Date of Hearing: January 13, 2016

ASSEMBLY COMMITTEE ON ELECTIONS AND REDISTRICTING
Sebastian Ridley-Thomas, Chair
AB 887 (Ting) – As Amended January 4, 2016

SUBJECT: Military and overseas voters: ballot submission by electronic mail: Internet voting.

SUMMARY: Permits a military or overseas voter to return his or her vote by mail (VBM) ballot by electronic mail (email), as specified, and allows a military or overseas voter to cast his or her vote on the Internet, as specified. Specifically, **this bill**:

1) Permits a military or overseas voter to return his or her VBM ballot by email, as specified.

2) Provides that, to be counted, the ballot returned by email must be received by the voter's elections official no later than the closing of the polls on election day and must be accompanied by a copy of an identification envelope and an oath of voter declaration, as specified.

3) Provides that in order for a ballot to be submitted by email, the ballot, identification envelope, and oath of voter declaration, must be scanned to create electronic copies of the documents. Requires the electronic copies of the documents to be included in the email sent to the elections official as attachments.

4) Requires the Secretary of State (SOS) to adopt uniform regulations for the use of email in returning ballots.

5) Requires each elections official to adopt appropriate procedures to protect the secrecy of the ballots returned by email.

6) Requires the elections official, upon receipt of a ballot returned by email, to determine the voter's eligibility to vote by comparing the signature on the scanned copy of the identification envelope with the signature on the voter's affidavit of registration

7) Allows a military or overseas voter to cast his or her vote on the Internet by electronically marking his or her ballot and securely transmitting the voted ballot to the appropriate election official using the Internet. Provides that, in order to be counted, the voted ballot must be received by the voter's elections official no later than the closing of the polls on election day.

8) Requires the SOS to adopt uniform regulations for military and overseas voters to cast votes using the Internet.

9) Provides that the Internet voting provisions of this bill shall become operative only if the SOS certifies that he or she has identified and addressed all issues regarding the security of casting a vote using the Internet.

10) Makes conforming changes.

EXISTING LAW:

1) Defines a "military or overseas voter" as an elector absent from the county in which he or she is otherwise eligible to vote who is any of the following:

   a) A member of the active or reserve components of the United States (U.S.) Army, Navy, Air Force, Marine Corps, or Coast Guard; a Merchant Marine; a member of the U.S. Public Health Service Commissioned Corps; a member of the National Oceanic and Atmospheric Administration Commissioned Corps of the U.S.; a member on activated status of the National Guard or state militia;

   b) A citizen of the U.S. living outside of the territorial limits of the U.S. or the District of Columbia; or,

   c) A spouse or dependent of a person described above.

2) Provides that when a military or overseas voter applies for a VBM ballot, the application shall be deemed to be an affidavit of registration and an application for permanent VBM status.

3) Requires each elections official to have a system available which allows a military or overseas voter to electronically request and receive a VBM application, an unvoted ballot, and other information.

4) Requires elections officials to request an email address from each military or overseas voter who registers, as specified.

5) Requires elections officials to send VBM ballots by means of transmission (mail, facsimile, or electronic transmission) requested by a qualified military or overseas voter.

6) Requires the elections official to send a VBM ballot to a military or overseas voter not earlier than 60 days, but not later than 45 days, before the election.

7) Allows a military or overseas voter who is temporarily living outside of the U.S. to return his or her ballot by facsimile transmission. Requires a ballot returned by facsimile transmission to be accompanied by an identification envelope and an oath of voter declaration in which the voter acknowledges that the electronic transmission of a completed ballot may compromise the secrecy of the ballot.

8) Requires the county elections official to determine the voter's eligibility to vote by comparing the voter's signature from the materials returned by facsimile transmission to the signature on the voter's affidavit of registration.

9) Allows a military or overseas voter who is unable to appear at his or her polling place because of being recalled to service after the final day for applying for a VBM ballot to appear before the elections official in the county in which the voter is registered to apply for a VBM ballot.

10) Permits a military or overseas voter to use a federal write-in absentee ballot in any election in which he or she is qualified to vote.

FISCAL EFFECT: Unknown. State-mandated local program; contains a crimes and infractions disclaimer and reimbursement direction.

