Open Source Election Technology Institute
530 Lytton Avenue
2nd Floor
Palo Alto, CA 94301 USA
+1 650.600.1450

OSET INSTITUTE

TRUST THE VOTE PROJECT

Friday, 06.July 2018

Hon. Pedro Nava
Chairman
Hon. Sean Varner
Vice Chairman

Milton Marks Commission on
California State Government Organization and Economy
925 L Street, Suite 805
Sacramento, CA 95814

RE: Submission of Public Testimony Regarding Voting Equipment Security
to Little Hoover Commission Hearing, Thursday, 26th July 2018

May it please Chairman Nava & Vice Chairman Varner—

My name is John Sebes, and I have been authorized by my Board of Directors to respond to your invitation and prepare written and oral testimony on behalf of the Open Source Election Technology (OSET) Institute, Inc.—a 501(c)(3) nonprofit election technology research organization headquartered in Palo Alto, CA with over a decade of experience at the intersection of election system design and cyber-security.

I, together with review by our Chief Legal Officer offer this testimony to the Milton Marks Commission ("Little Hoover Commission" or "LHC") for reference in its information gathering process regarding election and voting system technology cyber-security. We have made every effort to ensure I provide accurate information to the best of my knowledge and experience.

We appreciate the invitation to submit this testimony and my opportunity to appear. We hope this will help inform the Commission's investigation.

Respectfully Submitted,

E. John Sebes
Co-Founder &
Chief Technology Officer

Christine M. Santoro
Chief Legal Officer &
Corporate Secretary

Before the
LITTLE HOOVER COMMISSION

In the Matter of	)	OPEN HEARING
	)	
VOTING EQUIPMENT SECURITY	)	Thursday, July 26th, 2018
	)	
AND SECURITY BEST PRACTICES	)	10:00 am PDT
	)	
IN THE STATE OF CALIFORNIA	)	Room 437, State Capitol Building

PUBLIC TESTIMONY SUBMISSION

THE OSET INSTITUTE'S STATEMENT BY CHIEF TECHNOLOGY OFFICER E. JOHN SEBES REGARDING VOTING EQUIPMENT SECURITY AND SECURITY BEST PRACTICES

Introduction

May it please the Chair and Vice Chair, my name is John Sebes and I have been authorized by my Board of Directors to prepare this written (*and related oral*) testimony on behalf of the Open Source Election Technology (OSET) Institute—a nonprofit election technology research organization located in the Silicon Valley with over a decade of experience at the intersection of election system design and cyber-security.

We appreciate that the Commission is examining voting equipment security in California to better understand the strengths and vulnerabilities of the current systems, the policies, processes and procedures around their use and plans to utilize available funding to update this equipment. We further understand that the Commission also plans to learn about the implementation of security best practices in California and opportunities to further improve voting equipment security.

Due to our Institute's subject matter expertise in election technology, and my expertise in information security in particular, the Little Hoover Commission believes my perspective would be valuable. Accordingly, the Commission particularly requests that I respond to eight topics and questions. I do so hereunder.

1. Please provide a brief overview of your background, the OSET Institute's mission and the TrustTheVote Project.

I, John Sebes, am a digital technology professional with over 35 years of experience, focused on cyber-security, government computing, and enterprise computing. Specifically, I have been, and continue to be skilled and adept in computer and digital device software architecture, engineering, and development; digital technology project and product management; and research and development team leadership in both principal investigator and management roles. I am also a serial entrepreneur and technology strategy consultant. I have been immersed in the government I.T. sector of election technology for over a decade, with a particular focus on election cyber-security. Links to my current C.V., and list of publications and patents appears in the Appendix to this testimony.

My organization, which I co-founded in late 2006, the OSET Institute is a tax-exempt 501(c)(3) non-profit, non-partisan California public benefit corporation, with a charter to increase confidence in elections and their outcomes in order to help preserve democracies worldwide. Our mission is to increase integrity and security, lower cost, and improve usability of election administration and voting technology by producing publicly available research, development, and reference implementations of said technology, and advocate for its adoption, adaptation, and deployment to protect and preserve what has become critical democracy infrastructure. Implementation of said infrastructure should produce evidence-based elections that are more "Verifiable, Accurate, Secure, and Transparent" (*in process and technology*) — the so-called "*VAST mandate*" — than any alternative to date.

