Testimony Submitted to the Little Hoover Commission
Hearing Date: July 26, 2018

Pamela W. Smith, Verified Voting
Voting System Security

Honorable Members of the Commission: I serve as Senior Advisor to Verified Voting, a national non-partisan non-profit educational and advocacy organization committed to safeguarding elections in the digital age. Verified Voting advocates for the responsible use of emerging technologies to ensure that Americans can be confident their votes will be cast as intended and counted as cast. We promote auditable, accessible and resilient voting for all eligible citizens. I previously served as President of Verified Voting for more than a decade. I have provided information and testimony on voting technology and policy issues at federal and state levels, including to the US House of Representatives Committee on House Administration, and earlier this year at the Joint Hearing of Assembly Elections and Redistricting and Senate Elections and Constitutional Amendments Committees, on Cyber-security and California's Elections[1].

I have curated an extensive information resource on election equipment and regulations nationwide, and co-authored several key works on election security policy, including Principles & Best Practices for Post Election Audits[2] and the introductory chapter of Confirming Elections: Creating Confidence and Integrity through Election Auditing[3]. I participate in the Future of California Elections, a collaboration between election officials, civil rights organizations and election reform advocates to examine and address the unique challenges facing the State of California's election system[4]. I also serve on the Los Angeles County Voting Systems for All People (VSAP) Technical Advisory Committee[5].

In my capacity at Verified Voting I have worked with advocates, election officials and lawmakers from all across the country. In my view, the states that do the best on metrics relating to voting system security are often the ones that continue to look for and embrace opportunities to improve. As security threats do not stand still, neither can those whose work it is to safeguard our elections and consequently our democracy. I applaud the Little Hoover Commission for taking up this crucial topic of investigation, and am pleased to participate in and contribute to that effort.

Election security is not an on-off switch, where a thing either is secure or it is not. Rather it involves incrementing layers of effort, analysis, systems and procedures, all created or conducted by people, all while balancing costs and priorities. Such incremental measures

[1] March 7, 2018. https://selc.senate.ca.gov/content/oversightinformational-hearings

[2] Electionaudits.org/principles

[3] Palgrave/MacMillan, 2012.

[4] Futureofcaelections.org

[5] Vsap.lavote.net

harden a system, making it more secure than before and solving for problems when they occur. Perfect security is not attainable, but diligence in the pursuit of secure elections is.

As hard as we try, there will always be another vulnerability discovered; this should not discourage our effort. We should take those steps, and not make it easy for tampering to occur, even while recognizing that there's no such thing as a completely tamperproof system. Instead, our focus should be on reducing and mitigating for vulnerabilities, and on recoverability, such that no matter what happens, we can say to the public "We take these steps to ensure all will be able to have confidence in the accuracy of the outcome and that everyone who wanted to participate was able to do so."

Voters need to know elections are working the way they should, or they won't have the confidence to participate. Ensuring voters know we are taking all possible steps to secure the vote is a way to remove the obstacle of "lack of confidence" and we do this to protect and support all the other things we do to make it possible for every eligible person to vote.

This work cannot be the responsibility of elections officials alone; lawmakers must also support this effort by finding ways to ensure those hard-working officials have the resources they need to meet both the demands of running elections generally, and the special requirements of addressing today's intense security threat environment and meeting the inevitable issues that arise with resilience.

1. Define security as it relates to voting equipment.

Good elections require technology to be *available* and *functioning correctly* and *reliably*; secure elections require us to be able to <u>prove</u> that this was the case.

It can be useful to look at security issues through the filter of how they will affect the ability of voters to cast an effective ballot. In this context, "effective" means that:

- the voter is not derailed in their quest to vote by a failed electronic poll book, or tampered registration list;
- the ballot is *available* to the voter (including any system to be used for marking the ballot);
- the voter receives the *correct* ballot, that it is presented *complete*;
- it is feasible to *mark, check/verify and cast* the ballot safely, and privately;
- the ballot is *counted correctly*, along with all the other ballots; and
- we can *demonstrate* that fact to the satisfaction of the public, including those on the side of the losing candidate or issue.

