



State of California

925 L Street, Suite 805  
Sacramento, CA 95814  
PH: 916-445-2125

Report #247

March 4, 2019

The Honorable Gavin Newsom  
Governor of California

The Honorable Toni Atkins  
President pro Tempore of the Senate  
and members of the Senate

The Honorable Shannon Grove  
Senate Minority Leader

The Honorable Anthony Rendon  
Speaker of the Assembly  
and members of the Assembly

The Honorable Marie Waldron  
Assembly Minority Leader

**Re: Voting Equipment Security**

Dear Governor and Members of the Legislature:

A healthy democracy requires faith in the security of its voting equipment and accuracy of the votes it counts. The vulnerability of election systems nationwide has grabbed the public's attention since the Department of Homeland Security stated that Russians had targeted election systems in at least 21 states in the run-up to the 2016 General Election.<sup>1</sup> Security means much more than protection against malicious threats, however. It means assuring every component of every system used in the election process functions to accurately count and report votes. It means every process and policy surrounding that equipment is followed correctly. It means election officials can prove to the public with certainty that the reported outcome actually represents their votes.

The Legislature, Secretary of State and local election officials have taken important measures to protect California's voting equipment and ensure election results reflect voters' intent. This letter highlights the opportunities and challenges that remain:

- Old and outdated voting equipment presents one of the greatest threats to election integrity in California.
- California could better prove election results.
- California lacks statewide goals for election system innovation.

Pedro Nava  
Chairman  
Sean Vamer  
Vice Chairman  
David Beier  
Iveta Brigis  
Cynthia Buiza  
Bill Emmerson  
Chad Mayes  
Assemblymember  
Bill Quirk  
Assemblymember  
Richard Roth  
Senator  
Cathy Schwamberger  
Janna Sidley

## **Background**

The Commission initiated this study to ensure voting equipment in California meets certain standards, including impenetrable security, to provide confidence in the integrity of California's election systems. During the course of its recent review on voter participation,<sup>2</sup> the Commission determined it needed to learn more about how California protects its voting equipment to ensure that all votes count. Thus, with this study, the Commission sought to review how the state operates and protects its elections equipment, as well as identify new opportunities to sustain and enhance that security.

Importantly, this review focused on the security of the equipment involved in voting, and not an assessment on individual's access to voting. Additionally, throughout this study, the term voting equipment security refers comprehensively to the different components used in election systems. In testimony to the U.S. House of Representative, security expert Matt Blaze said these components include the software and hardware used in voter registration, ballot definition, voting machine provisioning, absentee and early voting processing, tallying and reporting, as well as the voting machines found at the precincts, which includes optical scan ballot readers for pen-and-paper ballots, ballot-marking devices for voters who benefit from assistive technologies, direct recording equipment machines, and electronic poll books.<sup>3</sup>

During this review, the Commission heard debate on the many nuances of implementing best practices for securing voting equipment. However, the Commission did not weigh the benefits and risks of these various practices. This letter is intended to raise thought-provoking questions for policymakers to consider so that each jurisdiction accurately and efficiently records and reports votes.

## **Challenges and Opportunities**

The Commission learned about measures the state takes to protect its voting equipment. These include:

- Certifying all elections equipment before use in California and testing that equipment before each election;
- Requiring a paper record of every vote cast in the state;
- Auditing the results of each election by checking the physical record of a vote against the recorded result; and,
- Establishing the Office of Elections Cybersecurity to keep up with the evolving nature of security threats.

Despite these efforts, the Commission believes that the Governor and Legislature should recognize the ongoing and persistent challenges to California's voting equipment security and take appropriate action. Sustained commitment and diligence to address these challenges will ensure that no eligible California voter casts a useless vote in any election due to government error, malicious attacks or other failures.

## **Old and outdated voting equipment is a threat to election integrity in California.**

Aging voting systems are one of the greatest threats to the integrity of our elections, according to Secretary of State Alex Padilla.<sup>4</sup> Some counties use voting systems that date back to the 1990s and early 2000s. Not only is this outdated equipment vulnerable to modern threats, but it also is more likely to malfunction and incorrectly record votes. “Imagine trying to use your laptop from 15 years ago,” Inyo County Clerk-Recorder Kammi Foote told the Commission.<sup>5</sup> For example, the calibration on older voting equipment becomes less accurate over time on touchscreen machines, and the sealant erodes over time, causing the screen to become misaligned.<sup>6</sup> This can result in vote flipping – when the voter selects one candidate but the machine records a vote for a different candidate.<sup>7</sup> Voting machine malfunctions occurred in at least 13 states during the 2018 General Election as a result of machine age, environmental conditions, and other factors.<sup>8</sup>

Further, when election officials have to replace parts in derelict machines no longer supported by manufacturers, they sometimes have to turn to insecure sources. For example, Secretary Padilla stated that election officials in California sometimes buy replacement parts on EBay and other insecure venues.<sup>9</sup> This not only raises obvious inefficiencies, but exposes the machines to various methods in which bad actors could compromise the voting process.

