Date of Hearing: April 30, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1043 (Irwin) – As Introduced February 21, 2019

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

SUMMARY: This bill would authorize the use of campaign funds to pay for, or reimburse the State for, certain costs related to the cybersecurity of electronic devices of a candidate, elected officer, or campaign worker, as specified. Specifically, **this bill would**:

1) Specify that, notwithstanding certain prohibitions in the Political Reform Act of 1974 (PRA) against the use of campaign funds for various types of payments, as specified, campaign funds may 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.

2) Require that the candidate or elected officer report any expenditure of campaign funds made pursuant to this bill in the candidate's or elected officer's campaign statements filed pursuant to the PRA, as specified.

3) Set forth various findings and declarations, including:

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

   - 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.

   - 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) Requires expenditures of campaign funds to be reasonably related to a political purpose when seeking office, and requires expenditures of campaign funds to be reasonably related to a legislative or governmental purpose when holding office. Further requires an expenditure of campaign funds that confers a substantial personal benefit to be directly related to a political, legislative, or governmental purpose. (Gov. Code Sec. 89512.)

2) 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. (Gov. Code Sec. 89517(a).)

3) Prohibits the use of campaign funds to purchase real property. Except as provided, above, campaign funds may be used to lease real property for up to one year at a time where the use of that property is directly related to political, legislative, or governmental purposes. (Gov. Code Sec. 89517(b).)

4) Permits, notwithstanding the above prohibitions, campaign funds to be used, to pay or reimburse the state for the costs of installing and monitoring an electronic security system in the home or office (or both) of a candidate or elected officer who has received threats to his or her physical safety, provided that the threats arise from his or her activities, duties, or status as a candidate or elected officer and that the threats have been reported to and verified by an appropriate law enforcement agency, as specified. No more than $5,000 in campaign funds may be used, cumulatively, by a candidate or elected officer pursuant to this provision. (Gov. Code Sec. 89517.5.)

FISCAL EFFECT: None. This bill has been keyed nonfiscal by the Legislative Counsel.

COMMENTS:

1) **Purpose of this bill**: This bill seeks to permit candidates, elected officers, and campaign workers to use campaign funds to pay for or reimburse costs related to the cybersecurity of their electronic devices. This is sponsored by the Secretary of State (SOS) Alex Padilla.

2) **Author's statement**: 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 Elections 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.

3) **Assembly Elections & Redistricting Committee informational hearing background**: Last year, the Assembly Elections & Redistricting Committee held a Joint Informational Hearing with the Senate Committee on Elections & Constitutional Amendments on the topic of Cybersecurity and California Elections. According to the Assembly Elections & Redistricting Committee analysis of this bill, witnesses at that hearing (which included the 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) all stressed

the importance of continuing to evaluate cyber and other security threats to election infrastructure. Among other testimony, one witness at the hearing reportedly emphasized the importance of political campaigns implementing cybersecurity best practices to protect their systems and data.

4) **Recent Federal Election Commission Advisory Opinion**: In December of last year, the Federal Election Commission (FEC) (the federal counterpart to this state's Fair Political Practices Commission with respect to campaign finance responsibilities) issued an advisory opinion concluding 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. (*See* FEC Advisory Opinion 2018-15.)

   Leading to that opinion was an inquiry by Senator Ron Wyden. The opinion recognized that Senator Wyden did not report any specific threats to his personal electronic devices or accounts, but noted "the dangers elected officials face in the cyber realm, including attacks by sophisticated state-sponsored hackers and intelligence agencies against personal devices and accounts." Senator Wyden proposed to use campaign funds for several types of expenses he might reasonably incur in order to protect his personal devices and accounts or to recover from cyberattacks, including: (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 applications, 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. (*Id*. at p. 2.) The FEC authorized such expenses as they fall within the ordinary and necessary expenses incurred in connection with the duties of an individual as a holder of federal office. (*Id*. at pp. 2-3.)