For election system security, prevention and detection of tampering is obviously important. For secure election outcomes and ensuring that all voters who show up can cast an effective ballot, even more critical is the <u>ability to recover, both real time and after the fact</u>. This means that even in the face of a voter registration breach that we were unable to prevent, even if there were undetected tampering in your voting system software, even if

some systems failed or were caused to fail on Election Day, people can vote and votes are counted correctly.

Equipment for *voting* is but one part of a broad array of election technology infrastructure that supports the conduct of elections today. Technology touches the voter and the vote at various stages of the electoral process, from getting information to registering to checking in to vote, to marking, casting, counting and reporting votes. Election systems therefore include not only the systems we use for marking our ballots and for tallying the votes, but also the systems we use for registering to vote or updating our registration, the systems that election officials use to set up the many ballot styles with the correct candidate names and ballot measures and languages and so on. Other systems include electronic poll-books and ballot on demand systems, which must be able to find the right information for the voter and produce the right ballot, and even networks on which election officials provide information to voters and/or election night reporting.

To the extent that any of these can be compromised or manipulated, can contain errors, or can fail to operate correctly—or at all—this can potentially affect the vote. So election system security requires not only working to prevent breaches and malfunctions, but also fail-safes that address breaches and malfunctions that do occur. Cyber security experts agree that security breaches are not a matter of "if" but "when." Assuming such problems will occur, fail-safes must be in place.

For technology used for marking and counting votes, voters must be able to confirm first-hand their ballots were indeed marked as they intended, and election officials must be able to use those ballots to demonstrate that all the votes were included and were counted as cast.

This bridge between the voter and correctly reported outcomes requires a physical artifact as evidence of the voter's intent, and a process for checking. That artifact is typically the paper ballot the voter marked, either manually or through the use of an accessible interface such as a ballot marking device; alternatively it may be the voter-verified paper audit trail (VVPAT) produced by a direct recording electronic voting machine. It can also be the printout that gets mailed in when a voter uses a remote accessible ballot marking method from home. Whatever the physical record, it must have been available to the voter for his or her review prior to casting in order to serve as a record of voter intent.

Not all voters will take the opportunity to review their ballot, and there is no requirement to do so, but the ballot they had the opportunity to review is the <u>only</u> record that can be construed to represent their intent. Although voting systems have other ways to produce physical records like print-outs of what are called ballot images or printouts of cast vote records from voting or vote counting machines after the fact, if the voter did not have the opportunity to review that printed record, it cannot serve as a record of voter intent.

While a voter can review choices on an electronic screen, unlike the physical artifact the electronic version is not independent of software that enables marking, casting or counting of ballots, and of the software that may –possibly incorrectly—render an image of the

physical ballot. This property of software independence[6] is crucial for checking the correct functioning of the software. Given that either an attack on the electronic system's software or a malfunction in that same system can produce an incorrect rendering of an individual ballot's contents or of the overall results, the ability to make a separate and independent check that the voters' intent was captured correctly is crucial for security.

The process for checking the functioning of the software is the post-election audit. In a good audit, a sufficient portion of voter-verified paper ballots will be checked to ensure the voting system correctly captured their intent. This process does not stand alone. Other compliance procedures ensure that all ballots are accounted for and the numbers of ballots cast reconciles with the number of voters who signed in, and that important chain of custody security procedures have been followed each election. Put together, these practices create a trustworthy record that enables us to confirm or correct our election outcomes.

One common concern is whether voting systems are connected to the Internet, a common avenue for hacking intrusion or transmittal of malware. California's voting system requirements prohibit connection to the Internet. This safety measure reduces the "attack surface" available to those who would tamper, to mitigate for remote attacks on live voting and for other purposes. However, experts note that even systems not directly connected to the Internet are "vulnerable to viruses and malware spread through portable memory devices. Furthermore, sophisticated software attacks can be designed to be inactive and undetectable during pre-election testing"[7] of voting systems, a process every county undertakes for each election.

Pre-election testing *is* important for several purposes, including confirming that the ballot styles are complete and correct, and voting systems are functioning as they are being prepared for deployment to polling places, and so on. To that extent, it is necessary for supporting secure practices in elections, though not sufficient on its own to confirm outcomes.

