Date of Hearing: April 23, 2013

ASSEMBLY COMMITTEE ON ELECTIONS AND REDISTRICTING
Paul Fong, Chair
AB 19 (Ting) – As Amended: April 16, 2013

SUBJECT: Internet Voting Pilot Program.

SUMMARY: Establishes processes and procedures for an Internet Voting Pilot Program. Specifically, this bill:

1) Defines the following terms for the purpose of this bill:

   a) "Internet voting" to mean the casting of a secure and secret electronic ballot that is transmitted to the appropriate elections official using the Internet;

   b) "Internet voting system" to mean a voting system that uses electronic ballots and allows a voter to transmit his or her voted electronic ballot to the appropriate elections official over the Internet;

   c) "Program" to mean the Internet Voting Pilot Program authorized by this bill;

   d) "Red team or penetration testing" to mean a method of evaluating the security of an Internet voting system, including its hardware, storage devices, or software, by simulating unauthorized access to the Internet voting system; and,

   e) "Top-to-bottom review" to mean a comprehensive and scientifically rigorous examination and analysis of an Internet voting system.

2) Permits a county, in order to test the viability of conducting a public election via the Internet, to conduct an Internet Voting Pilot Program under which the county may offer Internet voting as an additional method of voting in a local election held within the county if all of the following are satisfied:

   a) The county board of supervisors authorizes the county to conduct the program;

   b) The election is a regularly scheduled or special county, municipal, or district primary or general election. Provides that a local election that includes a candidate for a federal or state office or a state measure on the ballot is not eligible to be included in the program;

   c) The program uses an Internet voting system that was certified by the Secretary of State (SOS) prior to the election in the county at which the system is to be first used; and,

   d) The Internet voting system is offered as an additional and supplemental method of voting, but does not replace any other method of voting or voting system in place within the county.

3) Requires the program to test the viability, accuracy, security, integrity, efficacy, accessibility, and public acceptance of an Internet voting system certified by the SOS.

4) Permits a county, person, or corporation owning or being interested in an Internet voting system to apply to the SOS to examine and certify the Internet voting system. Requires the applicant to submit to the SOS all relevant documentation and information required by the SOS.

5) Requires the SOS, upon receiving an application to examine and certify an Internet voting system, to conduct a top-to-bottom review of the Internet voting system and report on its accuracy, security, integrity, efficacy, and accessibility. Provides that if the SOS's report states that the Internet voting system meets the standards of accuracy, security, integrity, efficacy, and accessibility, then the Internet voting system is deemed to be certified by the SOS and may be used by a county in conducting a program.

6) Requires the top-to-bottom review to include all of the following:

   a) Review and analysis of the Internet voting system's documentation and specifications, security features, and source code for its software and firmware;

   b) Red team or penetration testing to interactively analyze the function and performance of the Internet voting system and identify and document any part of the Internet voting system that may be vulnerable to tampering or error that could cause incorrect recording, tabulation, tallying, or reporting of votes or that could alter critical election data;

   c) Testing and observation of the Internet voting system to evaluate whether it is accessible to voters with disabilities and to voters who require assistance in a language other than English, if the language is one in which a ballot or ballot materials are required to be made available to voters;

   d) Review of reports and available data from any independent examination of the Internet voting system; and,

   e) Review and analysis of any available data relating to the deployment, implementation, and use of the Internet voting system in other jurisdictions.

7) Requires the SOS to make the top-to-bottom review process and the results of each review public.

8) Requires a county that conducts a program to evaluate the program and the county's experience with the Internet voting system and report thereon to the Legislature and the SOS. Requires the report to include a summary of the demographic information of voters who chose to use traditional voting methods compared to those who chose to use Internet voting. Requires the report to be submitted in accordance with specified provisions of existing law.

EXISTING LAW:

1) Defines a "voting system" as any mechanical, electromechanical, or electronic system and its software, or any combination of these used to cast or tabulate votes, or both.
2) Prohibits a voting system or part of a voting system from being connected to the Internet at any time, or from electronically receiving or transmitting election data through an exterior communication network, including public telephone system, when the communication originates from or terminates at a polling place, satellite location, or counting center; or from receiving or transmitting wireless communications or wireless data transfers.

3) Prohibits a voting system, in whole or in part, from being used unless it has received the approval of the SOS prior to any election at which it is to be first used.

