Changes Ahead:

A Look At Voting System Testing and Certification

Pamela Smith
Verified Voting Foundation

June 2013

Table of Contents

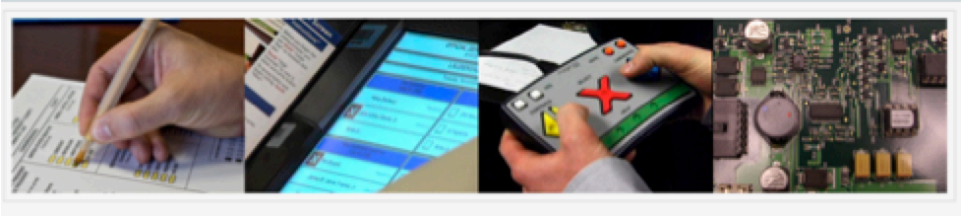
Introduction

Voting is fundamental to who we are as citizens, a right to express our views that we may take for granted, whether or not we exercise it each election. But however engaged we may be in the political issues or processes of the day, most of us think about the *mechanics* of how we cast our votes very rarely if at all. Most simply assume that our voting infrastructure will work and work correctly, that ballots will be available and equipment will function when we go to the polls and when the votes are being counted. And many may assume there is one centralized federal system to govern how voting equipment is tested and qualified for use. In fact there is a patchwork of 51 different sets of rules and policies, which govern how those systems are approved for use on Election Day. Though each state has its own requirements, many similarities exist.

This informal report provides a look inside that framework for voting system testing and certification in the states and the nation, and explores how California's current process fits into that framework. What do states do to approve a voting system? How do they do it? Who does it? What works well? It also examines potential changes to the framework: what processes or steps are not done but perhaps should be, to better ensure the security and usability of voting systems?

This is not intended to be a comprehensive statutory or regulatory review. Instead, examples of key elements of how technology is tested are included to further inform our understanding of voting system certification – even from outside of the voting machine realm. Included also are key recommendations and challenges that remain to be resolved.

In preparing this report, Verified Voting interviewed individuals from federal, state and local jurisdiction agencies involved in testing, certification or related matters, as well as researchers and policy analysts who have examined the subject matter. We also gleaned insights from conferences on voting system testing and certification at both state and federal levels. We are grateful to all for their willingness to share their extensive knowledge on the topic. In particular we would like to thank the Future of California Elections project team, and most especially the Irvine Foundation, without whose support this project would not have been possible.



What is Voting System Testing, Certification, or Approval?

Voting systems generally undergo testing of various kinds prior to their permitted use in real elections by actual voters. In most states, the county election official decides what voting system to obtain and use, but they may be required to select from systems that have undergone a **state** approval process, a **federal** approval process, or **both**. Testing of the voting system usually precedes the approval process, or certification, and afterward even more testing is done.

1. First, **testing may be conducted by the manufacturer** or vendor that developed the product. For example, vendor testing of voting systems for accessibility is called for in current federal guidelines; the vendor is expected to document that testing.

2. Some vendors submit their voting systems to a battery of **tests conducted by the federal entity** tasked with that responsibility, the Election Assistance Commission (EAC), according to an approved set of standards, through accredited testing laboratories. They do so because some states require such testing and/or **EAC Certification** prior to consideration of that system's use in their state. The next section details federal testing.

3. Voting systems are also **tested by states**, often for **state level certification** or approval, prior to their use in some states, though this is not required by all states. Many states, like California, use more than one type of voting system, and have voting systems at varying stages of their expected life cycle. Sometimes changes to voting systems become necessary, without replacing the entire system, to meet changing statutory requirements or to replace an obsolete or faulty component. These **changes are tested** also.

4. Voting systems undergo **acceptance testing** when delivered, either by the state or local jurisdiction or both. There are **periodic examinations** to ensure the correct (approved) software version or operating system is installed in voting systems in the field, usually conducted by the state, sometimes with EAC collaboration. In some states, California included, the chief state election official or board may require a **review of fielded voting systems** from time to time. Such evaluations may be extensive, involving **penetration testing** or open-ended vulnerability testing and **review of the source code** such as occurred in the landmark 2007 Top to Bottom Review of voting systems in CA[1].

5. Voting systems are also tested for "**logic and accuracy**" before each election in varying degrees. This is done on systems configured for the upcoming election to ensure correct and complete ballot proofing, proper calibration, functioning of accessible features, such as audio interfaces, and so on. It is carried out at the local jurisdiction level or by the state for the local jurisdiction where the voting system is used.

6. Voting systems can undergo **parallel monitoring**, a test conducted on Election Day simulating real election conditions, on randomly selected pieces of equipment. This test examines performance of equipment in election mode rather than in test mode. California's statute calls for this procedure under certain conditions (see note).[2]

7. Voting systems can be subject to a **post-election reprise of the pre-election L&A test**. This is often conducted prior to recounts, usually by the local election official.

