ASSEMBLY COMMITTEE ON ELECTIONS & REDISTRICTING
AND
SENATE COMMITTEE ON ELECTIONS & CONSTITUTIONAL AMENDMENTS

JOINT INFORMATIONAL HEARING

Subject: Cybersecurity and California Elections

Wednesday, March 7, 2018, 9:00 AM
State Capitol, Room 444

Hearing Overview

Since the 2016 elections, there has been an increased focus on election security, and on the increasingly sophisticated threats posed to our elections systems. In a declassified intelligence assessment released shortly after the November 2016 presidential election, the United States (U.S.) intelligence community concluded that Russia attempted to influence the 2016 election in an effort to "undermine public faith in the U.S. Democratic process," and noted that while Russian efforts to influence elections in this country were not new, the 2016 effort "demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations."

The intelligence assessment concluded that Russia's efforts to influence the election were multifaceted, and included cyber operations against political organizations and the public disclosure of information gained from those efforts, cyber intrusions into state and local electoral boards, and propaganda efforts. While there is no evidence that these efforts affected the tallying of votes, they may harm confidence in our electoral process.

Amid the backdrop of these nationwide efforts by outside actors to influence elections, Californians, in particular, have received conflicting information about whether our own systems have been compromised. In September of last year, California was publicly identified as one of the 21 states that were notified by the federal Department of Homeland Security (DHS) of Russian efforts to target their Internet-connected election networks; just last week, NBC News reported that the U.S. intelligence officials determined that Russian operatives compromised state websites or voter registration systems in seven states—including California—before the 2016 election.

Secretary of State Alex Padilla, however, has stated that the DHS confirmed that Russian attempts to identify weaknesses in California's Internet-connected systems had not actually occurred on the Secretary of State's website, and that they have "no information or evidence that our systems have been breached in any way or that any voter information was compromised." Furthermore, DHS has disputed the NBC News report, calling it "factually inaccurate and

misleading," and stating that it has "no intelligence – new or old – that corroborates NBC's reporting that state systems in 7 states were compromised by Russian government actors."

U.S. intelligence officials warn, however, that external threats to our elections will continue. Last month, Mike Pompeo, the Director of the Central Intelligence Agency, testified in a U.S. Senate Intelligence Committee hearing that "we have seen Russian activity and intentions to have an impact on the [2018] election cycle." Security and intelligence experts worry that attackers might be more aggressive and successful in their attacks especially because many states are using out-of-date voting equipment with more significant security vulnerabilities than newer machines.

According to a Brennan Center for Justice report, "Securing Elections from Foreign Interference," over 40 states are currently using voting machines that were purchased more than a decade ago. California's aging election infrastructure is no exception and, consequently, may pose its own set of security challenges. A report last year by California's Legislative Analyst's Office ("The 2017-18 Budget: Considering the State's Role in Elections") found that most California counties are using antiquated voting systems that, in many cases, include components that are no longer produced by the voting system manufacturer. In some cases, county voting systems run on operating systems that are no longer supported by the manufacturer and that do not receive security upgrades. The report found that "all but a few counties in the state use voting systems that are more than a decade old." Under voluntary voting system guidelines adopted by the United States Election Assistance Commission (EAC)—the federal commission established by the Help America Vote Act of 2002—voting systems must be designed to have a useable life of ten years.

While ensuring the security of voting systems plays an essential role in protecting the integrity of elections and in promoting voter confidence in election results, other aspects of the electoral process similarly present potential cybersecurity concerns. The DHS confirmed that voter registration systems were targeted in some states during the 2016 elections; in Illinois, attackers accessed approximately 90,000 records from its voter registration database, and in Arizona, state officials took their voter registration database offline for nine days after a hacker using a server in Russia tried to access the database using a county election official's login and password. Furthermore, a breach of election night reporting systems could undermine public confidence in election results even if actual vote tallies were not affected.

Fortunately, California has already taken a number of important steps to protect our elections systems from threats. Votes cast in California are primarily cast on paper ballots, and the use of paperless voting systems has been banned in California since 2006. Direct recording electronic voting systems—which are used as the primary polling place voting system in two counties, and are used on a more limited basis elsewhere to assist disabled voters in casting ballots independently and secretly—must produce an accessible voter-verified paper audit trail which is used for audit, recount, and manual tally purposes. In counties that use electronic voting systems, state law requires election officials to provide paper ballots at the polling place. Paper ballots are used if the electronic voting system fails, and every voter has the right to request a paper ballot even if the electronic voting system is functioning. State law additionally prohibits any part of a voting system from being connected to the Internet at any time, and California's voting system standards prohibit voting systems from having the capability to communicate individual votes or

vote totals over public communications networks or from having wireless communications capabilities.

In an effort to address California's aging voting systems, the Governor's proposed 2018-19 budget includes $134.3 million in General Fund moneys for the replacement of county voting systems. The figure assumes that each county will pay for half of the cost of its voting system replacement, with the state picking up the other 50 percent of the costs. More details about the Governor's budget proposal can be found in the approved Budget Change Proposal available here: http://web1a.esd.dof.ca.gov/Documents/bcp/1819/FY1819_ORG0890_BCP1787.pdf.

Additionally, the federal government has taken steps to provide additional resources to states and to local governments to identify and address cybersecurity threats to elections systems. On January 6, 2017, then-Secretary of the 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 EAC has produced a white paper explaining the significance of the designation, and DHS has prepared a catalog of cybersecurity services available to protect election infrastructure. Those documents are available here:

- EAC White Paper: https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf

- DHS Catalog of Cybersecurity Services: https://www.eac.gov/assets/1/6/DHS_Cybersecurity_Services_Catalog_for_Election_Infrastructure.pdf

Additionally, the EAC maintains an online hub of information about election security preparedness with many other resources here: https://www.eac.gov/election-officials/election-security-preparedness/.

The purpose of this hearing is to explore and discuss 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. The Committees will hear 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.