Date of Hearing: April 11, 2018

ASSEMBLY COMMITTEE ON ELECTIONS AND REDISTRICTING
Marc Berman, Chair
AB 3075 (Berman) – As Amended March 20, 2018

SUBJECT: Office of Elections Cybersecurity.

SUMMARY: Creates the Office of Elections Cybersecurity (OEC) within the Office of the Secretary of State (SOS), and charges it with coordinating efforts to reduce the likelihood and severity of cyber incidents that interfere with election security or integrity. Specifically, **this bill**:

1) Establishes the OEC and specifies that the primary mission of the OEC is to coordinate efforts between the SOS and local elections officials to reduce the likelihood and severity of cyber incidents that could interfere with the security or integrity of elections in the state.

2) Requires the OEC to do all of the following:

    a) Coordinate with federal, state, and local agencies the sharing of information on threats to election cybersecurity, risk assessment, and threat mitigation in a timely manner and in a manner that protects sensitive information.

    b) In consultation with federal, state, and local agencies and private organizations, develop best practices for protecting against threats to election cybersecurity.

    c) In consultation with state and local agencies, develop and include best practices for cyber incident responses in emergency preparedness plans for elections.

    d) Identify resources, such as protective security tools, training, and other resources available to state and county elections officials.

    e) Advise the SOS on issues related to election cybersecurity, and make recommendations for changes to state laws, regulations, and policies to further protect election infrastructure.

    f) Serve as a liaison between the SOS, other state agencies, federal agencies, and local elections officials on election cybersecurity issues.

    g) Coordinate efforts within the SOS's office to protect the security of Internet-connected elections-related resources, including all of the following:

        i) The state's online voter registration system;

        ii) The statewide voter registration database developed in compliance with the requirements of the federal Help America Vote Act of 2002 (HAVA);

iii) The SOS's election night results Internet website;

iv) The SOS's online campaign and lobbying filing and disclosure system commonly referred to as the Cal-Access system; and,

v) Other parts of the SOS's Internet website.

EXISTING LAW:

1) Provides that the SOS is the chief elections officer of the state.

2) Requires the SOS to administer the provisions of the Elections Code.

3) Requires the SOS to see that elections are efficiently conducted and that state election laws are enforced. Permits the SOS to require elections officers to make reports concerning elections in their jurisdictions.

4) Requires each state, pursuant to HAVA, to implement a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the state level that contains the name and registration information of every legally registered voter in the state and assigns a unique identifier to each legally registered voter in the state.

5) Permits a person who is qualified to register to vote and who has a valid California driver's license or state identification card to submit an affidavit of voter registration electronically on the SOS's Internet website.

6) Requires the SOS to provide online and electronic filing processes for use by specified political committees, lobbyists, lobbying firms, and lobbyist employers. This online reporting and disclosure system is commonly referred to as the Cal-Access system.

FISCAL EFFECT: Unknown

COMMENTS:

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

> Earlier this year, the Assembly Elections & Redistricting Committee and the Senate Elections & Constitutional Amendments Committee held a joint informational hearing on the topic of Cybersecurity and California Elections. At that hearing, the committees heard from federal, state, and county elections officials and other experts regarding the extent of the threat to the security of our elections and options for additional steps that California can take to protect the integrity of our elections and to bolster public confidence in the election results.
>
> One of the recurring themes that emerged during the testimony at the informational hearing is that maximizing the cybersecurity of our state's elections will require additional resources dedicated to that purpose. In particular, many

witnesses emphasized the importance of information sharing and coordinated efforts between federal, state, and local government agencies.

AB 3075 would create the Office of Elections Cybersecurity (OEC) within the Secretary of State's office. The OEC would coordinate efforts between federal, state, and local officials, including county registrars of voters, to reduce the likelihood and severity of cyber incidents that threaten the integrity of California elections.

Given the ongoing and increasingly sophisticated threats posed to our elections systems, California cannot afford to be complacent about the security of our elections. AB 3075 is an important step forward to ensuring that state and county elections officials have the information and the tools necessary to defend our democracy from cyber-attacks.

2) **Joint Informational Hearing on Election Cybersecurity**: On March 7, 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, a member of the United States Election Assistance Commission (EAC), 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.

   There were several common recommendations made by witnesses at the hearing for putting state and county elections officials in the best position to defend against and respond to cyber threats, and to protect public confidence in California elections. Many witnesses stressed the importance of funding elections, and expressed support for the $134 million included in the Governor’s proposed 2018-19 budget to assist counties with the costs of replacing their voting systems. Witnesses also noted that the lack of reimbursement by the state for elections-related state mandates and for the costs of special elections for filling vacancies in the Legislature and Congress had the effect of limiting resources that were available at the local level for election security. Several witnesses also stressed the importance of coordinating the sharing of cybersecurity information and resources, particularly with smaller counties that have more limited resources, and of developing robust post-election auditing procedures—including risk-limiting audits—to improve voter confidence in the accuracy of election results. Other recommendations included improving efforts to take advantage of

security expertise in the private sector and at academic institutions in the state, ensuring that elections officials develop cyber incident response plans that include considerations of how to recover from cyber incidents, and working with third-party validators to help disseminate accurate information about elections as a way to counter bad information that could negatively impact elections and voter confidence.

3) **Critical Infrastructure Designation**: On January 6, 2017, then-Secretary of the federal Department of Homeland Security (DHS) Jeh Johnson announced that he was designating election infrastructure in the country as critical infrastructure, a decision that was later reaffirmed by the Trump administration. According to information from DHS, critical infrastructure is a designation "established by the Patriot Act and given to 'systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.'" In his announcement, Secretary Johnson noted that the designation generally gives DHS the ability to provide additional cybersecurity assistance to state and local elections officials, but does not mean that there will be new or additional federal regulation or oversight of the conduct of elections by state and local governments.

   The DHS has prepared a Cybersecurity Services Catalog for Election Infrastructure that outlines the services and other assistance available to the election infrastructure community, including state and local elections officials. Among the services provided are various no-cost cybersecurity assessments, information sharing about cybersecurity threats, cybersecurity training, assistance in cyber incident planning and cyber incident response, and network protection.

4) **Federal Election Security Funding**: On March 23, 2018, President Trump signed the Consolidated Appropriations Act of 2018 (Act)—the omnibus spending bill for the federal fiscal year ending on September 30, 2018. Among other provisions, the Act provided $380 million in HAVA funding to the EAC to make payments to states for activities to improve the administration of elections for Federal office, including to enhance election technology and make election security improvements. States that receive federal funds are required to provide a match of five percent of the funds received within two years of receiving the federal funds.

   According to information from the EAC, California's share of the federal funding is $34,558,876, and the state's required five percent match totals $1,727,944. The EAC notes that a joint explanatory statement prepared by Congress to indicate congressional intent on how the funds may be spent specifies that states may use the funds to replace electronic voting equipment that does not have a paper trail; to implement a post-election audit system; to upgrade election-related computer systems to address cyber vulnerabilities; to facilitate cybersecurity training for state and local election officials; to implement established cybersecurity best practices; and to fund other activities that will improve the security of elections for federal office.

5) **Related Legislation**: AB 2748 (Chau) requires the Office of Information Security in the Department of Technology, the Office of Emergency Services, and the California Military

Department to establish a pilot program to conduct independent security assessments of election infrastructure in participating counties. AB 2748 is pending in the Assembly Privacy & Consumer Protection Committee and has been double-referred to this committee.

REGISTERED SUPPORT / OPPOSITION:

Support

California Common Cause
League of Women Voters of California
Secretary of State Alex Padilla

Opposition

None on file.

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