Date of Hearing: April 15, 2026

ASSEMBLY COMMITTEE ON ELECTIONS
Gail Pellerin, Chair
AB 2281 (Berman) – As Introduced February 19, 2026

SUBJECT: Office of Elections Cybersecurity.

SUMMARY: Authorizes the Office of Elections Cybersecurity (OEC) within the Secretary of State's (SOS) Office to consult with academic researchers to develop best practices for protecting against threats to election cybersecurity. Requires the SOS to assess whether additional state resources are needed to replace election cybersecurity resources previously provided by the federal government.

EXISTING LAW:

1) Establishes the OEC within SOS's office. Provides that the primary missions of the OEC are both of the following:

    a) 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.

    b) To monitor and counteract false or misleading information regarding the electoral process that is published online or on other platforms and that may suppress voter participation or cause confusion and disruption of the orderly and secure administration of elections. (Elections Code §10.5(a), (b))

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 to protect the security of Internet-connected elections-related resources, including the state's online voter registration system, the statewide voter registration database (referred to as VoteCal), the SOS's election night results Internet Web site, online campaign and lobbying filing and disclosure system developed by the SOS (also known as CalAccess), and other parts of the SOS's website.

h) Assess the false or misleading information regarding the electoral process that is published online or other platforms, mitigate the false or misleading information, and educate voters, especially new and unregistered voters, with valid information from elections officials such as a county elections official or the SOS. (Elections Code §10.5(c))

FISCAL EFFECT: Unknown

COMMENTS:

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

> I was proud to author legislation in 2018 to create the Office of Elections Cybersecurity (OEC), which is tasked with coordinating efforts between federal, state, and local officials to reduce the likelihood and severity of cyber incidents that threaten the integrity of California elections. Unfortunately, the Trump Administration has cut critical funding, coordination, and support that helped states guard against threats to our election systems. Given the loss of federal election cybersecurity infrastructure, AB 2281 would direct the OEC [to] assess if additional state resources are needed to ensure that California officials continue to have the information and tools necessary to defend our democracy from cyber-attacks. Additionally, this bill would strengthen OEC by authorizing them to consult with academic researchers, allowing them to utilize their expertise in support of OEC's mission.

2) **Cybersecurity and Previous Legislation**: In 2018, the Assembly Elections & Redistricting Committee (now referred to as the Assembly Elections Committee) and the Senate Elections & Constitutional Amendments Committee held a joint informational hearing on the topic of Cybersecurity and California Elections. Due to 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 its elections systems in an environment where the number and sophistication of threats to election infrastructure continues to increase. 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.

   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. One of the recurring themes that emerged during the testimony at the informational hearing was that maximizing the cybersecurity of our state's elections will require additional resources dedicated to that purpose. Many witnesses 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.

Subsequently, the Legislature approved and Governor Brown signed AB 3075 (Berman), Chapter 241, Statutes of 2018, to establish the OEC within the SOS's office. The OEC has two primary missions. First, it is responsible for coordinating 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 California. The OEC is also tasked with monitoring and counteracting false or misleading information regarding the electoral process that is published online or on other platforms that may suppress voter participation, cause confusion, or disrupt the ability to ensure a secure election. According to the OEC's website, the office serves California with the sole purpose of keeping every Californian's vote safe from online interference, especially the spread of mis- and disinformation

3) **Critical Infrastructure Designation:** In January 2017, the Department of Homeland Security (DHS) designated election systems as critical infrastructure. 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.'" This designation enabled DHS to prioritize cybersecurity and physical security assistance to elections officials.

   DHS 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 Services**: In 2018, the Cybersecurity and Infrastructure Security Agency (CISA) was established, within DHS, and made responsible for maintaining public trust and confidence in United States election systems. CISA has worked with government agencies and the private sector to address election threats, including cybersecurity threats and physical security concerns. Since CISA's creation, many state and local elections officials have relied on CISA's free and voluntary assistance, expertise, and resources—as well as its partnerships with other agencies—to help protect election systems by sharing timely and

actionable threat information and offering cybersecurity services to safeguard their election systems. For instance, CISA has sponsored regional tabletop training exercises and drills to teach local elections officials how to respond when cyber or physical incidents threaten the conduct of elections.

Moreover, through its partnership with the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), CISA has provided elections officials with the information they needed to protect themselves from cyber threats and shared actionable information about electoral infrastructure incidents with states and local governments. In 2024, EI-ISAC was a crucial resource for providing elections officials with information about Election Day bomb threats and suspicious white powder mailings that occurred in 15 states, including California.

Additionally, through its partnership with Multi-State Information Sharing and Analysis Center (MS-ISAC), state and local governments were provided with no-cost and low-cost cybersecurity threat prevention, protection, response, and recovery. CISA has provided funds to support the MS-ISAC under a cooperative agreement with the Center for Internet Security (CIS) for nearly 20 years.

5) **Recent Federal Changes to CISA:** Last year the federal government made considerable changes to federal election cybersecurity support, funding, and infrastructure. In February 2025, media articles reported that CISA had made significant staffing cuts and froze all of its election security work as part of a review of CISA's operations by DHS. While DHS completed its review of CISA's election security activities last March, the results of the review have not been publicly released. Subsequent media reports stated that acting CISA Director Bridget Bean circulated a memo announcing that the administration had cut off all funds to support EI-ISAC, which was funded through DHS grants.

   Additionally, last March, CISA announced a $10 million cut in funding for MS-ISAC. It was reported that the $10 million allocated by CISA accounted for just under half of MS-ISAC's funding.

   In an effort to address its funding gap, media articles report that CIS, the non-profit that operates and houses both MS-ISAC and ES-ISAC, is temporarily transitioning into charging state and local governments for memberships in the EI-ISAC and MS-ISAC and providing a fee-based service to some non-government, election-related organizations.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file.

Opposition

None on file.

Analysis Prepared by: Nichole Becker / ELECTIONS / (916) 319-2094