Despite significant problems and costs caused from using outdated equipment, county officials only have received two influxes of federal and state funding to upgrade their election equipment since the turn of the century. The first resulted from the aftermath of the “hanging chad” debacle in the 2000 General Election, when California received \$392 million from the federal government and \$200 million from voter-approved funds.<sup>10</sup> The second occurred in 2018, following reports of Russian interference in the 2016 General Election, when Congress directed roughly \$34.5 million to California to modernize voting equipment and voter registration databases.<sup>11</sup> Additionally, in his 2018-19 budget, Governor Brown allocated \$134.3 million from the General Fund for counties to upgrade their voting systems.<sup>12</sup>

This sporadic funding cycle does not allow election officials to plan for maintaining, upgrading, and replacing their voting equipment on a continuous basis. County supervisors often must make hard decisions among competing funding priorities to determine if they should supplement limited elections budgets for these purposes. The County of Inyo’s elections operations budget of roughly \$60,000 per year, for example, makes it difficult to set money aside to purchase new systems without federal or state assistance.<sup>13</sup>

Questions for policymakers to consider:

- Could disbursement of state funding for voting equipment be restructured to allow election officials to plan for routine upgrades and replacement?
- Are current funding levels for voting equipment security sufficient to ensure election security across all counties?
- Would additional funding result in future efficiencies and cost savings?

## California could better prove election results.

Proving the veracity of election results means both ensuring the physical security of ballots from the time they are issued to voters and cast, as well as verifying the accuracy of the vote count following an election. California was innovative in instituting a post-election ballot audit in 1965, but it has not updated its audit methodology as statistical methodology has evolved. Further, when conducting ballot audits, election officials assume that the ballots themselves are secure and trustworthy, but the state does not publicly prove it to voters.

“Good elections require technology to be available and functioning correctly and reliably; secure elections require us to prove this was the case,” testified Pam Smith, senior advisor at Verified Voting.<sup>14</sup> Proving to the officials running an election, the losing candidates and their supporters, and the population at large that reported election results accurately captured voters’ selection is critical for two reasons: The process provides an opportunity to uncover and correct mistakes and it creates trust in election results, which provides legitimacy to elections.

Before election officials audit election results, they must verify, with certainty, the trustworthiness of the ballots. Audits are worthless if doubts exist about the integrity of the ballot, from casting through its proper storage and disposal. Although California has laws in place to protect the handling, storage, and ultimately, destruction of the ballots, it has no audit policies to prove election officials follow these security procedures statewide.<sup>15</sup>

Noncompliance – intentional or unintentional – with policies and procedures can threaten election integrity. Nationwide reports of compliance lapses that affected voters’ ability to cast a ballot during the 2018 General Election include officials forgetting to give voters the second page of their ballot, forgetting to turn on ballot scanning equipment, not finding the voting machines, being unable to unlock polling places, shipping voting machines to the wrong location, and encountering difficulties entering passwords to access voting equipment.<sup>16</sup>

Witnesses told Commissioners California should implement a compliance audit for physical security measures. They said election officials should conduct compliance audits through a publicly verifiable process and include audit findings submitted from all jurisdictions.<sup>17</sup> A sample framework for a compliance audit submitted by Philip Stark, U.C. Berkeley Associate Dean of Mathematical and Physical Sciences, is available on the Commission’s website.<sup>18</sup>

California counties currently conduct post-election ballot audits called the 1 percent manual tally. In these audits, election officials randomly select 1 percent of participating precincts and review the ballots cast in those precincts to “ensure agreement between what the voter sees, what the voting system records and what is counted by back-end tabulation systems.”<sup>19</sup> Election officials have a few options on how to conduct the manual tally that leave them with the discretion to exclude vote-by-mail and provisional ballots from the audit.<sup>20</sup> Though innovative when first implemented in 1965, witnesses described some problems with the manual tally. Specifically, it does not guarantee election officials will catch and correct errors. If they find a discrepancy between how someone voted and how that vote was recorded or reported, election officials have no obligation to take any specific action except report on what they did about it.<sup>21</sup> It does not require an audit of all types of ballots. Finally, it does not require

scrutiny of close races. If a candidate or members of the public have concerns about accuracy in a tight race, they can request a recount – but only if they pay for it.<sup>22</sup>