Similarly, the battery of tests conducted during the process of voting system certification provides useful information about the correct functioning of a voting system and its components—at the time it is tested. Once a system is in the field, however, it cannot be assumed to be in the same state that it was upon certification. Software and election configurations have been uploaded and potentially modifications have occurred. Further, it should be noted that each voting system that was found to have vulnerabilities in the past was tested and certified in some measure. The only way to ensure it performed correctly in

---

[6] Software independence in voting systems was described by Ron Rivest (MIT) and John Wack (NIST) as follows: "*A voting system is software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome*," in their 2006 paper "On The Notion of Software Independence in Voting Systems." https://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf

[7] Voting Machine Security Toolkit, June 2018, The Brennan Center for Justice, Common Cause, National Election Defense Coalition and Verified Voting. https://www.verifiedvoting.org/wp-content/uploads/2018/06/Securing-the-Nation-s-Voting-Machines-A-Toolkit-for-Advocates-and-Election-Officials.pdf

the field in a real election is to check the outcome after the fact, using sufficient records of voter intent in a robust audit.

For voter registration systems and the networked systems that support the voter lists during the election, a fail-safe would be a system that enables election officials and voters to be able to check their electronic registration record to ensure their name is included and a means to resolve the record if it was not, so that a voter is not prevented from participating even if something went wrong with the registration system just prior to the election, or the electronic poll roster of voters, or the like. Election officials must have a working copy of the voter list that is completely separate from a protected, off-line "original" master list, so the master is never at risk.

2. Please provide an overview of how the nature of perceived security threats against voting systems has changed over the past decade. Is CA prepared for its Secretary of State's office and county election officials to be the front line against attacks from foreign actors?

Savvy election officials everywhere – from county level to state level – have always taken election security seriously, but after breaches of voter-registration sites were initially reported in mid-2016 the subject has risen to a top-level priority nationally. At many conferences for state and local election officials, security now is a topic of keynotes and workshops, efforts led by some of California's own election officials.

At the federal level, the number of Congressional hearings related to election security is in the double digits since mid-2016, more than in the past ten years combined. The Department of Homeland Security declared election infrastructure as part of "critical infrastructure" and now provides tools and services to county and state level elections offices on request. Earlier this year the sum of $380 million was allocated in federal appropriations for states to spend on improving election security, including for replacement of paperless voting systems with systems like California's that provide a voter-verified paper record, upgrading election-related computer systems to address vulnerabilities, provide cyber security training and best practices implementation, and for conducting post-election audits.[8] California's share of those funds requested by Secretary of State Padilla is nearly $34.6 million.

Is California prepared in its front line against nation-state adversaries? California is more prepared than some states, and has been taking security seriously for some time. In 2004 California took steps to ensure that all our elections require the use of a voter-verifiable paper ballot or VVPAT for most voting.[9] Since 1965, when California first started using

[8] https://www.eac.gov/2018-hava-election-security-funds/#how-can-states-use-the-funds

[9] An exception is the use of electronic return of voted ballots via fax, for military and overseas voters. Fax transmissions no longer mean dedicated phone lines and specific-use equipment but instead can be transmitted via the Internet, or via a conversion to email, methods not contemplated at the time of the provision's passage and which present additional security vulnerabilities. A ballot transmitted through this method becomes an electronic file vulnerable to tampering and alteration, and may or may not represent the intent of the voter when it is received in the elections office.

electronic methods for scanning and counting votes, we have had a requirement in place for a basic manual tally audit conducted by every county after every election[10]. We subsequently tested more robust methods known as risk-limiting audits through a pilot program passed by the legislature in 2010[11], and a bill is currently under consideration in California's legislature relating to the conduct of risk-limiting audits[12].

The state has led the nation in its significant efforts to examine voting system security more closely, including but not limited to efforts such as the 2007 *Top to Bottom Review of Voting Systems*[13]; initiating the regular practice of volume testing of voting systems under conditions that simulate a high-volume election, of voting systems submitted for certification; and the passage of a more stringent set of requirements for voting system testing and certification[14] at a time when the Federal body for setting testing standards was (temporarily) moribund. California also certifies ballot-on-demand printers and remote accessible vote by mail systems. These are important steps to ensure such systems meet basic functional requirements.