COMMENTS:

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

> The nonpartisan Overseas Vote Foundation (OVF) claims 2012 was a tipping point in the use of electoral technology by Uniformed and Overseas Citizens Absentee Voting [Act] voters (UOCAVA voters). That year, UOCAVA voters nearly doubled the rate at which they returned their ballots via email and more UOCAVA voters than ever cast their votes online. This technological transition eliminated the biggest roadblocks preventing these voters from participating in the democratic process.
>
> Research shows paper ballots often arrive too late for voters overseas to meet the required deadline to return their ballots, that ballots are lost in the mail, and that many ballots are undeliverable.
>
> Over thirty states already offer their UOCAVA voters the option of submitting their ballots through email and two states offer UOCAVA voters the option of casting their votes online. Unfortunately, California does not offer either of these options. We mandate a paper process. Assembly Bill 887 enables California to catch up with the times. By giving California's UOCAVA voters the option to cast vote online and to submit their ballots through email, California can start to administer elections in electronic formats, which have permeated how our citizens live and work. Through these means, we will reduce the largest voting barriers facing California's overseas voters.

2) **New Ballot Return Election Policies**: This bill breaks new ground and permits new methods by which a voted ballot may be returned and how a ballot may be cast that have never been used in California. This bill allows a military or overseas voter to return his or her VBM ballot by email. For the ballot to count, the voter must send electronic copies of the voted ballot, a copy of the identification envelope and an oath of voter declaration to the voter's elections official no later than the closing of the polls on election day. Returning a voted ballot by email is not currently allowed under existing law. As mentioned above, military or overseas voters currently are only allowed to return a voted ballot by mail, fax, or in-person return.

   In addition, this bill allows a military or overseas voter to cast his or her vote on the Internet by electronically marking his or her ballot and securely transmitting the voted ballot to the appropriate elections official using the Internet. In order for the ballot to be counted, the voted ballot must be received by the voter's elections official no later than the closing of the polls on election day. Again, this change proposes a major departure from how a military or overseas voter may currently cast his or her ballot.

3) **How Would a Voter Cast a Ballot on the Internet?** While this bill authorizes a military or overseas voter to cast his or her ballot on the Internet by electronically marking his or her

ballot and securely transmitting the voted ballot to the appropriate elections official using the Internet, it does not, however, indicate how or by which method this new procedure to vote on the Internet will occur. Will a military or overseas voter vote on the Internet via a kiosk, a web-based application, or his or her own personal computer? This bill does not provide any detail as to how this new process or system would work. Theoretically, some sort of new voting system would need to be reviewed, certified, and approved for use in order for a military or overseas voter to utilize this option to cast his or her ballot. Under current law, no voting system or part of a voting system may be connected to the Internet at any time. Consequently, new testing and certification protocols and procedures will need to be developed to ensure the system is appropriately tested and examined. Because this bill requires the SOS to adopt uniform regulations for military and overseas voters to cast votes using the Internet, an argument can be made that the SOS will include those details in the regulations. The committee, however, may wish to consider requiring the SOS to develop new testing and certification protocols and procedures for a voting system that allows for Internet voting. Currently, there are no state laws or regulations governing the use of Internet voting systems and the committee staff is unaware of any official federal standards.

Moreover, this bill provides that the Internet provisions of this bill will not become operative until the SOS certifies that he or she has identified and addressed all issues regarding the security of casting a vote using the Internet. This language, however, is vague and ambiguous. This bill does not include specific safeguards or safety measures to protect a voter's private information and voting selections, nor does it include any requirements for encryption or other safeguards to protect against information being intercepted during transmission. Again, while an argument can be made that those provisions will not be operative until the SOS certifies that all security issues have been addressed, more detail and specificity is needed to understand what it means for an Internet voting system to be secure. As noted later in this analysis, various documented studies and reports generally conclude that the current architecture of the Internet and the variety of ways in which its security can be compromised pose a significant threat and risk to Internet voting systems. Many specifically state that Internet voting systems can be vulnerable to a variety of different attacks, the most common attacks include, but are not limited to, denial of service, Trojan horse viruses, malware, website spoofing, and phishing. Depending on the attack, a variety of outcomes can result, all of which could compromise the integrity of the election.

In addition to the security issues mentioned, there are other important concerns that are not currently addressed or contemplated in this bill, such as usability, transparency, auditability and verifiability. If it is the will of the committee to approve this bill, it may be appropriate to include more detail to address these important issues.

