



RECEIVED

By Office of General Counsel at 9:52 am, Jul 15, 2022

10 G Street NE, Suite 600 | Washington, DC 20002

RECEIVED

By Office of the Commission Secretary at 9:10 am, Jul 25, 2022

July 14, 2022

BY ELECTRONIC MAIL DELIVERY

Office of General Counsel
Attn: Lisa J. Stevenson, Esq.
Acting General Counsel
Federal Election Commission
1050 First Street NE
Washington, DC 20463
ao@fec.gov

Re: Advisory Opinion Request

Dear Ms. Stevenson:

Pursuant to 52 U.S.C. § 30108, we seek an advisory opinion on behalf of Warren Democrats to confirm that it may pay for reasonable cybersecurity measures to protect Senator Elizabeth Warren’s home network, which connects to her electronic devices and the electronic devices of other members of her household, under the Federal Election Campaign Act of 1971 (the “Act”) and Federal Election Commission (“FEC” or the “Commission”) regulations.

I. FACTUAL DISCUSSION

Warren Democrats, Inc. (the “Committee”) is registered with the FEC as the principal campaign committee of Senator Elizabeth Warren, who is running for re-election to the U.S. Senate in 2024.¹

As a high-profile elected official, Senator Warren faces threats greater than those faced by the general public, including heightened vulnerability to cyberattacks against her electronic devices and accounts. As former Director of National Intelligence Dan Coats testified in a 2018 hearing before the U.S. Senate Select Committee on Intelligence, hackers target the accounts and devices of government officials because they “can contain information that is useful for [U.S.]

¹ FEC, FEC Form 1: Statement of Organization, Warren Democrats, Inc. (March 23, 2020), <https://docquery.fec.gov/pdf/575/202003239215621575/202003239215621575.pdf>.

adversaries.”² In a 2018 opinion, the Commission recognized the “current heightened threat environment of cyberattacks faced by Senators.”³

In fact, in recent years, hackers have repeatedly targeted U.S. government officials, including U.S. Senators. In 2018, foreign government hackers targeted the personal Gmail accounts of several U.S. Senators and their aides.⁴ In 2020, hackers also targeted officials at the U.S. Department of the Treasury.⁵ Cybersecurity experts have warned that government officials continue to be vulnerable to cyberattacks today.⁶

As such, the Committee seeks to pay for reasonable cybersecurity measures to protect Senator Warren’s home network, which connects to her electronic devices, as well as the electronic devices of other members and visitors of her household. Such measures include professionally-managed security services to provide ongoing network monitoring, patch management, backup management, and remote incident remediation services to ensure overall network security. The Commission authorized the use of campaign funds to pay for such services in Advisory Opinion 2018-15, but noted in that instance that campaign funds could not be used to pay for any cybersecurity measures “for devices and accounts of family members, staff, or other persons.”⁷ In the present case, although the Senator will continue to pay personally for internet services to her home, the Committee’s purpose in paying for cybersecurity measures to protect Senator Warren’s home network is to protect the Senator’s accounts and devices. However, such security measures will also benefit members and visitors of Senator Warren’s household, because their devices and accounts also connect to the Senator’s home network.

II. QUESTION POSED

The Committee asks the Commission to confirm that under the Act and Commission regulations, the Committee may pay for reasonable cybersecurity services to protect the Senator’s home network, which connects to her electronic devices and the electronic devices of other members and visitors of her household.

² FEC, Adv. Op. Request 2018-15 (Wyden) at AOR008, https://www.fec.gov/files/legal/aos/2018-15/201815R_1.pdf.

³ FEC, Adv. Op. 2018-15 at 4 (Wyden), <https://www.fec.gov/files/legal/aos/2018-15/2018-15.pdf>.

⁴ Frank Bajak and Raphael Satter, *State-backed hackers target Gmail of US senators, aides*, Associated Press (Sept. 20, 2018), <https://apnews.com/article/bfeedaedbe9473eacd6ee20d06e832d>.

⁵ Raphael Satter, *‘Dozens of email accounts’ were hacked at U.S. Treasury -Senator Wyden*, Reuters (Dec. 21, 2020), <https://www.reuters.com/article/us-global-cyber-idCAKBN28V2DX>.

⁶ Maggie Miller, *Why we can expect more hacking of politicians’ phones*, Politico (May 31, 2022), <https://www.politico.com/news/2022/05/31/hacking-politicians-phones-00035848>.

⁷ FEC, Adv. Op. 2018-15 at 4 (Wyden), <https://www.fec.gov/files/legal/aos/2018-15/2018-15.pdf>.