4) Prohibits a jurisdiction from purchasing or contracting for a voting system, in whole or in part, unless it has received the approval of the SOS.

5) Permits a person or corporation owning or being interested in a voting system or a part of a voting system to apply to the SOS to examine it and report on its accuracy and efficiency to fulfill its purpose.

6) Requires the SOS to study and adopt regulations and specifications governing the use of voting machines, voting devices, vote tabulating devices, and ballot marking systems and any software used for each, including the programs and procedures for vote tabulating and testing. Requires the criteria for establishing the specifications and regulations to include, but not be limited to, the following:

    a) Requires the machine or device, and its software, to be suitable for the purpose for which it is intended;

    b) Requires the system to preserve the secrecy of the ballot; and,

    c) Requires the system to be safe from fraud or manipulation.

FISCAL EFFECT: Unknown

COMMENTS:

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

> As voters grow accustomed to a world in which they complete more and more personal and business tasks over the internet, including voter registration, it is counterintuitive that they cannot use the internet to participate in the electoral process. In a December, 2012, USA TODAY/Ipsos poll of non-voters which asked what policies would have encouraged them to participate in the election, 28% responded that being able to vote online would help – the top response cited. In addition to encouraging voter turnout, online voting systems offer many benefits to voters that traditional polling place and mail systems do not provide, such as the ability to signal to voters if they make an error in marking their ballot that would have disqualified it from being counted. In a state as diverse as California, it would allow for ballots to be seamlessly translated into any language, improving access for all citizens.

Many other states are exploring how technology can improve voting efficiencies. West Virginia ran a successful online voting pilot program in 2010 with 80% of eligible voters participating in the election, compared to an overall statewide turnout rate of 23%. Colorado has also passed legislation to develop a pilot program, and six other states – Arizona, Connecticut, Hawaii, Illinois, New Jersey, and New York are considering online voting pilot programs this year.

AB 19 would create a pilot program authorizing counties to conduct a local election through an online voting system. This pilot program would allow counties to utilize secure voting systems with a goal of improving Election Day efficiencies, as well as promoting increased access to and participation in the democratic process.

2) New Online Voting System: The change to current law this bill proposes is a major departure from what currently constitutes a voting system. Under current law, no voting system or part of a voting system may be connected to the Internet at any time. This bill would fundamentally change that by allowing the use of an Internet voting system. This measure establishes processes and procedures for the use of an Internet Voting Pilot Program. Specifically, this bill sets up a process whereby an Internet voting system that is tested and certified by the SOS, and subsequently authorized by a county board of supervisors, could be used as a method of voting in a local election. A system, like the one described above, is not currently allowed for use in California elections.

3) What is an Internet or Online Voting System? According to the U.S. Election Assistance Commission's 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. Additionally, 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 (i.e. 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 (i.e. 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.

4) California Internet Voting Task Force: In 1999, Secretary of State Bill Jones convened the California Internet 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.

   The definitions of an Internet voting system and Internet voting as proposed by this bill are substantially similar to the recommended definitions outlined in the Task Force's report

5) Past Voting System Mishaps: In 2002, DRE devices were certified for use in California. DREs are paperless, electronic voting systems that electronically process and store all election data. Many DREs, though not all, use electronic touch screens. Due to the way in which DREs functioned, a voter would have no way of verifying whether or not the voting system was correctly recording his or her votes. For example, the machine could be displaying one candidate's name on the screen while mistakenly or maliciously storing another candidate's name on the official electronic record as the voter's choice. According to a Caltech/MIT Voting Project's 2012 report, because of these concerns, various studies were done and a number of teams examined the voting systems' software and found that although no overtly malicious code was found, the systems were so poorly engineered that they exhibited a high risk of compromise. Furthermore, the report states that other studies that followed showed how the systems could be controlled by malicious parties and infected by viruses.

   In 2004, in an effort to enhance voter confidence and ensure every vote cast is counted, Secretary of State Kevin Shelley decertified DREs, requiring the vendor to retest and

recertify its equipment. Shortly after, Governor Schwarzenegger signed legislation requiring all touch screen electronic voting machines to produce voter-verified paper audit trails of electronic ballots to verify that the voter's preferences were accurately recorded.

