Date of Hearing: March 27, 2019

ASSEMBLY COMMITTEE ON ELECTIONS AND REDISTRICTING
Marc Berman, Chair
AB 1043 (Irwin) – As Introduced February 21, 2019

SUBJECT: Political Reform Act of 1974: campaign funds: cybersecurity.

SUMMARY: Permits campaign funds to be used for costs related to the cybersecurity of electronic devices of a candidate, elected officer, or campaign worker. Specifically, **this bill**:

1) Permits campaign funds to be used to pay for, or reimburse the state for, the costs of installing and monitoring hardware, software, or services related to the cybersecurity of electronic devices of a candidate, elected officer, or campaign worker. Requires a candidate or elected officer to report any expenditure of campaign funds made for these purposes in the candidate's or officer's campaign disclosure reports.

2) Contains the following findings and declarations:

    a) The integrity of state and local officials' political campaigns is of critical importance to ensuring free and fair elections in the state.

    b) Officeholders, candidates, and those assisting with campaigns have become targets of efforts to breach the confidentiality, integrity, and availability of electronic devices with sensitive campaign information.

    c) The Federal Election Commission (FEC) adopted an advisory opinion last December that concluded that it is permissible under federal campaign law for federal officeholders to use campaign funds to pay for cybersecurity protection for personal devices and accounts.

    d) State and local officials in California are similarly situated to federal officeholders as high-value targets for hacking and other cyberattacks.

    e) Clarity in California law regarding the propriety of using campaign funds for cybersecurity is necessary to ensure officeholders and candidates take appropriate action to secure themselves and their campaigns.

EXISTING LAW:

1) Creates the Fair Political Practices Commission (FPPC), and makes it responsible for the impartial, effective administration and implementation of the Political Reform Act (PRA).

2) Requires expenditures of campaign funds to be reasonably related to a political, legislative, or governmental purpose. Requires an expenditure of campaign funds that confers a substantial personal benefit on any individual with authority to approve the expenditure of campaign funds to be directly related to a political, legislative, or governmental purpose.

3) Prohibits the use of campaign funds for payment or reimbursement for the lease of real property or for the purchase, lease, or refurbishment of any appliance or equipment if the

lessee or sub lessor is, or the legal title resides in, a candidate, elected officer, campaign treasurer, any individual with authority to approve the expenditure of campaign funds, or a member of the immediate family of any of the previously mentioned individuals. Permits campaign funds to be used, notwithstanding this prohibition, to pay or reimburse the state for the costs of installing and monitoring an electronic security system in a candidate or elected officer's home or office, as specified.

4) Provides that the expenditure of campaign funds for real property, an appliance, or equipment is considered to be directly related to a political, legislative, or governmental purpose as long as its use for other purposes is only incidental to its use for political, legislative, or governmental purposes.

FISCAL EFFECT: None. This bill is keyed non-fiscal by the Legislative Counsel.

COMMENTS:

1) **Purpose of the Bill**: According to the author:

> In addition to the widely publicized hacking of emails related to the presidential campaign of 2016, three California candidates for the US House of Representatives were targets of cyberattacks in 2018, marking just the tip of the iceberg of a widespread and growing threat.
>
> According to cybersecurity expert and Professor of Strategic Studies at Johns Hopkins Thomas Rid, cyber criminals often focus on profiting from their victims through identity theft, fraud, and other scams. Elected officials and candidates for public office, however, face additional threats from sophisticated, persistent, and often well-funded adversaries due to their access to sensitive and personal information.
>
> AB 1043 builds on the guidelines established in a recent advisory opinion by the Federal Election[] Commission by allowing candidates and their campaigns to purchase cybersecurity services and technologies with campaign funds. By providing candidates and their campaigns the means to guard against malicious cyberattacks, this bill will help safeguard the integrity of our elections and democracy.

2) **Joint Informational Hearing on Election Cybersecurity**: Last year, this committee held a Joint Informational Hearing with the Senate Committee on Elections & Constitutional Amendments on the topic of Cybersecurity and California Elections. In light of the increased focus on election security since the 2016 elections, the purpose of the hearing was to explore California's policies for protecting the security of our elections systems in an environment where the number and sophistication of threats to our election infrastructure continues to increase. Witnesses that participated in the hearing included the Secretary of State (SOS), a member of the United States Election Assistance Commission, three California county elections officials, the former Senior Director for Cybersecurity Policy at The White House, and a Senior Advisor and Past President to a nonprofit organization that advocates for legislation and regulation that promotes accuracy, transparency and verifiability of elections.

Witnesses at the hearing generally agreed that there was no evidence to suggest that voting machines or vote tallying in California were compromised during the 2016 election. Nonetheless, all of the witnesses stressed the importance of continuing to evaluate cyber and other security threats to election infrastructure and to regularly evaluate processes and procedures to protect against those threats and to promote voter confidence in the accuracy of election results. Among other testimony, one witness at the hearing emphasized the importance of political campaigns implementing cybersecurity best practices to protect their systems and data.