To achieve that, the Institute's flagship initiative is its fiscally-sponsored TrustTheVote™ Project, which is designing and developing ElectOS™ ("Elect-Oh-S"), a comprehensive technology framework to meet the VAST mandate for voter records management, election preparation, ballot casting and counting, tabulation, reporting, and related analytics and upon which can be deployed voter-facing Apps and services. This project represents 85 percent (85%) of the Institute's activities. Another 10 percent (10%) is directed at providing election systems security assessment, advice, and counsel directly to election jurisdictions and often in collaboration with other cyber-security firms. The final 5 percent (5%) of our work is directed at public policy research and education, as well as advising several agencies and organizations of national and international security communities, including in the United States, at the federal level: DHS, NSC, House and Senate Committees on Intelligence and Homeland Security, Administration and Rules, and election-related caucus groups for both political parties; and at the States' level, legislatures and election administration committees and other legislative bodies on request, as with this Hearing. Internationally, we're providing input to the Alliance of Democracies, the Transatlantic Commission on Election Integrity, and collaborating with the International Federation of Election Systems, the International Republican Institute, the Democratic National Institute, USAID, and the U.S. State Department, as well as other election management bodies abroad on request. In short, we believe that the OSET Institute has built-up domain expertise on election technology rarely available anywhere outside of the U.S. Elections Assistance Commission (EAC); the National Institute of Standards and Technology (NIST); the few remaining commercial vendors of voting systems; several notable academic institutions, and a collection of academicians performing research and development in the discipline such as another witness for this Hearing, Dr. Philip B. Stark. Please refer to the Appendix for links to additional documents about the Institute, TrustTheVote Project, and related works.

2. What is "critical democracy infrastructure" and why should election technology be designated as such?

Critical Democracy Infrastructure, ("CDI") consists of all the technology assets and supporting assets that are required for U.S. state and local election officials to administer and conduct elections. These include technology for voter records management, voter check-in, casting and counting ballots, and managing the tabulation of election results. These and related election infrastructure are critical infrastructure (CI) for three reasons:

1. They have been formally designated as CI, and election officials (EOs) are now CI operators working with government and other organizations to operate like other CI sectors, especially those with government organizations as CI operators, in the power and water sectors for example;
2. They meet the definition of CI, including being necessary for the operation of processes that are critical to the nation's sovereignty (*elections*), assets whose defense is a matter of homeland security, and assets whose threats are a matter of national security;
3. The homeland security and national security aspects have been amply illustrated by attacks by nation state adversaries.

Let's step back for a moment to consider the larger picture. In 2016 we witnessed an unprecedented election cycle wherein at least one foreign state adversary launched successful attacks on our election processes and technology. One clear outcome is that U.S. election infrastructure is now a matter of national security. Arguably, that makes election technology part of the assets of critical infrastructure. Unless we protect this infrastructure against future attacks, the potential for damage recognized in 2016 could be realized as soon as the 2018 Midterm Election in just over 100 days, and certainly in 2020.

Russian state sponsored activities in 2016 are now a recipe for refined capabilities to inflict even greater damage by themselves and others. Protecting against this threat requires a new mindset and a new infrastructure to ensure that election administration can be resilient to attempts at disruption. We know our current election technology is obsolete, and relies on an untrusted dwindling supply chain of replacement parts. We also know there is a challenging and difficult reality regarding an inherently insecure underlying architecture of current voting and election administration technology. Like it or not, polling places are now pop-up data centers, and the allegation that no Internet connectivity is involved is irrelevant to their integrity and security. Moreover, elections workers cannot be expected to match wits and resources with increasingly capable cyber adversaries. Unless there is a reset of the priorities for resourcing election organizations across the nation with better protocols, policies, and technology, our electoral process will continue to be at greater risk of chaos, uncertainty, and upheaval. Proper protection of our election infrastructure is the basis for trust in the results of its operation: declared and accepted election winners and losers, and the orderly transfer of power. That is why we believe the designation of "critical infrastructure" is so imperative to election technology infrastructure, or what we refer to as "critical democracy infrastructure."