As an alternative, some witnesses recommend the state consider broadly employing risk-limiting audits. Risk-limiting audits review randomly-selected ballots from all cast ballots until sufficient evidence verifies the correct outcome.<sup>23</sup> “Sufficient evidence” is determined by the risk limit – the chance that an audit will not discover and correct a wrong outcome<sup>24</sup> – set by policymakers.<sup>25</sup> For example, a risk limit of 10 percent means there is no more than a 10 percent chance that the audit will not catch and correct a wrong outcome.<sup>26</sup> A smaller risk limit provides stronger evidence of a correct outcome than a larger risk limit.<sup>27</sup> In addition to providing a statistical guarantee that an audit will actually catch and correct any wrong outcomes, risk-limiting audits require election officials to pay particular attention to close races and those that show discrepancies between how voters voted on ballots and reported results.

Recently enacted legislation requires the Secretary of State to create a regulatory framework for counties that want to voluntarily use risk-limiting audits in the 2020 General Election in order to better protect against threats and improve transparency and accountability. According to its author, the legislation intended to modernize California’s post-election audit process to protect against hacking and fraud; allow election officials to do their jobs more efficiency and transparently, and; provide greater confidence to the public in the accuracy of their reported vote.<sup>28</sup> Witnesses discussed the potential benefits of this legislation, but shared that counties may encounter challenges given the lack of state funding available to implement the voluntary reforms.

Questions for policymakers to consider:

- How can the state ensure compliance with physical security procedures for voting equipment across all of California’s counties?
- Has the creation of a voluntary post-election audit program strengthened protections in some counties more than others? How can California ensure all counties equally have the highest levels of security, accountability, and transparency with regards to their election results?
- Does the Secretary of State plan to analyze what the impediments are to implementing a more robust audit across all counties and work with local officials and the Legislature to overcome those challenges?

### **California lacks statewide goals for election system innovation.**

Despite hearing several ideas to bolster voting equipment security from a diverse stakeholder community, from county election officials to Silicon Valley visionaries, the Commission found California has yet to develop a clear vision and plan to implement innovative improvements statewide.

The Commission heard several ideas to improve voting equipment security, from relatively straightforward actions that could be taken by the Secretary of State to large statewide projects. One example: The re-certification process for updated voting equipment can be lengthy and expensive, which can serve as a deterrent to making these critical updates.<sup>29</sup> Currently, any new or modified voting system must undergo extensive testing and evaluation of its hardware and software before the Secretary of State can certify it for use in elections. Testing may include hardware and software hacking, reviewing source code, and validating system function and performance under normal and abnormal

conditions. Tests also may evaluate the equipment's ability to withstand different environmental conditions, storage, maintenance and transportation.<sup>30</sup> One witness suggested the Secretary of State's office should consider ways to make the re-certification process more flexible and timely by allowing certification of individual components of an election system, rather than requiring re-certification of a system in its entirety.<sup>31</sup>

Witnesses observed that the profit structure in election equipment currently does not incentivize security. They said the infrequent purchases of voting equipment render security upgrades to already-certified equipment expensive and results in time-consuming re-certification processes.

Some witnesses suggested California fund a digital public works project to develop publicly-owned election technology. The Commission's witnesses stressed the benefits of making that technology open source, in this case meaning that individuals could examine the source code and identify security flaws, but only authorized personnel could make changes to the code. Compared to current technology, publicly owned election technology is "higher integrity, more secure, lower cost, easier to use and is more verifiable, accurate, secure, and transparent than anything commercially available," John E. Sebes, Chief Technology Officer for the Open Source Election Technology Institute explained.<sup>32</sup> Witnesses also suggested the flexibility of this system could accommodate the wide-ranging needs of California's counties. They said some counties might benefit from public-private partnerships to create a system compatible with commercial off-the-shelf products while other counties could incorporate publicly-owned technology into a new, customized system designed from the ground up.<sup>33</sup>

Whatever improvements in election equipment security it makes, California needs to engage in strategic planning to implement best practices consistently across California's 58 counties. The Commission heard from members of the election security community eager to engage in conversations about ways to boldly innovate elections security as well as those knowledgeable about the intricacies of running elections. State leaders should involve this community in conversations about goals to improve California's election equipment, and articulate a path to achieve those outcomes. This sort of strategic planning is evident in other policy areas, such as natural resources. Regarding strategic management of the Salton Sea, for example, the state has held workshops in which innovators can discuss their ideas for managing and improving the deteriorating environmental conditions. Additionally, it has facilitated a number of other workshops in which the public and local partners can weigh in on the state's master plan. Given the importance of maintaining secure elections, this type of engagement is a critical missing piece in improving election security.