4) **What is an Internet Voting System?** According to the U.S. Election Assistance Commission's (EAC) September 2011 report entitled, "A Survey on Internet Voting," the term "Internet voting" is used to refer to many different methods, or channels, of voting. What the channels have in common is the use of the communications connectivity and protocols by the Internet. The report classifies Internet voting as a subset of electronic voting. For the purposes of their study, an Internet voting system was defined as any system where the voter's ballot selections are transmitted over the Internet from a location other than a polling place to the entity conducting the election. Consequently, the term "remote electronic voting" is often used as a synonym.

The report states that the remote voting location can be either a controlled or an uncontrolled voting environment. It defines a controlled environment to mean a situation where the voting platform, such as the computer used for voting, was supplied by and under the control of the entity conducting the election. The report describes an uncontrolled environment to mean a situation where the voter supplies the computer used for voting, which may be the voter's personal computer, workplace computer, or any other public computer.

According to the survey, there are two forms in which a voter's ballot selections can be returned – electronic ballot return, where the entire ballot document, including the voter's selections, are transmitted, or vote data return, where only the voter's selections are transmitted. Furthermore, the survey describes that there are three channels, or methods, for electronic ballot return: a web-based communications application which uploads a digital representation of a voted ballot (e.g., pdf or jpeg) file to a website; a digital facsimile, where a voter's ballot is scanned and transmitted as a graphics file; and, email, where a digital representation (e.g., pdf or jpeg) of a voter's ballot is transmitted via email.

In addition, their survey outlines three methods for presentation of the ballot and vote data return. They include a web browser or computer application which the voter executes to display the ballot, record selections, and transmit selections; a direct recording electronic (DRE) device or kiosk connected to the Internet to transmit vote data; and a Voting Over Internet Protocol approach for the voter to access the ballot, record selections, and transmit selections.

5) **California Internet Voting Task Force**: In 1999, Secretary of State Bill Jones convened the California Internet Voting Task Force (Task Force) to study the feasibility of using the Internet to conduct elections in California. The goal of the Task Force, which was comprised of more than two dozen experts in the field of data security and elections and voter participation, was to examine the feasibility of Internet voting and develop a report that included recommendations, analysis, and suggested technical requirements. The Task Force issued a final report in 2000. According to the report, the implementation of Internet voting would allow increased access to the voting process for millions of potential voters who do not regularly participate in our elections. However, the Task Force concluded that technological threats to security, integrity, and secrecy of Internet ballots are significant and very real. Among the recommendations provided by the Task Force was that the election process would be best served by a strategy of evolutionary rather than revolutionary change. The report states that the implementation of Internet voting will be a complex undertaking with no room for error. Consequently, the Task Force recommended a phased-in approach that will allow for the gradual testing of various components of technology to authenticate voters and provide secure and secret ballots. Other recommendations included ensuring Internet voting would serve as a supplement to, not a replacement of, traditional paper-based voting, be accessible to all voters, and ensure there is large public support otherwise large levels of skepticism may compromise the fundamental trust in the democratic process.

6) **Security Concerns:** Many computer scientists and cyber security experts and documented studies and reports, generally conclude that the current architecture of the Internet and the variety of ways in which its security can be compromised, pose a significant threat and risk to Internet voting systems and electronic ballot delivery. Both private and public entities are susceptible to attacks via the Internet. Experts say they can happen by anyone, anywhere in the world who has a computer and an Internet connection. According to various studies and

reports, Internet voting systems and electronic ballot transmission can be vulnerable to a variety of different attacks.

Scientists at the National Institute of Standards and Technology (NIST), the technical advisors to the U.S. EAC, have been conducting research into the use of electronic technologies to support military and overseas voting, including casting a ballot over the Internet. In a 2008 report entitled, "A Threat Analysis on UOCAVA Voting Systems," NIST analyzed the use of several electronic technologies for different aspects of the absentee voting process. Their research concluded that widely-deployed security technologies and procedures could help mitigate risks associated with electronic ballot delivery, however the risks associated with casting ballots over the Internet were more serious and challenging to overcome.