In 2016 senior officials in the Obama Administration encouraged the OSET Institute to prepare a comprehensive briefing on election infrastructure as critical infrastructure. It took over a year for us to prepare a document worthy of their request. Thankfully, the new administration's Department of Homeland Security and various elements of Congress continued to be interested and we delivered the Briefing on 11th September 2017. The Appendix provides a link to that Briefing, comprehensive in nature — 75 pages — including a treatment of related cyber-security considerations.

3. How would you define voting equipment security?

To address the question of security of voting equipment carefully, let's start with a narrow definition of voting equipment as the hardware and software for:

1. Devices that voters and election officials (EOs) use for casting and counting ballots, and for managing the process of combining these devices' vote tally data in to vote totals and election results; these are the mission critical elements for turning ballots into election results.
2. The election management systems (EMSs) that include the essential function of preparing these devices for operation in a specific election, and also include a large number of ancillary functions that are not mission critical.

Today's voting systems' EMS include a great deal of non-critical functions that are bundled together as part of the EMS software, and hence pose a security threat to them; therefore, the security of voting equipment also depends the security of the entirety of election management, as well as the security of voting devices.

Security for all these systems includes several types of security including: cyber-security, physical security, personnel security, and more. Cyber-security is the set of technical protection mechanisms that protect these assets from tampering and abuse. Cyber-security includes protections for a variety of threats:

- Hardware-level threats;
- Threats to the systems software and other software that is the platform for the actual software of voting systems;
- Threats to that voting related software;
- Technical threats from physical access; and
- Abuse of insider privilege.

Cyber-security also includes exploitable weakness in protection measures like authentication, access control, and transaction logging.

The definition of voting equipment security, including cyber-security, also includes a definition of threats to be protected against. The threat model of today must be a model that includes threats from nation state adversaries with the most sophisticated teams of cyber-operatives, working in concert with teams that conduct information operations, disinformation, and propaganda.

That definition of voting equipment security is certainly broad in scope, but focusing on cyber-security, the current status is straightforward: there is currently no significant degree of protection of voting machine's and EMS's hardware and software. The basic technology platform for them is 90's PC technology that lacks any of cyber-security mechanisms that would be typical today for mission critical systems. As a result, almost all of voting equipment security today is not cyber-security, but rather several kinds of compensating physical and procedural controls that are operated by local elections staff who in most localities lack any training in critical infrastructure (CI) protection or cyber-defense.

Among the areas where there is *no* significant degree of protection via existing cyber-security mechanisms:

- Voting equipment that is completely vulnerable to hardware level attacks, which we now know is a credible threat to CI of all kinds from state sponsored adversaries. Voting equipment-manufacturing uses hardware components from uncontrolled and undocumented supply chains that can include suppliers based in adversary nations. Local EOs routinely replace failing hardware parts with replacement parts purchased online.
- Voting equipment that is completely vulnerable to system-level attacks on the software platform that runs EMS and voting machine software. These voting system components are based on antique commodity OS technology that has a feature one characteristic that is antithetical to systems that must be certified to operate a fixed set of software. That feature is the *ability to run any compatible software, and for software to be freely modified whether by accident or by malice*.

Every independent assessment of voting system software (*including CA's own 2007 Top-to-Bottom Review*[1]) has yielded findings that the software has an unusual amount of evidence of poor quality yielding a variety of security vulnerabilities; as well as design flaws in the use of cryptography that result in the required data security measures be *essentially useless in the face of any skilled attacker*.