Questions for policymakers to consider:

- What mechanisms are available for policymakers and state officials to engage with stakeholders on developing "out of the box" ideas to improve voting equipment security?
- How can California implement innovative ideas to improve election security?

## **Conclusion**

The Commission acknowledges the state's commitment to voting equipment security and the important efforts already underway to secure California's elections. But malicious attackers do not take breaks, nor do time and tricky environmental conditions slow their deleterious effects on equipment. State officials

should be equally relentless when it comes to pushing the bar ever higher for security and ensuring that a vote cast in one county is no less secure than a vote cast in another county. The Commission hopes this letter report will assist the new administration and Legislature in considering how to focus their attention and state resources to ensure that every Californian's vote counts. The Commission stands ready to assist.

Sincerely,

A handwritten signature in black ink, appearing to be 'PN' with a stylized flourish extending to the right.

Pedro Nava  
Chairman

CC: Alex Padilla, California Secretary of State

## **Appendix A: Public Hearing Witnesses**

The lists below reflect the titles and positions of witnesses at the time of the hearings.

***Public Hearing on Voting Equipment Security  
July 26, 2018  
Sacramento, California***

Kenneth Bennett, Program Manager, Voting Solutions for All People (VSAP), Los Angeles County Registrar-Recorder/County Clerk

E. John Sebes, Chief Technology Officer, Open Source Election Technology (OSET) Institute

Kammi Foote, Clerk-Recorder, County of Inyo

Pamela Smith, Senior Advisor, Verified Voting

Susan Lapsley, Deputy Secretary of State, HAVA Director and Counsel, California Secretary of State

Philip Stark, Associate Dean, Mathematical and Physical Sciences and Professor, Department of Statistics, University of California, Berkeley

Noel Runyan, Owner, Personal Data Systems

## Notes

---

<sup>1</sup> Sari Horwitz, Ellen Nakashima, and Matea Gold. September 22, 2017. DHS Tells States about Russian Hacking During 2016 Election. *Washington Post*. [https://www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e\\_story.html?utm\\_term=.2a8bef41acae](https://www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.2a8bef41acae). Accessed December 26, 2018.

<sup>2</sup> Little Hoover Commission. October 2018. *Letter to Governor Brown and Legislature on Voter Participation in New Motor Voter Program*.

<sup>3</sup> Matt Blaze, Professor, Computer and Information Science, University of Pennsylvania. November 29, 2017. Written testimony to U.S. House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology and Subcommittee on Intergovernmental Affairs Hearing on Cybersecurity of Voting Machines. On file.

<sup>4</sup> Alex Padilla, Secretary of State, California. April 5, 2018. Testimony to Senate Budget Subcommittee #4. <https://www.senate.ca.gov/media-archive/default?title=&startdate=04/04/2018&enddate=04/05/2018>.

<sup>5</sup> Kammi Foote, Clerk-Recorder, County of Inyo. July 26, 2018. Sacramento, CA. Testimony to the Commission.

<sup>6</sup> Pam Fessler. October 26, 2016. "Some Machine are Flipping Votes, But That Doesn't Mean They're Rigged." *National Public Radio*. <https://www.npr.org/2016/10/26/499450796/some-machines-are-flipping-votes-but-that-doesnt-mean-theyre-rigged>. Accessed August 21, 2018.

<sup>7</sup> Kate Rabinowitz. February 17, 2018. "Assessing the Vulnerable State of America's Voting Machines." *Pacific Standard*. <https://psmag.com/news/our-voting-machines-are-getting-old>. Accessed August 28, 2018.

<sup>8</sup> Bryan Menegus. November 6, 2018. "Voting Machine Hell, 2018: A Running List of Election Glitches, Malfunctions, and Screwups." *Gizmodo*. <https://gizmodo.com/voting-machine-hell-2018-a-running-list-of-election-g-1830261900>. Accessed November 7, 2018.

<sup>9</sup> Padilla. See endnote 4.