6) History of Top-to-Bottom Review (TTBR): In 2007, the Secretary of State Debra Bowen conducted a TTBR of many of the voting systems certified for use in California. The review, led by computer scientists from the University of California, was launched in response to years-long serious, yet unresolved questions, about voting system reliability, security, and transparency. The reliance on proprietary source code for electronic voting systems precluded open, public examination of the entirety of voting systems and many questioned the ability of these voting systems to protect the security of the vote. Consequently, the TTBR was designed to restore the public's confidence in the integrity of the electoral process and to ensure that California voters cast their ballots on machines that are secure, accurate, reliable, and accessible. On August 3, 2007, following the TTBR, Secretary Bowen released the results of the TTBR and issued decertification and recertification orders for the three voting systems subjected to the review and strengthened the security requirements and use conditions for certain systems.

   In short, computer scientists discovered, documented, and demonstrated source code and security vulnerabilities that called into question the security of the voting systems. The review cast doubt on the ability to prevent exploitation of these vulnerabilities, or detect after the fact that these vulnerabilities had been exploited, to manipulate voting systems in ways that could affect the outcome of an election. Moreover, the review found that malicious software code might propagate throughout an entire voting system, including infecting the central tabulation system. Based on those findings, the SOS decertification and recertification orders restricted the number of DRE voting units that could be used at a polling place to one for certain voting systems. The use of one DRE per polling place was permitted so that elections officials could comply with state and federal accessibility requirements. Additionally, the SOS imposed new security measures on all systems to limit and prevent exploitation of voting system source code vulnerabilities. Moreover, with the collaboration of county elections officials and voting system vendors, new use procedures were developed to ensure consistent, uniform implementation of security measures. Finally, new, more stringent post-election auditing requirements of results produced by the voting systems examined in the review were put in place to ensure that tampering or errors did not produce incorrect outcomes in close contests.

   After the TTBR, California's voting system testing and approval processes were modified to be consistent with and include practices and procedures employed in the TTBR. Any new voting system brought forward for approval is now subject to a testing and approval process that incorporates the protocols for source code review in the TTBR.

7) District of Columbia Pilot and Other Security Breaches: 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. A recent example of the vulnerabilities of today's technology can be illustrated by the hack on a pilot Internet voting project in Washington D.C. The Internet voting pilot project was intended to allow overseas absentee voters to cast their ballots using a website. Prior to deploying the system in the

general election, Washington D.C elections officials held a unique public mock trial during which anyone was invited to test the system or attempt to compromise its security. Within 48 hours of the system going live, a team of computer scientists from the University of Michigan hacked into the system, gained near-complete control of the election server, successfully changed votes that had already been cast, retrieved voter identity passwords, and more. The attack went undected for nearly two days.

In addition, recent security breaches have occurred at a variety of large, sophisticated corporations, like Google and Facebook. Reports indicate that the attack on Google targeted email accounts and the perpetrators stole critical assets, like its source code. Moreover, as many as two dozen other companies were targeted with similar attacks and intrusions. However, not only private corporations, but government entities have been vulnerable to attacks. FBI Director Robert Mueller said in 2010 that "hackers actively target our government networks. They seek out technology, our intelligence and our intellectual property."

8) Types of Attacks: As mentioned above, both public and private 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 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.

   Furthermore, scientists at the National Institute of Standards and Technology (NIST), the technical advisors to the EAC, have been conducting research into the use of electronic technologies to support military and overseas voting, including casting ballot over the Internet. In a 2008 report, 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. Moreover, a more recent 2011 NIST study concluded that malware on voters' personal computers poses a serious threat that could compromise the secrecy or integrity of voters' ballots. Additionally, NIST concluded that the United States 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.

9) Secretary of State's Review Process: As mentioned above, this bill permits the use of a new type of system that has never been used in California. Consequently, new testing and certification protocols and procedures will need to be developed to ensure the system is appropriately tested and examined. This bill attempts to address those issues by listing broad terms that the SOS's TTBR must include, such as testing its accuracy, security, integrity, efficacy, and accessibility. Additionally, the bill incorporates some testing features from the 2007 TTBR as part of its review process for an Internet voting system. Despite all of these requirements, the bill does not include specific safeguards or safety measures to protect a voter's private information and voting selections. For example, the bill does not prohibit any vendor of an Internet voting system from capturing or storing any voter information or ballot

selection data derived from the process of marking and transmitting the ballot. As a result, any and all data could be permanently stored, and could theoretically be vulnerable to manipulation. In addition, the bill does not contain any requirements for encryption, security, or other safeguards to protect against the information being intercepted during transmission.