III. LEGAL ANALYSIS

The Act and Commission regulations permit Members to use campaign funds to pay for reasonable cybersecurity measures to secure their home network that connects to their electronic devices, even if the network also connects to the electronic devices of other members and visitors of their household.

Federal law prohibits using candidate committee funds for any individual's "personal use."⁸ The term "personal use" means "any use of funds in a campaign account . . . to fulfill a commitment, obligation or expense of any person that would exist irrespective of the candidate's campaign or duties as a Federal officeholder."⁹ While certain expenses automatically qualify as a prohibited personal use, other expenses are subject to a case-by-case determination. If the expense would exist irrespective of candidacy or official duties, campaign funds may not be used to pay for it; alternatively, if the expense would not exist irrespective of candidacy or official duties, campaign funds may be used to pay for it.¹⁰

Payments for residential cybersecurity measures are not included as a prohibited *per se* personal use.¹¹ Accordingly, campaign funds may be used to pay for such measures if the expense would not exist irrespective of the Senator's candidacy or official duties.

For Members of Congress, the Commission has already held that the purchase of residential security systems is a permissible use of campaign funds. In 2017, the U.S. Capitol Police recommended that all Members upgrade their residential security due to a heightened threat environment. Pursuant to this recommendation, the FEC expressly authorized Members to use campaign funds to pay for costs associated with residential security systems that are not structural improvements, without such use constituting personal use of campaign funds.¹² A Member does not need to face a specific or ongoing threat or obtain an individualized assessment from U.S. Capitol Police in order to purchase a non-structural residential security system, such as the installation or upgrade and monitoring costs of cameras, sensors, distress devices, and similar non-structural security devices, as well as locks, in and around a Member's residence.¹³

In 2018, the FEC recognized that Members also face a heightened threat environment of cyberattacks, and issued an advisory opinion permitting Members to also use campaign funds to pay for cybersecurity measures to secure their personal electronic devices and accounts.¹⁴ The

⁸ 52 U.S.C. § 30114(b)(1).

⁹ 11 C.F.R. § 113.1(g).

¹⁰ 11 C.F.R. §§ 113.2(e); 113.1(g).

¹¹ 11 C.F.R. § 113.1(g)(1)(i)(A)-(J).

¹² FEC Adv. Op. 2017-7 (Sergeant at Arms), <https://www.fec.gov/files/legal/aos/2017-07/2017-07.pdf>.

¹³ *Id.*

¹⁴ FEC Adv. Op. 2018-15 (Wyden), <https://www.fec.gov/data/legal/advisory-opinions/2018-15/>.

FEC held 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.”¹⁵ As a result, the Commission authorized the use of campaign funds to pay for reasonable expenses incurred in protecting a Member’s personal electronic devices and accounts from, and responding to, cybersecurity threats.¹⁶

By extension, the Commission should find that it is permissible for the Committee to pay for reasonable cybersecurity measures to secure the Senator’s home network that connects to her electronic devices and accounts, including professionally-managed security services to provide ongoing network monitoring, patch management, backup management, and remote incident remediation services to ensure overall network security. The use of campaign funds for such expenses remains permissible even if the network also connects to the electronic devices and accounts of other members and visitors of the Senator’s household. The heightened risk to the Senator’s home network would not exist if not for the Senator’s role as a federal officeholder and candidate, and the Committee’s purpose in paying for the cybersecurity measures is to specifically protect the devices and accounts of the Senator; other household members or visitors connecting to the Senator’s home network only benefit as third-party beneficiaries. Just as the use of campaign funds for cameras or locks around a Member’s residence is permissible even as other members of the Member’s household also benefit from such measures as third-party beneficiaries, the use of campaign funds for cybersecurity measures to protect home networks that connect to the Senator’s electronic devices and accounts is permissible even as other members of the Senator’s household may benefit from such measures as third-party beneficiaries.

For those reasons, we ask the Commission to confirm that the Committee may use its funds to pay for reasonable cybersecurity measures to protect Senator Warren’s home network, which connects to her electronic devices and accounts, and the electronic devices and accounts of other members and visitors of her household.

¹⁵ *Id.* at 4.

¹⁶ *Id.*

Office of the General Counsel
July 14, 2022
Page 5

Very truly yours,

A handwritten signature in blue ink, appearing to read "Kate Sawyer Keane". The signature is fluid and cursive, with a long horizontal flourish extending to the right.

Kate Sawyer Keane
Sarah N. Mahmood

Counsel to Warren Democrats, Inc.