<sup>10</sup> Legislative Analyst's Office. March 2017. "The 2017-18 Budget: Considering the State's Role in Elections." Page 6. <http://www.lao.ca.gov/reports/2017/3634/state-role-elections-033017.pdf>. Accessed June 15, 2018.

<sup>11</sup> U.S. Election Assistance Commission. "HAVA Funds: State Chart View." <https://www.eac.gov/payments-and-grants/hava-funds-state-chart-view/>. Accessed June 15, 2018.

<sup>12</sup> SB 840. Mitchell. Budget Act of 2018-19. [http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill\\_id=201720180SB840](http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB840).

<sup>13</sup> Kammi Foote, Clerk-Recorder, County of Inyo. July 26, 2018. Written testimony to the Commission.

<sup>14</sup> Pam Smith, Senior Advisor, Verified Voting. July 26, 2018. Written testimony to the Commission.

<sup>15</sup> California Elections Code. Division 4, Chapter 1. Also, California Elections Code. Division 14. Also, California Elections Code. Division 17. Chapter 4. Sections 17301 and 17302 .

<sup>16</sup> Menegus. See endnote 8.

<sup>17</sup> Philip Stark, Associate Dean, Mathematical and Physical Sciences and Professor, Department of Statistics, University of California, Berkeley. July 26, 2018. Written testimony to the Commission. Also, E. John Sebes, Chief Technology Officer, Open Source Election Technology (OSET) Institute. Sacramento, CA. July 26, 2018. Testimony to the Commission.

<sup>18</sup> Framework available in Philip Stark's testimony from the July 26, 2018 hearing. <https://lhc.ca.gov/report/voting-equipment-security>.

<sup>19</sup> Joseph Lorenzo Hall. February 11, 2009. "Improving the Security, Transparency and Efficiency of California's 1% Manual Tally Procedures." USENIX/ACCURATE Electronic Voting Technology Workshop 2009. [https://www.usenix.org/legacy/event/evt08/tech/full\\_papers/hall/hall\\_html/](https://www.usenix.org/legacy/event/evt08/tech/full_papers/hall/hall_html/). Accessed September 14, 2018.

<sup>20</sup> California Elections Code Division 15. Chapter 4. Article 5.

<sup>21</sup> Stark. See endnote 17.

<sup>22</sup> California Secretary of State. Statewide Recounts – Frequently Asked Questions.

<https://www.sos.ca.gov/elections/statewide-recounts/statewide-recounts-faq/>. Accessed December 20, 2018.

<sup>23</sup> Mark Lindeman and Philip B. Stark. March 2012. "A Gentle Introduction to Risk Limiting Audits." *IEEE Security and Privacy*, Special Issue on Electronic Voting. Page 1.

<https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf>. Accessed January 29, 2019.

- 
- <sup>24</sup> Dwight Shellman, County Support Manager, Elections Division, Colorado Department of State. June 15, 2015. "Risk-Limiting Audits in Colorado." Presentation to the National Conference of State Legislatures conference: The Future of Elections. [http://www.ncsl.org/Portals/1/Documents/Elections/RLA\\_20170615.pdf](http://www.ncsl.org/Portals/1/Documents/Elections/RLA_20170615.pdf). Accessed September 19, 2018.
- <sup>25</sup> Lindeman and Stark. See endnote 23.
- <sup>26</sup> Lindeman and Stark. See endnote 23.
- <sup>27</sup> Lindeman and Stark. See endnote 23.
- <sup>28</sup> Senate Rules Committee. August 23, 2018. Senate Floor Analysis AB 2125. [http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill\\_id=201720180AB2125](http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB2125).
- <sup>29</sup> Foote. See endnote 5.
- <sup>30</sup> California Secretary of State. October 2014. California Voting System Standards. <http://elections.cdn.sos.ca.gov/pdfs/california-voting-system-standards.pdf>. Accessed September 3, 2018.
- <sup>31</sup> Foote. See endnote 5.
- <sup>32</sup> E. John Sebes, Chief Technology Officer, Open Source Election Technology (OSET) Institute. July 26, 2018. Written testimony to the Commission.
- <sup>33</sup> Philip Stark, Associate Dean, Mathematical and Physical Sciences and Professor, Department of Statistics, University of California, Berkeley; E. John Sebes, Chief Technology Officer, Open Source Election Technology (OSET) Institute; Kammi Foote, Clerk-Recorder, County of Inyo; and Kenneth Bennett, Program Manager, Voting Solutions for All People (VSAP), Los Angeles County Registrar-Recorder/County Clerk. July 26, 2018. Sacramento, CA. Testimony to the Commission.