As a result of the foregoing, not only are the systems highly vulnerable, so is the essential data. These systems exist to produce data: vote totals for election results. Since the systems that house and compute the data are fundamentally vulnerable, then so is the data. While proper use of cryptography can partly compensate, no independent review has yet found any evidence that cryptography is properly applied; in fact, quite the opposite.

For additional discussion, please see the Appendix for a link to the OSET Institute's "*Critical Democracy Infrastructure*" Briefing, which includes more detailed threat analysis, as well as a link to a briefing on "*National Security Threats to Election Infrastructure*," which summarizes the most essential points for a national security audience.

4. What are the strengths and weaknesses of the for-profit model of voting equipment with respect to security? How could a nonprofit model address those weaknesses? What are the weaknesses of the nonprofit model and what could be done to mitigate them?

[1] See: http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/

Existing for-profit election technology vendors are in the business of selling legacy technology that was not designed for cyber-security, and is wholly unsuitable as critical infrastructure ("CI"). With that, let's sequentially address each element of your question.

1. For-Profit Weakness: These vendors do not have the wherewithal to go back to the drawing board and create a wholly new generation of election technology designed for the current threat environment. They also lack the market motivation to do so: the current three largest vendors are the survivors of a decade of vendor shrinkage from 10 to 3, serving a market of local Election Officials ("EOs") with insufficient funds to pay for existing products, much less defray vendors' costs of new product development.
2. For-Profit Strength: Existing vendors have strong abilities to deliver voting system services and support of their products. With the exception of a few regional technical support companies, several other for-profit technology companies do have similar government-sector IT services and support abilities, but have chosen not to work in the election market because of burdensome de facto requirements: having developed a voting system product, and paid for a successful certification process at the Federal and state levels.
3. Non-Profit Strength: Non-profit organizations with philanthropic backing and corporate participation (*corporations typically donating technology employee labor*) can execute on a mission of technology development that meets market needs unaddressed by vendors, as has been shown repeatedly with success of technology nonprofits that support infrastructure technology such as Linux; MySQL; Apache; OpenSSL; and HyperLedger (*the latter being the open source software base for blockchain based immutable ledger applications*); as well as government relevant vertical applications in areas as disparate as disaster relief coordination and geospatial information services.
4. Non-Profit Weakness: These non-profit organizations have no capability to deliver government oriented system integration services to deliver technology, and provide requisite customer services and technical support.
5. Unchanged For-Profit Delivery Model: Government organizations will continue to procure integration services and support from commercial organizations. A wide variety of IT integration, services, and support companies already serve government sectors with services based on a variety of open source technology. The existence of open source technology for elections can remove their current barriers to entry in the election market.

5. Is there a role for commercial companies in the above-mentioned nonprofit model?

Yes, *absolutely*. Commercial companies are and will continue to be the source for IT integration and support services that are sought by state and local government procurement processes for election technology. Global, national, and regional IT companies have substantial track records in delivering on procurements that include integration of open source technology.

However, to fully appreciate the role of commercial companies in light of this question and the preceding question (4), we should be clear about the so-called "nonprofit model" in terms of what it is, and what it is not.

The "nonprofit model" *is not*:

- A provider of finished systems delivered to acquiring election organizations.
- A customer service or first-line technical support organization or provider.
- Any sort of business model wherein finished goods are delivered at market pricing.
- A source of completely "free" software.

The "nonprofit model" *is*:

- A source of publicly available election technology (*available by means of an open-source license*) providing access to software source code and related intangible and tangible artifacts or assets.
- A means to develop public software wherein said development costs are paid for by any or all of: philanthropic gifts, grants, and donations; municipal funding; federal or state research and development grants; and/or voluntarily contributed software development labor.
- A "perpetual harvest" of improvements and modifications due to the licensing scheme that requires all such alterations to be offered to all other licensees under the same terms of the public license by which the maker of improvements acquired said software in the first place.
- A lower cost of acquisition for said software technology due to an absence of software licensing costs (*royalties*), but the total cost of ownership may require professional grade services for software adaptation, deployment, service, and support, thus the software is not completely "free."
- A means of enabling complete transparency of the software source code in at least its completed state for purposes of peer-reviewed quality assurance and operational audit.
- A secondary (*not primary*) source of technical support provided to those commercial companies that make and deliver finished systems. In other words, because the nonprofit organizations or source of technology exist only to provide the foundational software, and the market looks to

commercial entities for delivery of finished systems, therefore, the "nonprofit model" avails technical support for the technology researched and developed to those technically adept at commercially delivering said technology in finished goods and services.

