Date of Hearing: April 25, 2018

ASSEMBLY COMMITTEE ON ELECTIONS AND REDISTRICTING
Marc Berman, Chair
AB 2748 (Chau) – As Amended March 23, 2018

SUBJECT: Election infrastructure: independent security assessments.

SUMMARY: Establishes a pilot program until 2023 under which participating counties would have an independent security assessment (ISA) of their election infrastructure conducted by specified state government entities. Specifically, **this bill**:

1) Requires the Office of Information Security (OIS) within the California Department of Technology (CDT), the Office of Emergency Services (OES), and the California Military Department (CMD) to conduct an ISA of election infrastructure in participating counties. Requires OIS, OES, and CMD to consult with county elections officials to identify and select counties to participate in the pilot program and requires the first set of ISAs to be completed by January 1, 2020.

2) Requires OIS, OES, and CMD to do all of the following in coordination with the county elections officials in participating counties:

    a) Determine criteria and rank counties based on an information security risk index that may include analysis of the relative amount of the following factors within counties:

        i) Personally identifiable information protected by law;

        ii) Voter registration information;

        iii) Information on voted ballots;

        iv) Self-certification of compliance and indicators of unreported noncompliance with security provisions in the following areas:

            (1) Information asset management;

            (2) Risk management;

            (3) Information security program management;

            (4) Information security incident management; and,

            (5) Technology recovery planning; and,

        v) Other information identified by OIS, OES, and CMD, in coordination with county elections officials, that may present a security risk.

    b) Determine the basic standards of services to be performed as part of ISAs conducted in accordance with this bill.

3) Requires OIS, OES, and CMD to transmit the complete results of each ISA and recommendations for mitigating system vulnerabilities, if any, to the applicable county elections officials and the Secretary of State (SOS).

4) Provides that information and records concerning an ISA are confidential and shall not be disclosed, except as specified, during the process of conducting the ISA.

5) Provides that the results of a completed ISA and related information are subject to all disclosure and confidentiality provisions of state law, including a provision of state law that exempts from disclosure an information security record of a public agency, if, on the facts of the particular case, disclosure of that record would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency.

6) Requires OIS, OES, and CMD to notify the Department of the California Highway Patrol (CHP) and the Department of Justice (DOJ) of any criminal or alleged criminal cyber activity affecting a state entity or critical infrastructure of state government.

7) Defines "election infrastructure," for the purposes of this bill, as "storage facilities, polling places, and centralized vote tabulation locations used to support the election process, and information and communications technology to include voter registration databases, vote tabulating devices, and other systems to manage the election process and report and display results."

8) Contains various findings and declarations, and declares the intent of the Legislature to do both of the following:

    a) Leverage the state's cybersecurity resources to assist county elections officials in their assessments of election infrastructure in order to be best prepared for future cybersecurity threats; and,

    b) Recognize election infrastructure as critical infrastructure and an important subsector within the Government Facilities Sector identified by the federal government and California.

9) Includes a January 1, 2023 sunset date.

EXISTING LAW:

1) Establishes the CDT within the Government Operations Agency, under the supervision of the Director of Technology, also known as the State Chief Information Officer. Establishes the OIS within the CDT. Specifies that the purpose of OIS is to ensure the confidentiality, integrity, and availability of state systems and applications, and to promote and protect privacy as part of the development and operations of state systems and applications to ensure the trust of the residents of this state.

2) Establishes the OES within the office of the Governor. Requires OES to be responsible for the state's emergency and disaster response services for natural, technological, or manmade disasters and emergencies, including responsibility for activities necessary to prevent, respond to, recover from, and mitigate the effects of emergencies and disasters to people and property.

3) Establishes the CMD, and provides that it includes the office of the Adjutant General, the California National Guard, the State Military Reserve, the California Cadet Corps, and the Naval Militia.

4) Requires OIS to develop an information security program and establish policies, standards, and procedures directing state agencies to effectively manage security and risk.

5) Permits the OIS to conduct, or require to be conducted, an ISA of every state agency, department, or office. Requires the cost of an ISA to be funded by the state agency, department, or office being assessed. Requires the OIS, in consultation with OES, to require no fewer than 35 state entities to perform an ISA each year, as specified.

6) Permits the Military Department to perform an ISA of any state agency, department, or office, funded by the agency, department, or office being assessed.

7) Requires state agencies and entities required to conduct or receive an ISA to transmit the complete results of that assessment and recommendations for mitigating system vulnerabilities, if any, to the OIS and the OES.

8) Requires the OIS to report any state entity found to be noncompliant with information security program requirements to the CDT and the OES.

