constitute ordinary and necessary expenses incurred in connection with your duties as a holder of federal office, which are a permissible use of campaign funds. These expenses must be reported as "cybersecurity expenses" on campaign-finance reports; simultaneously with the approval of this Advisory Opinion, the Commission will add "cybersecurity expenses" to its list of reporting purposes deemed "adequate" for campaign disbursements.[3]

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

This response constitutes an advisory opinion concerning the application of the Act and Commission regulations to the specific transaction or activity set forth in your request. *See* 52 U.S.C. § 30108. The Commission emphasizes that, if there is a change in any of the facts or assumptions presented, and such facts or assumptions are material to a conclusion presented in this advisory opinion, then the requestor may not rely on that conclusion as support for its proposed activity. Any person involved in any specific transaction or activity which is indistinguishable in all its material aspects from the transaction or activity with respect to which this advisory opinion is rendered may rely on this advisory opinion. *See* 52 U.S.C. § 30108(c)(1)(B). Please note that the analysis or conclusions in this advisory opinion may be affected by subsequent developments in the law including, but not limited to, statutes,

---

[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.

regulations, advisory opinions, and case law. Any advisory opinions cited herein are available on the Commission's website.

On behalf of the Commission,

Caroline C. Hunter,
Chair