Date of Hearing: March 27, 2019

ASSEMBLY COMMITTEE ON ELECTIONS AND REDISTRICTING
Marc Berman, Chair
AB 1044 (Irwin) – As Amended March 18, 2019

SUBJECT: Elections: Secretary of State.

SUMMARY: Permits the Secretary of State (SOS) to require applicants for voter registration information to complete an online cybersecurity course, as specified. Specifically, **this bill:**

1) Authorizes the SOS to require an applicant to take a training course regarding data security as a condition for the receipt of voter registration information if that course is made available at no cost to the applicant.

2) Allows the SOS to require elections officers to provide information about the identity of, and contact information for, the elections official who is responsible for conducting elections in the jurisdiction.

EXISTING LAW:

1) Provides, except as specified, that voter registration information shall be confidential and shall not appear on any computer terminal, list, affidavit, duplicate affidavit, or other medium routinely available to the public at the county elections official's office.

2) Provides that specified voter registration information shall be provided to any candidate or committee, or to any person for election, scholarly, journalistic, political, or governmental purposes, as determined by the SOS. Requires a person who seeks this information to complete an application and submit it to the SOS or to the county elections official.

3) Provides that the California driver's license number, California identification card number, social security number, and any other unique identifier used by the State of California for purposes of voter identification shown on the affidavit of voter registration of a registered voter are confidential and shall not be disclosed to any person, including candidates, ballot measure committees, and persons for election, scholarly, journalistic, or political purposes.

4) Provides that the signature of a voter shown on the affidavit of voter registration is confidential and shall not be disclosed to any person, including candidates, ballot measure committees, and persons for election, scholarly, journalistic, or political purposes, except as specified.

5) Provides that voter registration information shall not be used for any personal, private, or commercial purpose, including, but not limited to any of the following:

    a) The harassment of any voter or voter's household;

    b) The advertising, solicitation, sale, or marketing of products or services to any voter or voter's household; or,

c) Reproduction in print, broadcast visual or audio, or display on the internet or any computer terminal unless pursuant to specified permissible uses.

6) Makes it a misdemeanor for a person in possession of specified voter registration information to knowingly use or permit the use of that information for any purpose other than as permitted by law.

7) Requires that an application for voter registration information available pursuant to law and maintained by the SOS or by the elections official of any county be made pursuant to specified requirements.

8) Requires a person or entity who has received voter registration information pursuant to these provisions, following discovery or notification of a breach in the security of the storage of the information, to disclose the breach in security to the SOS.

9) Requires the SOS to adopt regulations describing best practices for storage and security of voter registration information received by an applicant.

10) Provides that the SOS is the chief elections officer of the state and requires the SOS to see that elections are efficiently conducted and that state elections laws are enforced.

11) Authorizes the SOS to require elections officers to make reports concerning elections in their jurisdictions.

FISCAL EFFECT: Unknown

COMMENTS:

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

> Under existing state law, the Secretary of State stores and restricts access to voter registration information, which includes personally identifiable information (PII) such as a voter's name and address. Political campaigns, journalists, and academic researchers, however, can apply to receive the data for certain non-commercial purposes as long as they justify how it will be used in conformance with state law.
>
> AB 1044 would allow the Secretary of State to require applicants for voter registration information to complete a free, online cybersecurity course. Many candidate and ballot campaigns lack staff members trained in basic cybersecurity measures, particularly at the local level. By ensuring that recipients of voter registration data have completed basic cybersecurity lessons, this bill will help safeguard the personal information of millions of Californians.

2) **Access to Voter Registration Information**: As detailed above, the voter registration information for every voter is confidential under existing law, though specified information from a voter's registration records are available for election, scholarly, journalistic, political, or governmental purposes. When information is provided to individuals and organizations pursuant to these provisions, a voter's driver's license number, identification number, social security number, and signature are not disclosed. Individuals or entities who wish to receive voter registration information for one of those permissible purposes must submit an

application that includes a description of the intended use of the voter registration information.

3) **Storage and Security of Voter Registration Information**: Over the last two years, there were media reports of various instances in which the security of California voter registration information that was held by third parties was compromised. In December of 2017, the *San Diego Union-Tribune* reported that cyber criminals accessed a voter registration database that contained the registration information of more than 19 million California registered voters, and held that information for ransom. While it is not known who compiled that database, it appears to have included voter registration information that was obtained from California election officials in accordance with state law. Similarly, a February 7, 2018, article in the *Sacramento Bee* reported that two of their databases on a third-party computer server were seized by an anonymous hacker who demanded the *Bee* pay a ransom in Bitcoin to get the data back. One of the databases contained the voter registration database legally obtained from the SOS pursuant to existing law.

   Last year, in an effort to better protect and secure the voter registration information obtained and held by third parties, the Legislature passed and the Governor signed AB 1678 (Berman), Chapter 96, Statutes of 2018, which requires the SOS to adopt regulations that describe the best practices for storage and security of voter registration information that is requested and received by a candidate or committee, as specified, or by a person for election, scholarly, journalistic, political, or governmental purposes, as specified. Additionally, AB 1678 requires a person or entity who has received voter registration information to disclose any breach in the security of the storage of the information to the SOS and requires disclosure to occur in the most expedient time possible and without reasonable delay following discovery or notification of the breach.

   This bill authorizes the SOS to require an applicant to take a training course, at no cost to the applicant, regarding data security as a condition for the receipt of voter registration information.

4) **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 elections systems in an environment where the number and sophistication of threats to election infrastructure continues to increase.

   Witnesses that participated in the hearing 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.

   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.

5) **Duties of the Secretary of State**: Under existing law, the SOS is required see that elections are efficiently conducted and that state election laws are enforced, and is permitted to require elections officials to make reports concerning elections in their jurisdictions. In line with these responsibilities, this bill clarifies that these reports may include information about the identity and contact information for the elections official who is responsible for conducting elections in the jurisdiction.

REGISTERED SUPPORT / OPPOSITION:

Support

Secretary of State Alex Padilla (sponsor)

Opposition

None on file.

Analysis Prepared by: Nichole Becker / E. & R. / (916) 319-2094