- An alternative, but arguably essential means to providing imperative innovation in election and voting software technology, available equally and fairly to any organization, wherein there is no available business incentive for the commercial industry to invest in the required research and development to produce said innovations on its own.

Thus, in sum and substance, the nonprofit model is a source of much needed technology innovation, where the costs of such research and development are covered or defrayed through philanthropic and government funding. That technology becomes equally available to all for the commercial market to adapt, deliver, enhance, and support finished voting and election administration products, systems, and services. This is because the "nonprofit model" does not typically include or cover the balance of commercially provided services including but not limited to customer service and technical support. The "nonprofit model" is purely a source for the required innovations unlikely to be produced by the industry due to persistent market constraints.

6. In its study on voter participation, the Commission learned about the in-house voting system that Los Angeles County is creating. When might it make sense for county election officials to design and build their own voting system and when might it make sense for county election officials to work with an organization like yours?

Let's begin by observing that Los Angeles County's situation is unique, its government having chosen to:

- Not adopt any of the early 21st century voting technology now being replaced;
- Develop its own in-house election management system based on LA County's IT system; and
- Reserve both HAVA and State funds for this and other development of election technology that meets the unique needs of the largest local election jurisdiction.

No other California county has any of these characteristics. For California's smaller counties, in particular, it appears that it would be more expedient to participate in public technology development projects that can create necessary software for individual voting systems components that meet needs common to several counties, and that can take advantage of California's ability to create voting system technology certification processes that include publicly available (*i.e., subject to OSI-accredited open* *source licensing*) technology. A good starting point might be components that perform tabulation management or central count optical scan.

Next, let's consider a fuller answer to the larger underlying question. There are layers to the inquiry taken here in points:

1. Off-The-Shelf vs. Custom Build. At the highest level there is an inherent "make-or-buy" question. Any county election organization can consider this question if what is currently available in the marketplace cannot meet or exceed their requirements for a new voting system. If the answer is that the marketplace is unable to provide what the county requires, then the question becomes whether to design and develop internally, or partner with, collaborate with, or hire the resources to do so. Therefore, we believe the answer is, "*When what is currently available as a voting system product cannot meet or exceed the minimum requirements to achieve the so-called "VAST mandate" of trustworthy election administration; that is, a system that is Verifiable, Accurate, Secure, and Transparent, the county should turn to a custom-developed solution.*"

2. Capacity Planning. Now, the "make-or-buy" question shifts to whether the custom build can occur in-house or needs to be out-sourced. The answer is first and foremost gated by the extent to which the county has internal access to I.T. technical development resources to do this "in-house." If they (*as in the vast majority of California counties*) lack the in-house capability, then they are compelled to seek an external (*out-sourced*) development firm on contract or pursuant to some sort of collaborative development agreement.

3. The Procurement Decision. Once the out-sourcing decision is made, then comes the procurement process of a call for bids, selecting, and negotiating a services agreement with a vendor. The challenges of procuring an outsourced development will have cost, intellectual property ownership, and other contractual considerations worthy of a separate paper. I focus in this testimony on the most important factors that weigh on your second question regarding the type of collaboration partner (*commercial vs. nonprofit*), and that is below.