Work remains to be done to support the preparedness of the state and its county election offices in their shifting role on the cyber security front lines, however. The state does not yet require audits robust enough to strictly limit the risk of confirming an incorrect outcome. Manual recounts of specific contests are available upon request, but even if it falls to a candidate or her supporters to ensure a particular outcome was correct, doing so may prove cost prohibitive, and omits confirmation of other contests on the ballot.

California is one of a few states requiring certification of electronic poll book (EPB) systems. The state recently promulgated a set of regulations for testing EPB systems; we felt these were insufficiently stringent and not altogether clear. We submitted comments highlighting areas for improvement, though few changes were made. These requirements should be strengthened, in light of EPBs' potential to impact the ability of a voter to cast an effective ballot, so that counties seeking to buy such systems are supported in their efforts at diligence in securing elections.

Some counties have substantially greater resources than others, but all counties need security resources. Secretary of State Padilla's calls for funding for more up to date equipment and for cyber security efforts were supported in recent appropriations[15]. The Secretary has moved forward with the establishment of an Office of Elections Cybersecurity (OEC), which would coordinate information sharing between federal, state and county officials to address reducing the likelihood and severity of cyber incidents that could

---

[10] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=15360.&lawCode=ELEC

[11] https://codes.findlaw.com/ca/elections-code/elec-sect-15560.html

[12] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB2125

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

[14] Senate Bill 360, Padilla, Certification of Voting Systems, passed in 2013: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB360

[15] http://www.sos.ca.gov/administration/news-releases-and-advisories/2018-news-releases-and-advisories/ca-budget-invests-134-million-new-voting-systems-3-million-strengthen-election-cybersecurity/

threaten the state's elections. Ensuring that such an entity aids election officials and their staff in understanding cyber hygiene and best practices in cyber security will strengthen the state's preparedness.

3. Please provide a high level introduction to general security threats to voting equipment that election officials face in the process of voter registration, at the polling place on Election Day and in counting and reporting election results.

Election officials are faced with efforts by attackers to breach their registration systems, websites and networks through a variety of means. These can include direct web-based attacks that seek to inject or send commands to enable the attacker to gain unauthorized access to information; denial of service (DoS) attacks that prevent legitimate users from being able to use election information or services; ransomware attacks that block legitimate users' access to a system until a ransom is paid; and more. Phishing attacks involve forged emails or other messages designed to get the recipient to click on malicious links or otherwise provide an entry point for stealing credentials such as passwords, spread malware or disrupt voting operations. Foreign adversaries successfully used some of these methods in 2016.

Security practices prevent most, but not all, such attacks from being successful. These include keeping applications and operating systems patched with the latest updates; whitelisting, or making sure only specified programs are allowed to run while blocking all others; restricting administrative privileges to help limit the spread of malware; and ensuring appropriate firewalls are in place and properly configured. While these methods can block up to 85% of targeted attacks, the Department of Homeland Security recommends additional steps[16] for protecting voter registration systems from harm and ensuring continuity of operations, including penetration testing, vulnerability scanning and patching, development of an incident response plan, and staff training on cyber security best practices.

Election officials also must securely store, maintain, prepare and test their voting systems in preparation for each election, ensuring that unauthorized access is prevented and security protocols are followed for uploading new ballot definitions and preparing systems for deployment. Once deployed to a polling place, poll workers oversee physical security of the voting system until the system is returned to the county office. Both poll workers and elections staff must manage the secure chain of custody of election materials, including voted ballots and signed rosters. Threats to voting systems can include insider tampering via injection of malware through a tampered memory device or other communication method, tampering or damage to a voting system en route to or at a polling location which could result in "denial of service" if the voting system is not functioning, or altered results.

Election officials initiate counting of voted ballots on Election Day, with vote by mail ballots counted at the county's election facility and, depending on the type of voting system used, polling place ballots counted in the local polling place once voting has finished. Threats to

[16] https://www.dhs.gov/sites/default/files/publications/Securing%20Voter%20Registration%20Data_0.pdf

central count tally systems are similar to those for polling place voting systems, except that such centrally located systems are accessed by significantly fewer people. Election night reporting methods could involve risks if systems for communicating results were breached. Although incorrect or tampered reports can be corrected, because of intense public interest and scrutiny such reports can lead to significant public concern.