Specifically, the report concluded that the use of email to return ballots presents several significant security challenges. Several different computer systems are involved in sending an email from a voter to an election official. Many of these systems, such as the voters' computers and email servers, are outside the control of election officials. Attacks on these systems could violate the privacy of voters, modify ballots, or disrupt communication with election officials. Because other individuals or organizations operate these systems, there is little election officials can do to prevent attacks on these systems. The security challenges associated with email return of voted ballots are difficult to overcome using technology widely deployed today.

Additionally the report stated that casting ballots via the web (the Internet) also pose a large number of security challenges that are difficult to overcome. Using this transmission method, voters would log into a web site and submit their selections on a web page. A great deal of trust must be placed in the software on the election server to accurately record votes, as there would be no opportunity for voters to directly verify that their ballots have been recorded correctly. Furthermore, the reports states that similar to email voting systems, a web-based system for casting ballots would rely on computer systems outside the control of election officials. Attacks on these systems, such as voters' computers, could significantly threaten the integrity of elections or the ability of voters to cast ballots. Moreover, less sophisticated attacks, such as phishing and spoofing, could trick voters into giving up their voting credentials to an attacker. Such attacks are common in the banking industry, and are difficult to defend against.

Moreover, in 2011 NIST released a report entitled, "Security Considerations for Remote Electronic UOCAVA Voting," which studied Internet voting in more detail. The report identified and analyzed current and emerging technologies that may mitigate risks to Internet voting, however it also identified several areas that require additional research and technological improvements. Ultimately, the study concluded that Internet voting systems cannot currently be audited with a comparable level of confidence in the audit results as those for polling place systems. The report also concluded that malware on voters' personal computers poses a serious threat that could compromise the secrecy or integrity of voters' ballots. Finally, the report stated that the U.S. currently lacks a public infrastructure for secure electronic voter authentication and recommended that additional research and development is needed to overcome these challenges before secure Internet voting will be feasible.

7) **Electronic Transmission of Ballots in Other States**: According to a 2015 report by the National Conference of State Legislatures, two states permit some voters to return ballots via the Internet. In addition, the District of Columbia and 22 states (Colorado, Delaware, Idaho, Indiana, Iowa, Kansas, Maine, Massachusetts, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, North Dakota, Oregon, South Carolina, Utah, Washington, and West Virginia) permit UOCAVA voters to return their voted ballots by email or fax. Five of the 22 states, however, only permit a UOCAVA voter to return his or her voted ballot via email or fax under certain circumstances, such as when a more secure method is not available, only in certain emergency situations, if the voter is in an area eligible for imminent danger, serving in a hostile fire area, or must also send a hard copy of the ballot via postal mail. The report also states that 19 states do not allow electronic transmission and voters must return voted ballots via postal mail.

   As mentioned above, California permits a military or overseas voter to return a voted ballot via mail or fax.

8) **Existing Laws to Facilitate Voting by Overseas and Military Voters**: On October 28, 2009, President Obama signed into law the Military and Overseas Voter Empowerment (MOVE) Act to expand the 1986 UOCAVA, which was established to protect the rights of service members to vote in federal elections regardless of where they are stationed. The MOVE Act builds on UOCAVA to provide greater protections for service members, their families, and other overseas citizens.

   The provisions of the MOVE Act have been in effect since the November 2010 election. However, given that California law already included provisions to facilitate voting by military members and other California residents who are outside of the U.S., the SOS's office and local elections officials only had to make minimal adjustments to their practices in order to be in compliance. For example, the MOVE Act requires states to establish procedures to allow overseas voters to request voter registration applications and absentee ballot applications by mail or electronically, and requires at least one means of electronic communication for voters to request, and for all states to send, voter registration applications, absentee ballot applications, and voting information. Current law allows a military or overseas voter to register to vote and apply for VBM ballot by facsimile transmission and allows elections official to send a VBM ballot by mail, facsimile, or electronic transmission. Exceeding the requirement of the MOVE Act, current law allows a military or overseas voter who is temporarily living outside of the US to return his or her ballot by facsimile transmission.

   In addition, the MOVE Act requires states to transmit a requested absentee ballot to overseas voters not later than 45 days before an election for federal offices. Again, California law exceeds this requirement by specifically requiring the county elections official to send ballots to overseas voters with a list of all candidates who have qualified for the ballot beginning on the 60th day before the election, along with a list of all measures on which the voter is qualified to vote.