4. The Nonprofit Collaboration Partner. Turning to the second question of "*when might it make sense to collaborate or partner with an external organization like the OSET Institute,*" I assume for sake of this question that you are separating non-profit organizations such as ours, from other commercial software development firms that perform work-made-for-hire. Such separation is astute. The

decision to work with a unique organization such as the OSET Institute should be predicated on the issues of **a**) cost to acquire the solution; **b**) domain expertise, special capabilities, and skills of the prospective development partner; and **c**) the ability to successfully acquire precisely to specifications the desired system solution. Under the circumstances—conditions that certainly contributed to the inability of Travis County, Texas to build their STARVote system, and conditions that may impact San Francisco, California's ability to build their own—an important consideration is the willingness of any collaborator, partner, or vendor to deliver, *without additional encumbrances*, one hundred percent (100%) of the finished software source code and commit to supporting that code base for all errors and omissions incurred in its initial development. Herein lies the distinct advantage in working with an organization such as the OSET Institute: *A nonprofit organization exists for the public benefit*. The objective is to build at cost, without any profit margin, the required technology solution, with the proviso that the results are one hundred percent (100%) the property of the County (*or State; see below*) without further encumbrance. Since taxpayer dollars are utilized to pay for such development costs, then the results should be publicly available to any other county that might want to adopt, adapt, and deploy the same or similar resulting system. Unlike commercial vendors of software development services (*where the vendor has a for-profit business model and a fair market margin is required*), a nonprofit development firm offers a distinct cost saving advantage—*there is no profit margin and often times portions of the development cost may already be absorbed elsewhere*. The reality is commercial vendors will charge one rate if the resulting technology is theirs to re-sell to others at some point after work is complete, and another, significantly higher rate if the development and delivery affords the commercial firm no intellectual property rights whatsoever. Thus, it makes sense to collaborate and partner with a public benefit corporation to develop this technology if the intent is to retain absolute and total unencumbered ownership of the resulting technology, as that nonprofit organization has (*or better have*) a mission to foster that same result.

Stepping back from this further and extrapolating to the entire State of California, we believe it would make very good sense for the State to seriously consider, on behalf of all California counties, whether it should fund a *digital public works project* to accomplish precisely that objective: a base of innovative publicly owned election technology that is higher integrity, more secure, lower cost, easier to use and is more verifiable, accurate, secure, and transparent than anything commercially available. We know for a fact, given substantial engineering cost-to-complete reviews by some of the best in the Silicon Valley, that such a technology project <u>*can*</u> be completed for a fraction of the cost expended on (*for example*) the California statewide voter registration database management system, or a fraction of the intended set aside of capital for counties to replace their current systems with largely the same caliber technology from the few remaining commercial vendors of existing systems. The very important point to remember in all of this: *solve for one is solving for all*. In other words, California could take a lead in solving for a more verifiable, accurate, secure, and transparent voting system platform and given its publicly owned (*open source*) status, that result could solve for the same problems that exist nationwide and even globally.

Thus, we believe the decision to work with an organization like ours or others (*e.g., academic, private, or public institutions performing research on this class of government technology*) makes tremendous, cost-effective, sense if the State and its counties conclude (*as they should*) that the currently available system alternatives cannot meet or exceed the requirements for truly trustworthy voting technology for which the State and its counties would have unfettered ownership of, and control over its development, enhancement, auditing, maintenance, and service.

7. What are the objections you most frequently hear about moving away from a for-profit model for voting equipment? What is your response to those objections?

First, we want to be clear that the OSET Institute does *not* believe that there should or needs to be a "*move away from a for-profit model for voting equipment*." The OSET Institute believes that in order to make possible the kind of innovative, higher integrity, lower cost, easier to use election administration technology required to serve as critical infrastructure, that the necessary research and development to produce such technology must be performed as a *digital public works project*—akin to how other fundamental technology innovations have been publicly funded and made available. For example, the development of the Internet infrastructure that gave rise to the entire digital economy was made possible through funding administered by the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency (DARPA). By injecting a new layer of technology innovation into the existing market for this sector of government technology, the flagging voting systems industry would experience:

- Lowering barriers to entry for new vendors;
- Reducing switching costs for counties;
- A more level playing field for all commercial delivery organizations of voting systems; and
- Shifting the business model away from proprietary systems vending to an open standards, open source, transparent systems integration business.