9) Provides that information and records concerning an ISA are confidential and shall not be disclosed, except as specified, during the process of conducting the ISA. Provides that the results of a completed ISA are subject to all disclosure and confidentiality provisions pursuant to any state law, including a provision of the California Public Records Act (CPRA) that exempts from disclosure an information security record of a public agency, if, on the facts of the particular case, disclosure of that record would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency.

10) Requires CDT to notify the OES, the CHP, and the DOJ regarding any criminal or alleged criminal cyber activity affecting any state entity or critical infrastructure of state government.

11) Provides that the SOS is the chief elections officer of the state. Requires the SOS to administer the provisions of the Elections Code. 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.

12) Requires the SOS to test and certify or otherwise approve voting systems, remote accessible vote by mail systems, ballot-on-demand systems, and electronic poll books prior to their use in an election in the state.

13) Requires each state, pursuant to the federal Help America Vote Act (HAVA) of 2002, 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.

FISCAL EFFECT: Unknown

COMMENTS:

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

> Free and fair elections are the cornerstone of our democracy. Ensuring that our election processes and voting systems are secure is vital to the integrity of our elections. There has been growing concern about the impact that cyberattacks may have on our election process and democratic institutions. In the aftermath of the 2016 elections, numerous states, including California, were found to be the targets of election interference by Russian hackers. In response to the similarly growing threat of cyberattacks on government systems the State of California previously enacted into law AB 670 (Irwin) to require [CDT], in partnership with [CMD] and [OES], to annually conduct no fewer than 35 independent security assessments of state agencies, departments or offices. These assessments evaluate the agency on how effectively it protects personally identifiable information, health information, and confidential financial information along with assessing information security management and incident management and response. AB 2748 builds upon AB 670 by requiring CDT, CMD, and OES to establish a pilot program to conduct an independent security assessment of election infrastructure in participating counties so that these counties can have the resources to proactively review their systems to ensure they are as secure as possible.

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 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 (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.

   The most thorough and extensive cybersecurity assessment offered by the DHS to the election infrastructure community is a Risk and Vulnerability Assessment (RVA), a no-cost service described by DHS as an "offering that combines national threat and vulnerability information with data collected and discovered through onsite assessment activities to provide customers with actionable remediation recommendations prioritized by risk. Engagements are designed to determine whether and by what methods an adversary can defeat network security controls. Components of the assessment can include scenario-based network penetration testing, web application testing, social engineering testing, wireless testing, configuration reviews of servers and databases, and evaluation of an [organization's] detection and response capabilities." Because of the extensive nature of the assessment and the fact that DHS is offering it at no-cost, there can be a long wait between the time that a jurisdiction applies for an RVA and the time that one is conducted. DHS indicates that the wait time to receive an RVA typically is at least 90 days, and an article last December reported that the wait could be as long as nine months (Starks, T. "The latest 2018 election-hacking threat: 9-month wait for government help." *Politico*, 29 December 2017, www.politico.com/story/2017/12/29/2018-election-hacking-threat-government-help-231512. Accessed April 2018), though DHS subsequently has said that they are prioritizing requests

for RVAs from state and local elections officials in an effort to get those assessments completed more quickly.

4) **Independent Security Assessments and Existing Law**: AB 670 (Irwin), Chapter 518, Statutes of 2015, requires OIS, in consultation with OES, to conduct no fewer than 35 ISAs of state agencies, departments, or offices annually, as specified. AB 670 also authorizes the CMD to perform an ISA of any state agency, department, or office, the cost of which shall be funded by the state agency, department, or office being assessed. The provisions of this bill are modeled after AB 670, though the language has been modified to focus more squarely on elections-related infrastructure, and certain other adjustments have been made.

   While the state offices, departments, and agencies with cybersecurity responsibilities have conducted ISAs for non-state entities in the past, the framework established by AB 670 focused on ISAs of state agencies, departments, and offices. By creating a framework for ISAs to be conducted on county elections offices, and by establishing clear lines of authority and responsibility for those ISAs, this bill could help make the state's cybersecurity expertise more broadly available in protecting California's election infrastructure.

5) **Funding for Independent Security Assessments**: In requiring an ISA to be performed for every state agency, department, or office, AB 670 specifically required each ISA to be funded by the state agency, department, or office being assessed. This bill is silent with respect to the entity that would be responsible for paying for an ISA that is conducted under the pilot program.

   As detailed above, a number of witnesses at this committee's joint informational hearing testified about the need to increase the resources that are available for election security. While many county elections officials may appreciate the opportunity to have an ISA performed by OIS, OES, and CMD, it is unclear how many counties would be able to take advantage of that opportunity if they are required to pay the full costs of the ISA. In particular, counties with more limited resources may find it particularly challenging to cover the costs of an ISA conducted by the state.