3a. *Does the new vote center model provided through the 2016 Voter Choice Act create opportunities for new security threats?*

The 2016 Voter Choice Act, or VCA, requires participating counties to establish vote centers, similar to precinct-based polling places but serving voters from the entire county rather than just from within a local area. In order to meet the needs of voters from anywhere within the county's borders, a vote center must be able to ascertain the voter's status and provide the correct ballot for the voter, out of a large number of ballot styles (which vary based on the voter's geographic area). Doing so means deployment of some potentially new equipment, including ballot-on-demand printing systems and electronic poll books or other means of access to the county's voter registration data.

Further, voters can now be registered to vote on the same day they arrive at a vote center in participating counties, even if they missed the pre-election deadline. This process of "conditional voter registration" also requires a means of connecting with the county's voter registration system. As San Mateo County described it in their VCA election administration plan[17]: "At each Vote Center, a network of computers will be linked to the County's Election Management System (EMS) through a secure VPN connection."

Any networked connection to a county's voter registration election management system[18] raises potential security concerns. VPNs can solve some issues, but vulnerabilities continue to be uncovered. Electronic voter registration management systems have been targeted[19] as was apparently a service provider of electronic poll book systems[20] that does business in several states including California.

One other new requirement that arose in part from the passage of the Voter Choice Act but which will apply to all counties is the use of remote accessible vote by mail systems to serve voters with disabilities who vote by mail.

4. Please explain for the Commission what attackers are trying to accomplish when targeting voting equipment. Are they always trying to alter the outcome of an election or do they sometimes have other goals?

---

[17] https://www.smcacre.org/sites/main/files/file-attachments/acre-electionadministrationplan_web.pdf

[18] In this instance, "EMS" does not refer to the system for managing the voting machines and ballot layout but rather the voter registration system and files.

[19] http://www.chicagotribune.com/news/local/politics/ct-met-illinois-elections-board-russia-indictment-20180713-story.html

[20] https://theintercept.com/2018/07/13/a-swing-state-election-vendor-repeatedly-denied-being-hacked-by-russians-new-mueller-indictment-says-otherwise/

It has been said that elections must not just show who won, but indeed must prove to the losers and their supporters that they lost legitimately. Today voters, election officials and elected officials alike are keenly aware that we face attacks on our democracy and the systems that support it. Voters need confidence in those systems, to encourage full participation. Doubts about the outcome of an election can be corrosive to voter confidence.

Disruption of elections can take many forms. Voting systems may be targeted. Systems that cannot be audited, or that are not robustly audited, are particularly vulnerable because tampering may not be apparent without a systematic review. Auditable systems and robust audits strongly mitigate the effects of such attacks, and correlate to a positive effect on voter confidence.[21]

One expert recently noted that the threat model usually considered by those outside the cyber security world is that a corrupt or dishonest candidate would attack an election in order to prevail, but that this threat model is outdated. If the goal instead (or in addition) the goal is to sow chaos by generating uncertainty, this opens new threats.[22]

An attacker may seek to disrupt an election to generate uncertainty about the results. Election night reporting systems may be targeted. Even if voting systems counted the votes correctly, an attacker could seek to *alter posted results* or *interrupt the reporting* of results, without affecting actual vote totals or counting equipment. Ensuring the public understands that preliminary results are just that—preliminary and not final—and that there are checks to ensure the accuracy of the final count are important tasks, but not necessarily easy to do.

Attackers also may seek to *interrupt the voting process*, even targeting specific communities in order to skew the outcome, without affecting voting or vote counting machines. This could happen when electronic poll books in certain parts of a jurisdiction—perhaps parts that skew more heavily to one party than to others—fail to boot up or are caused to slow down or stop working. Mitigations exist, but can take valuable time to deploy.

5. Given the increasingly sophisticated security threats to which voting and vote counting are subjected, please explain why we should use technology at all. Why not simply require all voting not requiring accessibility assistance to be conducted on paper with 100% manual counts?