With that premise, responding to your question, the most frequent objections are likely based on a misunderstanding of how publicly available (*open source*) technology has worked in government computing for decades. For example: most counties cannot build their own voting system even if all the components were available to do so. That is why commercial vendors will continue to be the principal and preferred source for professional-grade information technology ("I.T.") integration services and support, sought in State and local government procurement for election technology, including voting systems components based on publicly available (*open source*) technology.

Therefore, there is no need for an evolution away from a for-profit model for voting equipment, any more than there was a movement away from a for-profit model for Federal systems integration, which now has a larger set of competing vendors all of whom use publicly available (*open source*) technology where appropriate. The evolution is more of an expansion of the model for how voting systems' base technology is developed, to include open source technology. The availability of public technology can catalyze new competition with new for-profit participants in the voting systems market as suggested above in our preface to answering your question.

In the Appendix there is a link to a recent paper we produced at the request of members of Congress about the appropriate use of open source technology in government mission critical computing. That paper catalogs a complete assessment of the common objections.

8. The Commission is interested in any other information or recommendations you believe would be useful as it studies voting equipment security.

First, on behalf of my organization, I sincerely appreciate the opportunity to share our knowledge and perspectives on this topic, backed by over a decade of experience in research, design, and development of election technology using a user-centered design approach backed by a security-centric engineering practice. We have traveled the country, worked with over 200 election officials across more than two-dozen states, and have been actively participating in the conversations about how to better protect voting equipment as critical infrastructure, as well as participating in the development of open data standards, voluntary voting system design guidelines, and modernizing testing and certification processes. This has included participating in hearings, meetings, and providing consultative and educational services at both the federal and state levels. Thus, the opportunity to do so for the great state (*and our home*) of California is as important as anywhere else, even in light of California being more capable, prepared, and innovative than most, thanks to the State Secretary's thought leadership, and the innovative initiatives in counties such as Los Angeles and San Francisco. With that, three (3) recommendations follow.

1. Setting the Pace of Nationwide Innovation in Critical Election Technology Infrastructure

Our top recommendation is that California should actively pursue the role as a "*State Laboratory of Election Technology Innovation*" that can (*and likely would*) be followed by other States, nationwide. Specifically, California can, and should lead in three areas:

A. Election technology evaluation;
B. Cyber-security assessment and testing; and
C. Voting system certification.

The current Federal certification process is fundamentally ineffective, especially with regard to cyber-security. This includes uniform failure on cyber-security assessment in every case that a federally certified voting system product has been independently assessed, starting with California's own 2007 Top-to-Bottom Review. Specifically, there are several areas of activity where California can lead:

- Definition of individually certifiable voting system components that are mission-critical and security-critical, and that meet California's needs (*especially those of smaller counties*) such as: ballot scanning/counting devices and tabulation management devices.
- Assisting in accelerated completion of Federal data interoperability standards, and adoption of them as requirements for California certification of interoperating voting system components.
- Adding to the California certification process the use of existing Federal/military cyber-security assessment and certification programs, applied to individual voting system components with California-specific security requirements.

These and other positive changes to the certification process, including a renewed focus on cyber-security, can help the next generation of election technology to be developed by a wider range of organizations, and with a higher bar for cyber-security and protection of critical election infrastructure.

2. Setting the Standard of Nationwide Election Verification

A second recommendation is for California assuming leadership for what may (*arguably should*) be become national standards for non-technical, procedural elements of overall security of election processes, especially for county-level risk-limiting audits of paper ballots, supervised by the State for compliance with state requirements for procedures and published results.