6) **Confidentiality of Sensitive Information**: Consistent with the policy developed in AB 670, this bill provides that assessment results, while subject to all disclosure provisions of state law including the CPRA, are also subject to a provision of the CPRA that protects disclosure of any government information security record that "would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency." Thus, under this provision, any part of the result of an ISA that could reveal vulnerabilities is redactable, including potentially the entire assessment.

   Additionally, during the process of conducting the assessment, this bill provides that information and records concerning ISAs are confidential and shall not be disclosed except to specified entities as necessary to receive the information and records to perform the ISA, subsequent remediation activity, or monitoring of remediation activity. This provision also is based off existing public policy approved under AB 670.

7) **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.

8) **Suggested Amendments**: To ensure that this bill accurately reflects the author's intent and to tailor the language of the bill more closely to the types of assessments that would be conducted, committee staff recommends the following amendments to this bill:

   a) **Voluntary Participation**: According to information from the author's office, the intent of this bill is to conduct ISAs in counties that voluntarily have agreed to participate in the pilot program that this bill creates. Certain language in this bill, however, could be interpreted to permit the OIS to require an ISA of a county that did not want to participate in the pilot program. To clarify the intent of the bill, committee staff recommends the following amendments:

      On page 4, lines 4 and 5 of the bill, strike out "participating counties" and insert:

      counties that voluntarily choose to participate in the pilot program

   b) **Sharing Information with Relevant County Officials**: As detailed above, the language of this bill is based off an existing law that provides for ISAs of state agencies, departments, and offices. Because this bill provides for ISAs of *county* elections infrastructure, however, committee staff recommends that this bill be amended in a number of areas to ensure that relevant county officials receive information about the ISAs that are conducted, and the results of those ISAs. Additionally, committee staff recommends amendments to clarify that the results of an ISA conducted in a county will be shared only with the elections official in *that* county, and will not be shared with the elections officials in other counties in which ISAs were conducted as part of the pilot program. Specifically, committee staff recommends the following amendments:

      On page 5, lines 1 and 2 of the bill, strike out "applicable county elections officials" and insert:

      elections official of the county in which the assessment was conducted

      On page 5, line 8, strike out "employees and state contractors" and insert:

employees, state contractors, county employees, and county contractors

On page 5, line 23, strike out "government." and insert:

government, and shall notify the district attorney of the county regarding any criminal or alleged criminal cyber activity affecting any county entity or critical infrastructure of the county government.

c) **Reporting Requirement**: While this bill authorizes a four-year pilot program for conducting ISAs of county election infrastructure, it does not include a means for evaluating that program. Bills that authorize pilot programs commonly include a requirement that a report be prepared and be submitted to the relevant legislative committees in order to inform future discussion over extension or expansion of the program. Committee staff recommends that this bill be amended to require the OIS, OES, and CMD, if one or more ISAs are conducted pursuant to this bill, to prepare a report on the pilot program. Specifically, committee staff recommends the following amendments:

On page 5, between lines 33 and 34, insert:

(g) If one or more independent security assessments are conducted pursuant to this section, the office, the Office of Emergency Services, and the California Military Department shall prepare a joint report to the Legislature regarding the assessments conducted as part of the program on or before January 1, 2022, and shall submit that report in compliance with Section 9795. The office, the Office of Emergency Services, and the California Military Department shall develop the report in consultation with the counties in which the independent security assessments were performed. The report shall include, but not be limited to, all of the following:

(1) An identification of the counties in which independent security assessments were performed pursuant to this section.

(2) Information about the costs of independent security assessments performed pursuant to this section.

(3) A summary of relevant performance metrics, including county satisfaction with the performance of the assessments and a summary of the results of completed assessments, subject to all confidentiality provisions pursuant to any state law, including, but not limited to, Section 6254.19.

(4) Any legislative recommendations.

On page 5, line 34, strike out "(g)" and insert:

(h)

9) **Related Legislation**: AB 3075 (Berman), which is pending in the Assembly Appropriations Committee, creates the Office of Elections Cybersecurity within the Office of the SOS, and charges it with coordinating efforts to reduce the likelihood and severity of cyber incidents that interfere with election security or integrity. AB 3075 was heard in this committee on April 11, 2018 and was approved on a 6-0 vote.

10) **Double-Referral**: On April 17, 2018, this bill was approved by the Assembly Privacy & Consumer Protection Committee on a 10-0 vote.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file.

Opposition

None on file.

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