Manual counts of voted ballots were used in the past, but decreased over the years to now a very tiny percentage of the nation's overall ballot counting. For expedient initial election results, many would contend we cannot wait, so this practice is mostly confined to

---

[21] "Confidence in the Electoral System: Why We Do Auditing," with Fred Conrad. 2012. Chapter 3 in R. Michael Alvarez, Lonna Rae Atkeson, and Thad E. Hall (Editors), Confirming Elections: Creating Confidence and Integrity through Election Auditing. New York: Palgrave Macmillan.

[22] https://www.whitehouse.gov/sites/whitehouse.gov/files/docs/pacei-harri-hursti-presentation.pdf

jurisdictions that are small and where the ballots are brief enough that they can indeed provide results in a timely enough fashion to satisfy their public.

Although some jurisdictions do conduct hand counts of paper ballots, the practicality and benefits of doing so would need to be weighed against the costs factoring in the length of the ballot, the number of ballots cast and the resources of the county.

We can take advantage of the benefits to transparency and security of a manual review of the voted ballots without having to count all of the ballots. Counting a portion of the ballots – using appropriate selection methods – can ensure that the speed of a near-immediate result on election night does not sacrifice the security provided by the careful direct review of a post-election audit, to confirm the voters' intent.

6. Please share your assessment of what California is doing right with respect to voting security. What steps can state officials take to improve voting security?

As described above, California has long been a leader on improving security for election systems. The state has a relatively strong testing and certification program for voting systems that includes penetration testing and operational testing of voting systems under both normal and abnormal conditions, though as mentioned above there are some weaknesses in the requirements for electronic poll book systems. California requires all voting systems to use or produce a voter-verified paper ballot or record and conducts a manual tally of all contests on the ballot after every election. Though the manual tally is not robust enough to confirm electoral outcomes in most cases, the state has a track record of reaching toward more robust risk-limiting audits.

- We recommend that California commit to further development of risk limiting audits (beyond the currently pending bill which is time-delimited and opt-in only), and fund that development so that it is possible to conduct true statewide confirmation of election outcomes.
- We further recommend that California strengthen its requirements for electronic poll book testing.

California has seen some excellent examples of collaboration between officials and experts in auditing, accessibility and usability, and voting system security at both county and state levels. County-level examples of engaging experts to provide input on voting system requirements for security include the Los Angeles VSAP Technical Advisory Committee and the San Francisco Open Source Voting System Technical Advisory Committee[23]. Past state efforts have included the Top to Bottom Review of Voting Systems, Voting System Accessibility Study, Post-Election Audit Study Working Group, and the Risk Limiting Audit Pilot Study funded by the Election Assistance Commission. We hope that the newly established Office of Elections Cybersecurity will continue that collaborative tradition.

[23] https://osvtac.github.io/members#member-bios

- We recommend that the state continue to engage with technology experts; we have a wealth of scientists in the state that have already done substantial work relating to voting system security.

California recently has found ways to smooth the path for development of new systems that are both non-proprietary and voter-centric, including through enabling legislation such as SB 360 that changed how we test and certify systems for adoption, and through provision of funding for nonproprietary systems[24]. Open source systems still require the essential safeguards of a paper ballot and robust post-election audits, but as such systems are successfully developed and deployed, they can provide substantial cost-savings to counties, freeing resources for ongoing security improvements.

- We recommend that California continue to support the development of nonproprietary systems that meet or exceed current security guidelines.
- We further recommend that the state ensure it fulfills its funding commitments to the county elections offices.

Pursuant to statute, no part of a voting system can be connected to the Internet at any time, nor receive or transmit election data through an exterior communication network of any time. Aside from the carve-out for the electronic (fax) return of voted ballots, this remains a powerful safeguard that significantly reduces the threat surface to voting systems.

- Given the current threat environment, we recommend that California ensure this prohibition on Internet connections remains in place for the foreseeable future, and that the state reduce or eliminate the electronic transmission of voted ballots, while working to ensure that military and overseas voters are able to vote securely.

We appreciate the opportunity to participate in the important work of the Little Hoover Commission and are available to respond to any questions on this topic at any time.

[24] http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB1824