8. Last but not at all least, voting systems can be tested by carrying out a manual **post-election audit** which may check vote tabulation, the election outcome, and/or the functioning of specific machines, depending on how it is conducted.

So, while they are many, are these tests sufficient to ensure security and reliability of the vote? The breadth and comprehensiveness of testing varies to extremes around the country. That means some voters will vote on robustly tested equipment and some vote on systems that have had very little testing, a disparity that can have an impact on when and whether systems fail or malfunction – before, during or after Election Day.

The considerable value of robust audits for ascertaining correct outcomes goes well beyond what voting system testing and certification can do. While testing done before the election can help ascertain that equipment is designed, manufactured and installed properly, it cannot guarantee the equipment will function correctly on Election Day. A system could pass the requirements test and yet produce an incorrect outcome in the election. However, strong election audits of the ballots can check the correctness of the results from voting systems in actual use on Election Day (even if the system was not tested or certified at all).

To ensure the accuracy of the election outcome, **audits are a necessary component** in addition to testing for functionality and requirements. Audits can identify failures or flaws that might otherwise have gone unnoticed. A **feedback loop** to identify and make public any problem or issues identified in the voting system will enable better systems, not just in the jurisdiction that noted the issue, but also in any other jurisdiction using the voting system. While no voting system is perfect, a **continuous process of improvement** by examining the election and making adjustments for the future makes for better elections, and fewer disenfranchised voters. California continues to lead in identifying better methods for strong post-election ballot audits.[3]

In her Policy Brief examining "Modernizing California's Voting Technology: A look back, a look forward"[4] Kim Alexander of California Voter Foundation asks the key question:

> *What changes, if any, could be made to the state's voting system approval process to improve opportunities for innovation in California's voting systems?*

The following material seeks to assist in better understanding what California currently does—in the context of what the federal government does, and what other states do; what changes might be possible or desirable, if any; and to identify what challenges remain to be resolved in the voting system approval framework broadly.

FEDERAL TESTING AND CERTIFICATION

EAC Voting System Testing and Certification Program

The Help America Vote Act (HAVA) of 2002 called for the formation of the US Election Assistance Commission (EAC), and mandated that the EAC accredit voting system test laboratories and certify[5] voting equipment, the first time the federal government has offered these services to the states. The EAC made its certification program operational in 2007, and certified its first system in 2009.[6]

Before the EAC's Voting System Testing & Certification program existed, the Federal Election Commission (FEC) took responsibility for promulgating voluntary standards, but there was no government agency tasked with supervising voting system testing to those standards. To fill this void, the National Association of State Elections Directors (NASED) oversaw a process of qualification of voting systems as having met the voluntary standards developed by the FEC. A private entity, NASED did not release test plans nor test reports, and the process lacked transparency. When the EAC assumed responsibility, it:

- developed voluntary voting system guidelines replacing those earlier standards,
- developed testing manuals and protocols, and
- required laboratories that wish to test voting systems to meet certain requirements for accreditation.

The guidelines or standards against which voting systems are tested are referred to as the "**voluntary voting system guidelines**" (**VVSG**). The VVSG were developed by the EAC with its Technical Guidelines Development Committee (TGDC) and technical input from the National Institutes for Standards and Technology (NIST).

To receive EAC certification, a voting system must be tested by an EAC accredited testing laboratory and must meet the requirements of the guidelines. **But the federal guidelines are not mandatory on the states; the states determine whether or not to adhere to the guidelines and in what manner** when obtaining voting systems for use in the state.

This means some voting systems we use around the country are certified as having met the VVSG, and some – *most* – are not certified by the EAC. Many were certified to guidelines approved more than a decade ago, not by any federal body, but rather by NASED.

Supplemental Programs: Quality Monitoring and Clearinghouse of Reports

The EAC operates a "**Quality Monitoring Program**" designed to "ensure that voting systems certified by EAC are the same systems sold by manufacturers."[7] Participation is mandatory for systems certified by the EAC. This is to prevent problems that have occurred on a number of occasions where voting system components or software have been swapped out for untested, uncertified versions in the states.

States also do their own checking to ensure the correct version of software is being used, and that the "hashes" of the software match. In California, Indiana and elsewhere, fines have been levied in the past against vendors for installing uncertified software modifications (which seems to have resulted in improvements).

> *"Ohio recently conducted an audit of fielded systems in each county, checking that the software was the same as certified, but also that the operating systems and security set up were in the certified state. Every piece of software checked hashed against the certified hash was correct. For operating systems set up, there were more mixed results. Password requirements were not always stringently followed by the county, for example. A roving technician went to each county to ensure correct set up to remedy the inconsistency, and we were able to focus on training about secure practices for things like passwords – it turned out to be a valuable process. We now have a baseline."*[8]

The EAC also maintains a **Clearinghouse**[9] of reports submitted to it by states. Six states so far have submitted reports: CA, CT, KY, MI, NY and OH. These reports document some of the most comprehensive reviews of voting system vulnerabilities conducted to date, including California Secretary of State Bowen's 2007 Top To Bottom Review, and the 2008 Ohio EVEREST report. ***Those vulnerabilities were not found in previous certification tests, underscoring the limitations of testing only to standards***.