Conversely, because the definition of an Internet voting system, as defined by this bill, falls within the definition of a voting system, the system would be subject to existing laws for approval by the SOS. As such, the SOS would have the authority to establish specifications for, and regulations governing, the Internet voting system to ensure it accomplishes the purpose for which it is intended, preserves the secrecy of the ballot, and ensures the system contains safeguards to protect from fraud and manipulation. Furthermore, if an Internet voting system does not meet the SOS's requirements, it will not be approved for use in the Internet Voting Pilot Program. To clarify this, the committee may wish to amend the bill to explicitly state that an Internet voting system constitutes a voting system as defined by existing law, and therefore is subject to all existing laws pertaining to voting systems.

10) Federal Testing: As mentioned above, current law requires a voting system and any modification to a voting system to be approved by the SOS before it can be used in any elections. Additionally, electronic voting systems must be certified at the federal level by the EAC before they can be submitted to the SOS's office for review. When a voting system is brought to California for review, the SOS conducts a thorough examination and review of the proposed system that includes: a review of the application and documentation, end-to-end functional examination and testing, volume testing under election-like conditions of all voting devices used by the voter, security testing that includes a full source code review and penetration testing, accessibility examination and testing, a public hearing and public comment period. The SOS's review process is designed to augment, not duplicate the EAC review and approval process. However, neither the state nor federal standards include requirements to test and certify Internet voting systems.

With the desire and goal to improve the voting process for military and overseas voters, the EAC was directed to create electronic absentee voting guidelines. In response to that directive, it conducted a study to collect information about experiences of other countries that used Internet voting and Internet voting projects in the US. The goal of the research was to collect, understand, and present information that may be helpful in developing and establishing the guidelines. Consequently, the report explicitly states that EAC does not endorse, approve, or disapprove of any project or system discussed. The report presented a broad review of the Internet voting systems used in elections from January 2000 through November 2011. Among other information provided the report points out that currently there is no single comprehensive federal standard in place for developing and testing Internet voting systems. Previous pilot programs drew heavily from a variety of guidelines, standards, and best practices to develop and implement Internet voting systems, but the majority of the systems were not developed or tested to a single standard. Since no comprehensive federal standards are in place for testing and approving an Internet voting system, it is unclear how the testing and certification process would work for an Internet voting system in California. Furthermore, it may be premature to allow an Internet voting system for use in a local election until a single standard is developed.

11) Transparency: From a voting security standpoint one of the things that stands out is the need for transparency and verifiability of election outcomes. State and federal voting system testing and certification helps ensure voting systems used can mark and tally ballots accurately and securely, while protecting the voter's privacy. However, critics argue that front-end regulation and testing isn't enough and election audits must be included to help ensure the integrity of election outcomes. Consequently, one of the outcomes of the TTBR was the inclusion of new and more stringent post-election auditing requirements to ensure that tampering or errors did not produce incorrect outcomes in close contests. One way in which a post-election audit can be accomplished is by hand-counting a large random sample of cast paper ballots until a sufficient level of statistical confidence is established. Existing law requires an elections official, during the official canvass of every election in which a voting system is used, to conduct a public manual tally of ballots tabulated by those voting systems, including vote by mail ballots, cast in one percent of the precincts chosen at random by the elections official.

    Election audits, aside from providing confidence in the election results, also provide a level of transparency with respect to election results. Current law requires a county election official to report to the SOS the results of a one percent manual tally conducted after each election. The report is required to identify any discrepancies between the machine count and the manual tally and a description of how each of these discrepancies were resolved. Moreover, existing law requires these manual tallies to be conducted in public and further requires the elections official to provide a five-day public notice of the time and place of the manual tally. All of these steps provide transparency to the election process, especially when conducting the audit, to protect the integrity of the election results. It is unclear how an elections official could conduct a meaningful public audit of the election results of an Internet voting system. If a system was compromised and the results were re-run on that same system, they would potentially turn out the same.

    Furthermore, the 2011 NIST report, which extensively studied Internet voting, concluded in that Internet voting systems cannot currently be audited with a comparable level of confidence in the audit results as those for polling place systems.