3) **Restrictions on the Use of Campaign Funds**: As detailed above, existing law generally requires expenditures of campaign funds to be either *reasonably* related to a political, legislative, or governmental purpose, or *directly* related to a political, legislative, or governmental purpose in situations where the expenditure confers a substantial personal benefit on any individual with authority to approve the expenditure of campaign funds.

   The FPPC does not appear to have directly opined on the question of whether campaign funds may be used for cybersecurity hardware, software, and services as would be expressly permitted by this bill. Nonetheless, the purchase of such services and products to protect a candidate's personal electronic device could confer a substantial personal benefit on the candidate. If that was the case, existing law would require that the expenditure of funds on cybersecurity products or services be *directly* related to a political, legislative, or governmental purpose. Furthermore, to the extent that cybersecurity-related *equipment* is purchased using campaign funds, existing law provides that such an expenditure is directly related to a political, legislative, or governmental purpose if its use for other purposes is only incidental to its use for political, legislative, or governmental purposes. By regulation, the FPPC has specified that the use of appliances and equipment for personal purposes is incidental if the use occurs in conjunction with its use for political, legislative, or governmental purposes and constitutes only five percent or less of the total use of the item in any one calendar month with a value of less than $100.

   Increasingly, individuals (including candidates) use electronic devices such as smartphones, personal computers, and tablets both for personal purposes and for business purposes. Elected officials and candidates often use their personal electronic devices for personal use, campaign use, and for business purposes (including official governmental business). Accordingly, any expenditure of funds relating to the cybersecurity of those devices may have more than an incidental use for purposes other than political, legislative, or governmental purposes. In such a case, the FPPC could conclude that the expenditure of campaign funds for cybersecurity products or services is not permitted under existing law.

   In recognition of the fact that public officials may face threats to their security as a result of their political, legislative, or governmental activities, state law already includes one specific exception to the otherwise generally-applicable rules governing the expenditure of campaign funds. Specifically, state law allows campaign funds to be used for the costs of installing and monitoring an electronic security system in the home or office of a candidate or elected officer who has received threats to their physical safety, as specified. That law came about through the passage of SB 771 (Rosenthal), Chapter 1143, Statutes of 1993. SB 771 was enacted after the FPPC issued an advice letter concluding that the installation of a security system at the personal residence of a public official was not a permissible use of campaign funds because the security system would "serve a substantial function in protecting the

official's personal possessions," and consequently "the personal use of the system would be more than merely incidental."

4) **Federal Election Commission Opinion**: As referenced in the author's statement above and in the findings and declarations of this bill, last December, the FEC issued an advisory opinion in response to a request from Senator Ron Wyden in which the FEC concluded that the use of campaign funds to pay for the costs of security measures to protect the personal devices and accounts of certain federal officeholders is a permissible use of campaign funds. Under federal campaign finance laws, campaign funds may not be used for expenses that would constitute the conversion of campaign funds to "personal use." Conversion to personal use is considered to occur if campaign funds are used for expenses "that would exist irrespective" of an officeholder's or candidate's duties.

   In concluding that certain federal officials may permissibly use campaign funds for cybersecurity measures to protect the personal devices and accounts of officeholders, the FEC cited evidence that elected federal officials faced "a heightened threat of cyberattacks…with respect to [their] personal electronic devices and accounts by virtue of [their] role" as officeholders. The advisory opinion quoted information from a cybersecurity expert at Johns Hopkins University's School of Advanced International Studies who opined that "the personal accounts of Senators and their staff are high-value…targets" because those accounts "contain highly sensitive information about officials' activities, private communications, family life, finances, and movements." Accordingly, the FEC concluded 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."

5) **Related Legislation**: AB 1044 (Irwin), which is also being heard in this committee today, authorizes the SOS to require a person who applies to receive voter registration information, as specified, to take a training course regarding data security as a condition for the receipt of that information.

6) **Previous Legislation**: AB 1678 (Berman), Chapter 96, Statutes of 2018, required the SOS to adopt regulations that describe the best practices for storage and security of voter registration information, and required a person who received voter registration information, as specified, to disclose breaches in the security of the storage of that information, among other provisions.

   AB 3075 (Berman), Chapter 241, Statutes of 2018, created the Office of Elections Cybersecurity within the Office of the SOS, and charged it with coordinating efforts to reduce the likelihood and severity of cyber incidents that interfere with election security or integrity, among other responsibilities.

7) **Political Reform Act of 1974**: California voters passed an initiative, Proposition 9, in 1974 that created the FPPC and codified significant restrictions and prohibitions on candidates, officeholders, and lobbyists. That initiative is commonly known as the PRA. Amendments to the PRA that are not submitted to the voters, such as those contained in this bill, must further the purposes of the initiative and require a two-thirds vote of both houses of the Legislature.

8) **Double-Referral**: This bill has been double-referred to the Assembly Committee on Privacy and Consumer Protection.

REGISTERED SUPPORT / OPPOSITION:

Support

Secretary of State Alex Padilla (sponsor)

Opposition

None on file.

Analysis Prepared by: Ethan Jones / E. & R. / (916) 319-2094