   This bill acknowledges this FEC opinion in its findings and declarations, stating that:

   - On December 13, 2018, the Federal Election Commission adopted Advisory Opinion 2018-15, which concluded that it is permissible under the Federal Election Campaign Act (52 U.S.C. Sec. 30101 et seq.) for federal officeholders to use campaign funds to pay for cybersecurity protection for personal devices and accounts.

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

   This bill seeks to achieve a similar result by way of state law, not just for officeholders, but candidates for office and campaign workers as well.

5) **Electronic devices of candidates and elected officials represent vulnerabilities to the State and opportunities to hackers**: More and more, people use electronic devices such as their smartphones, personal laptops and computers, and tablets for both personal and business purposes – including in the public sector. Elected officials and candidates are no different in this regard. To the extent that they use their personal devices for their personal use, governmental or business purposes, or even campaign related activities, and this bill would

allow for the use of campaign funds to reimburse costs related to the cybersecurity of their devices, the benefit conferred upon them is not necessarily limited to political, legislative, or governmental purposes. By and large, existing law, the PRA, requires that campaign fund expenditures be related to either political purposes for individuals seeking office, or legislative or governmental purposes for those holding office. (*See* Gov. Code Sec. 89512.)

On the one hand, it could be that California law should simply prohibit the use of personal devices for campaign or governmental purposes. On the other hand, such a law would ignore the realities of how most people use their devices today and leave unnecessary vulnerabilities open to hackers who recognize that mixed-use devices present extra opportunities for exploitation. In that regard, this bill may very well provide greater protection against cybersecurity threats. Any public policy questions as to the appropriateness of allowing campaign funds to be used in this manner where it may confer great personal benefit to the candidate or elected official, is a policy question better suited for the Assembly Elections & Redistricting Committee, which previously approved this bill. (*See* Comment 10 below.)

In support of this bill, the Fair Political Practices Commission writes:

> Under current law, a candidate may use campaign funds to purchase an electronic security system. To do so, the candidate must have received threats to his or her physical safety because of his or her status as a candidate or elected official an the incidents must be verified by an appropriate law enforcement agency. No more than $5,000 may be spent and a report to the FPPC is required.
>
> Today's elected officials and candidates face countless cybersecurity threats including hacking and phishing schemes. These cybersecurity threats may invade devices and databases and steal personal or campaign-related information with the goal of profiting from the victims' information or releasing information and communications meant to be kept private. The Commission believes the use of campaign funds to secure a candidate's devices from these new electronic threats is related to political, legislative or governmental purposes.

Indeed, it is easy to imagine a candidate or elected official having their information compromised and used against them to by individuals seeking to coerce actions that would not be in the best interest of the State or Californians. This bill would arguably help protect against avoidable threats.

6) **Campaign workers**: Again, this bill applies not only to electronic devices held by elected officials or candidates, but also campaign workers. While it is unclear what this bill means by "campaign worker" – whether it includes paid workers and unpaid interns or volunteers alike – the inclusion of those workers is arguably understandable insofar as the cybersecurity vulnerabilities of one individual on a campaign team can be exploited to harm the team as a whole. The author also argues that their inclusion is appropriate, because "[c]ampaign workers typically have access to voter roll information for outreach purposes, which campaigns should also be able to protect using campaign funds." That being said, the author may wish to be more specific as to the "campaign workers" covered by this bill, particularly as there does not appear to be a working definition of this term in the PRA currently.

7) **Related Legislation**: AB 1044 (Irwin) would authorize 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. That bill is currently in the Assembly Appropriations Committee.

8) **Prior Legislation**: AB 1678 (Berman, Ch. 96, Stats. 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, Ch. 241, Stats. 2018) established the Office of Elections Cybersecurity within the SOS office, 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.

9) **Double-referral**: This bill was double-referred to the Assembly Elections & Redistricting Committee where it was heard on March 27, 2019, and passed on a 7-0 vote.

REGISTERED SUPPORT / OPPOSITION:

Support

Secretary of State, Alex Padilla (sponsor)
Fair Political Practices Commission

Opposition

None on file

Analysis Prepared by: Ronak Daylami / P. & C.P. / (916) 319-2200