9) **One Step Further**: In addition to being compliant with all provisions in the MOVE Act, California law also makes other accommodations to facilitate voting by military voters and other California residents who are outside of the U.S. Specifically, current law provides that an application for a VBM ballot by an overseas voter is deemed to be a request for voter

registration (if the voter was not already registered to vote) and an application for permanent VBM voter status. In addition, California makes all overseas voters permanent VBM voters, thereby eliminating the need for overseas military voters and other overseas voters to request a VBM ballot for each election.

More recently, in 2012 the Legislature passed and the Governor signed AB 1805 (Huffman), Chapter 744, Statutes of 2012, which established new voting procedures for military and overseas voters, as defined, to comply with the UOCAVA and implement the policies of that act and the Uniform Military & Overseas Voter Act adopted by the National Conference of Commissioners on Uniform State Laws. Among other provisions, AB 1805 expands the universe of people who can be considered military or overseas voters; expands the use of the Federal Write-In Absentee Ballot by allowing it to be used by military or overseas voters in non-federal elections; and makes other conforming changes, where appropriate in California, to ensure continuity and uniformity across state lines for military and overseas voters.

AB 1929 (Gorell), Chapter 694, Statues of 2012, established processes and procedures for the review and approval of ballot marking systems, as defined, for use in California elections. A ballot marking system speeds up the amount of time it takes for military or overseas voter to cast a ballot by allowing a military or overseas voter to electronically obtain a ballot specific to the precinct in which they reside and electronically mark his or her ballot. The information marked on the voter's ballot is formatted onto a document that the voter may print out and mail or fax to their county elections official.

SB 29 (Correa), Chapter 618, Statues of 2014, allows a VBM ballot to be counted if it is cast by election day and received by the elections official by mail no later than three days after the election, as specified.

10) **Efforts on the Federal Level**: The Federal Voting Assistance Program (FVAP) works to ensure service members, their eligible family members, and overseas citizens are aware of their right to vote and have the tools and resources to successfully do so - from anywhere in the world. The Director of FVAP administers UOCAVA on behalf of the Secretary of Defense. In general, the FVAP exists to: 1) assist uniformed services and overseas voters in exercising their right to vote so that they have an equal opportunity with the general population to have their vote counted; 2) assist states in complying with relevant federal laws by providing current information; and 3) advocate on behalf of the uniformed services and overseas voters, identifying impediments to their ability to exercise their right to vote, and proposing methods to overcome those impediments.

According to a 2015 Congressional Research Service report, entitled "The Uniformed and Overseas Citizens Absentee Voting Act: Overview and Issues," the FVAP has had a long history of conducting research on barriers to absentee voting and working with states to determine how these hurdles can be reduced or eliminated. In 2000, FVAP conducted a Voting Over the Internet (VOI) pilot project that was intended to address the specific needs of the military when attempting to vote absentee remotely. The VOI pilot was limited in scope and participation (only 4 states and a total of 350 potential voters were eligible to participate). The project was designed to explore the viability of using the Internet to assist UOCAVA voters, most of whom face unique challenges when registering and voting. According to the report, under the VOI, to request a ballot, a voter would fill out an electronic version of the request form and sign it with a digital certificate. A local elections

official would then post an electronic version of the ballot on a secure server, where it would be retrieved by the voter. Once the ballot was completed by the voter, it was digitally signed and encrypted and placed on a FVAP server. The completed ballot could only be decrypted by the appropriate election office, who printed the ballot and counted it with mail-in absentee ballots. In 2001, FVAP issued a report evaluating the program and noted, among other conclusions, that "further development is needed before Internet remote registration and voting can be provided effectively, reliably, and securely on a large scale."

According to a December 2015 FVAP research report, entitled "Review of FVAP's Work Related to Remote Electronic Voting for the UOCAVA Population," although the VOI was limited in scope and participation, Congress recognized the initial success of the VOI pilot and mandated the conduct of an electronic voting demonstration project (e.g. remote Internet voting) through the National Defense Authorization Act for Fiscal Year 2002 (FY 2002) for a statistically relevant population of absent uniformed service personnel.