12) Other States: According to information provided by the author's office, there are a handful of states – Colorado, Arizona, Hawaii, Illinois, and New York – that have introduced bills this legislative session dealing with Internet voting. These proposals vary in their details, and most propose a pilot program or a feasibility study, rather than a full-scale Internet voting program. In addition, Connecticut, and New Jersey, introduced legislation that proposes Internet voting pilot program for military and overseas voters. Moreover, according to a February report from the National Conference of State Legislature, Texas and Mississippi have also introduced feasibility studies on Internet voting.

    The author's office also provided the committee with information detailing West Virginia's 2010 military and overseas online voting pilot projects. In 2010 West Virginia's Legislature passed legislation authorizing the Uniformed Services and Overseas Voter Pilot Program, which allowed Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) voters to vote using an online voting system. As part of the legislation, the West Virginia SOS was charged with evaluating the pilot program for functional effectiveness and to terminate the program should it fail to "adequately and secretly ensure that absent uniformed services

voters and overseas voter have their absentee ballots cast and counted in the primary election." According to the 2010 report, 77 UOCAVA voters, from the five participating counties, applied for an online ballot, and of that, there was an 82 percent return rate for online voters. Additionally, the report states that because no significant deficiencies or concerns were identified with the primary online voting pilot program, it recommended that the project to be continued through the 2010 general election. Subsequently, the West Virginia Legislature passed an expansion bill allowing three additional counties to participate in pilot program for the 2010 general election. A 2011 report provided that 165 UOCAVA voters, in the eight participating counties, completed absentee applications to vote online and, out of that, 125 (76%) cast their ballots using the online voting pilot process.

The 2011 report provides that the online voting applications used a form of cryptography, including separate encryption and decryption algorithms, for creating keys to link the voter data with ballot data. Moreover, the report acknowledges that while neither of the two companies has submitted their processes for validation by the NIST Cryptographic Algorithm Validation Program, there is no current requirement for that review.

Other security measures taken, according to the report, include confidentiality statements for those individuals handling data provided or received by each vendor and the purging of all voter-related data from the vendor systems following the completion of the pilot program.

While neither report identifies any significant deficiencies or concerns raised during their pilot projects, the 2011 report states that after consideration of many factors involved in the conduct of the pilot programs, including voter participation and feedback, security considerations, cost-per-voter, legislative mandates and administration requirements, it recommends a study committee be convened to further review those factors.

Although the West Virginia online pilot program reports are helpful in illustrating that online voting may be a popular option for military and overseas voters, due to its limited scope, it is challenging to conclude whether it will be an attractive method for all voters. Furthermore, while neither report identified any significant deficiencies or concerns raised during their pilot projects and the Internet voting systems did contain similar security protocols necessary to protect the integrity of the election, it still does not definitively resolve the security issues discussed above.

13) Arguments in Opposition: Secretary of State Debra Bowen, writes, in opposition:

> There is widely shared agreement among private and public computer security experts, including cyber security officials at the U.S. Department of Homeland Security, that casting ballots over the Internet is not secure and cannot be made secure. Unlike other voting systems, Internet voting can be attacked by anyone, anywhere in the word who has a computer and an Internet connection…
>
> Large sophisticated corporations like Google and Citibank, both with enormous security resources, have been successfully hacked within the past three years and have had critical assets such as source code stolen. Source codes, as you are aware, are critical to the security and operation of voting systems.

I have many technical concerns with the language of the bill, including how a "top-to-bottom" review of an Internet voting system is defined. However, even if all of my technical concerns were addressed, I would remain strongly opposed to any measure that would permit an Internet voting system be used in any election in California.

14) Previous Legislation: AB 2519 (Shelley) of 2000, would have created an Internet Voting Pilot Program administered by the SOS for the conduct of local elections in not more than three counties. AB 2519 was vetoed by Governor Davis and in his veto message the Governor stated "[b]efore Internet voting can be successfully implemented, security measures to protect against fraud and abuse must be more fully developed. Other states are experimenting with online voting with varying degrees of success. I am not convinced the necessary safeguards are in place to begin this experiment in California."

SB 908 (Runner) of 2011, would have permitted a special absentee voter, as defined, who is temporarily living outside the United States or is called for military services within the United States on or after the final date to make application for a vote by mail ballot, to return his or her ballot by electronic mail, as specified. SB 908 failed passage in this committee.

REGISTERED SUPPORT / OPPOSITION:

Support

Everyone Counts

Opposition

California Common Cause
Secretary of State Debra Bowen
Voting Rights Task Force

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