3. Taking Leadership for Election Technology Innovation to Solve a State, National, & Global Challenge

Our final and admittedly bold, yet very tractable recommendation is for the State of California to commit to, fund, and lead the mission to develop and make available a new platform of publicly owned election technology. Using the most conservative projections, this would be a $40 million, 2-year initiative. It would showcase the best of this great States' technology sector innovation. It would result in a complete election administration technology platform for which a number of California based technology companies, academic institutions, and nonprofit organizations would contribute to the moral imperative of increasing integrity, lowering costs, and improving usability of critical democracy infrastructure. Solving for all of California would lead to solving for every State in the Union, and making available technology on a global basis on which to ensure confidence in elections and their outcomes in order to preserve democracy everywhere. And, it would catalyze a rejuvenated commercial industry to deliver finished systems based on the resulting public technology.

Certainly, in full disclosure, we envision this as a pathway for the TrustTheVote Project to complete its work, *but it would not be our efforts alone*. In addition to the State Secretary's office, state I.T. organizations, and county election organizations input, the contributions and work of individuals and organizations could potentially include, as a sample and certainly not limited to:

Academic and Nonprofit Organizations

- University California at Berkeley
- University California at Davis
- Leland Stanford Jr. University
- California Institute of Technology
- The OSET Institute
- The Verified Voting Foundation

Corporate Contributors & Supporters

- Apple, Inc.
- Alphabet Inc. & Google Inc.
- Hewlett Packard, Inc. (HP Labs)
- Intel Corporation
- Microsoft, Inc.
- Oracle Corporation

Indeed, this would be a bold, but we believe natural and near obvious undertaking for the State of California—the home of some of the greatest innovation in the world. We believe this legacy-making recommendation is a natural leadership move that the California State Legislature can and should make. We would be honored to discuss with the Commission how this could work.

In Closing

On behalf of the OSET Institute, I thank the Chair, Vice Chair, and the entire Commission for considering our contributions here, and on the 26th of July in person, toward your further understanding of the issues of voting equipment security and best practices.

We believe that America and California's electoral infrastructure is a matter of national security. We believe that any attempt to compromise that infrastructure, or the administration of elections, or any of the processes of free and fair elections as a part of the operational continuity of our democracy at any level of government, including every county in, and the State of California, is a violation of our nation's sovereignty.

Going forward, we further believe this electoral infrastructure must be updated and upgraded to afford it the verifiability, accuracy, security and transparency essential to free and fair elections where ballots are counted as cast, and confidence is high in elections and their outcomes. To this end, we appreciate your thought leadership in considering the security of voting equipment.

Respectfully Submitted,

E. John Sebes

Co-Founder & Chief Technology Officer
OSET Institute, Inc.
Palo Alto, CA

Friday, 06th July, 2018 4:00PM PDT

Appendix

Citation Links in Support of Testimony of E. John Sebes Before the Milton Marks Commission

About the Witness E. John Sebes

Summary:
http://www.osetfoundation.org/about-us#sebesbio

Professional C.V.:
https://www.linkedin.com/in/johnsebes/

List of Publications:
https://sebes.com/e-john-sebes-publications/

List of Patents:
https://sebes.com/e-john-sebes-patents/

About the OSET Institute, Inc.

Corporate Web Site:
https://www.osetfoundation.org

Fact Sheet:
https://trustthevote.org/wp-content/uploads/2018/07/2018_FactSheet-OSET.pdf

Executive Summary:
https://trustthevote.org/wp-content/uploads/2018/07/2018_1-PageIntro.pdf

About the TrustTheVote Project

Project Web Site:
https://www.trustthevote.org

2-Minute Introductory Video:
https://vimeo.com/181771227

A Visual Tour of the ElectOS Platform Design:
https://bit.ly/EOSt1

Fact Sheet:
https://trustthevote.org/wp-content/uploads/2018/07/2018_FactSheet-ElectOS.pdf

Important Resources in Support of Testimony

OSET Critical Democracy Infrastructure Briefing:
http://www.osetfoundation.org/research/2017/9/11/critical-democracy-infrastructure

National Security Threats to Election Infrastructure:
https://trustthevote.org/wp-content/uploads/2018/02/oset_protectingelectiontech_nov7.pdf

Appropriate Use of Open Source Technology in Government Mission Critical Computing:
http://www.osetfoundation.org/research/2018/3/12/appropriate-use-oss