As a result, according to the Congressional Research Service report, an expanded version of the VOI project was to be used in the 2002 elections and called on the Secretary of Defense to "carry out a demonstration project under which absent uniformed services voters [were] permitted to cast ballots in the regularly scheduled general election for federal office in November 2002 through an electronic voting system" called the Secure Electronic Registration and Voting Experiment (SERVE). The report states that SERVE was to provide the capability to authenticate voters and local election officials using unique digital signatures. In order to do so the voters and officials had to register with SERVE in order to be assigned the digital identity, which would allow them to access servers hosted by FVAP in order to register and vote. The SERVE program was expanded from four to seven states, with a target of 100,000 participants.

The Congressional Research Service reported that FVAP assembled a Security Peer Review Group to review the SERVE program's security design, and that several members of the group unofficially asserted that the program had fundamental security problems that made it vulnerable to a variety of well-known cyber attacks. The report also stated that as a result, in 2004, the FVAP's attempt to execute the SERVE project was suspended and the defense authorization act for FY 2005 instructed it to wait until the EAC issued guidelines for electronic absentee voting before pursuing another Internet voting project.

According to the December 2015 FVAP research report, in the National Defense Authorization Act for FY 2015, Congress eliminated the requirement for FVAP to conduct the electronic voting demonstration project and with the repeal of that requirement, the Department of Defense is no longer exploring program implementation in this area.

11) **Arguments in Support**: In support, the Inyo County Clerk/Recorder writes:

> Currently twenty-four states allow some voters to return ballots via electronic delivery, but California is not one of them. Military and Overseas voters from California must use either the Postal Service or a fax machine to return their voted ballot.
>
> The last 30 to 40 years have seen a steep decline in the availability of fax machines as demands to move from paper to electronic have increased. If a Military or Overseas voter does not have access to a fax machine, they may not have time to return their ballot

and have it counted in California. However, if that same voter lived in Colorado or the District of Columbia – they would be afforded the ability to use secure electronic methods to return their voted ballot.

12) **Arguments in Opposition**: In opposition, VerifiedVoting.org writes:

> We oppose the electronic transmission of voted ballots because ballots cast over the Internet are highly vulnerable to online failures through attacks and malfunctions of various kinds. We need to safeguard with special care the ballots of our military to ensure they are cast and counted as intended so that our service members are not disenfranchised. Online ballot transmission needlessly risks the security and secrecy of the troops' ballots.
>
> The Federal Voting Assistance Program (FVAP) of the Department of Defense does not support online return of voted ballots, pointing out that given unsolved security issues, postal mail is the "most responsible" method of ballot return. Researchers for the federal government have studied the electronic return of voted ballots for years and have concluded that it is currently not possible to ensure the security, privacy, auditability and integrity of ballots cast over the Internet. For this reason, the U.S. Election Assistance Commission has not set security standards or guidelines for Internet voting systems. There are no federal security guidelines because the federal government concluded online voting cannot be done securely. Return of voted ballots by email, as proposed in AB 887, is considered the "least secure" method of ballot return by election technology experts. Moreover, because federal researchers determined that secure online voting is not currently feasible, last year the federal government ended its effort to try to develop a secure online voting system for the military. The question of offering secure online voting for the troops has been asked and answered. It's not presently possible.
>
> It should be noted that California has a proud standard of requiring voter-verifiable paper records, which are used in post-election manual tallies to check the proper functioning of our systems. Ballots returned by email – even when printed on the receiving end – cannot be construed as voter-verified, because they are digital ballots subject to alteration in transit…

13) **Upcoming Deadlines and Amendments**: Due to impending committee deadlines, if this bill is approved in this committee today, it would need to be heard in the Assembly Appropriations Committee next week, absent a waiver of the Joint Rules. However, if this bill is amended in committee today, that may prevent this bill from being heard in the Assembly Appropriations Committee before next week's deadline for committees to hear and report two-year bills. In light of this fact, if it is the committee's desire to approve this bill with amendments, committee staff recommends that this bill be passed out of committee with the author's commitment to take those amendments subsequent to passage by this committee.

REGISTERED SUPPORT / OPPOSITION:

Support

American Legion-Department of California
AMVETS-Department of California
California Association of County Veterans Service Officers
California State Commanders Veterans Council
Inyo County Clerk/Recorder
Military Officers Association of America, California Council of Chapters
VFW-Department of California
Vietnam Veterans of America-California State Council

Opposition

Secretary of State Alex Padilla (Unless Amended)
VerifiedVoting.org
Five Individuals

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