Benefits and Challenges of Federal Voting System Certification

The existence of a federal testing and certification program enables states to know that the voting system with a federal certification has met certain requirements before arriving at their portal for state testing, acceptance or deployment. But the program's existence has impact beyond only the states that choose to require federally tested systems:

- The EAC program has made the process more **rigorous** than in the past, including with the requirements that testing laboratories must be inspected and meet conditions to be accredited. This means that states using the VSTLs for their own testing requirements – even if they do not require federal testing by the VSTLs – will benefit from using testing labs that have been approved to test systems for the EAC.

- Buying certified voting systems is not limited just to states requiring federal certification. A number of states and local jurisdictions, even those without a statutory requirement that voting systems first complete federal testing by the EAC, *do obtain voting systems that have been through the testing process*, and therefore have a greater chance of meeting many worthwhile baseline requirements for functionality.

- Some states work in collaboration with the EAC and the VSTLs to include *testing for some state-specific requirements* during the testing process for EAC certification, saving significant time, costs and effort.

> *"As [Indiana's] legacy systems are moving on, new systems are coming in – many are EAC certified. EAC certification allows us a greater degree of confidence in what we're doing. We don't require it, but there is significant overlap of requirements so it helps us reduce redundancies."*[10]

The current testing and certification process is also much more **transparent** than in the previous regime, with testing plans and reports of test results posted online, along with all correspondence and many other details. That information is useful to any stakeholder with interest in voting system technology, was not available under the previous NASED program, and would not be available anywhere else without this program.

Federal testing for voting system approval has **shortcomings**, however. First and foremost, both the guidelines and the testing and certification program are voluntary, and the EAC does "not have the authority to compel manufacturers or states and local jurisdictions to submit to its program, or to force them to correct any known problems or report future problems."[11] Federal testing is also limited by its guidelines and does not test for what is not included in the VVSG. This particularly affects areas of **security** and **usability**. For example, current certification does not guarantee a ballot format that is clear and easy to understand for all voters.[12] Other issues:

- The VVSG do not require adversarial penetration testing, like that conducted in the CA and OH voting system reviews cited above. Testing is primarily for compliance with a given standard, e.g. to determine if a required security control is in use. But **penetration testing** or **open-ended vulnerability testing** may determine if the security control is sufficient to prevent an attack on the voting system.

- The VVSG do not require, as a necessary security property of a voting system, "**software independence**" [13] (a property of a voting system that means an undetected change or error in its software cannot cause an undetectable change or error in an election outcome).[14] i.e., tested systems are not required to be auditable.

- The VVSG do not require **volume testing** of voting systems either (such as is currently done in California). Some experts recommend that volume testing be included in the VVSG, saying it is "… a vital element of certification with respect to voting system reliability… it simulates the load that a typical machine might encounter during its peak use period and does so on many devices at once"[15].

- The current VVSG require vendors to document that they have completed summative **usability tests** on the voting system using individuals representative of the general population. It also requires some pretty good basic standards for usability and accessibility, but no standardized usability test, nor benchmarks.[16]

> *"The VVSG 1.1 (2007) includes the first compliance requirements for a standardized usability test, with an accompanying test method. Experts spent significant time developing benchmarks, validating the protocol and ensuring repeatability with a general audience. …The benchmarks measure the number of errors, the distribution of errors across the ballot, and the distribution of errors within participants, and provide a quantitative threshold for a passing score. The benchmark score set by the Technical Guidelines Development Committee would have failed half of the systems tested for this purpose."*[17]

It should be noted that the term "voting system" has a meaning that may be more "elastic"[18] in the states than at the federal level; as a result, some states may test equipment or systems, excluded from federal testing, that go beyond the casting and tabulation of votes.

Finally, there are significant concerns around the country about the rigidity and limitations of the current structure, and about the future of EAC, the entity charged with certification.

Uncertain Future? New draft versions of the VVSG, which if approved would supplant the current version, have addressed some of the concerns identified above. But while the EAC can continue testing and certifying systems to the current VVSG, approval of new VVSG requires a quorum of EAC Commissioners. ***Currently there are no Commissioners and adoption of new guidelines is indefinitely stalled***. In May of last year, the National Association of Secretaries of State and the EAC held a joint meeting to discuss the "future of the EAC". Legislation has been introduced and passed in the US House of Representatives (though not in the Senate to date) to **eliminate the EAC**, allocating some of its functions to the FEC and abandoning the rest. Critics of that approach have said the EAC's role should be maintained, even expanded, but resolution does not appear likely in the near future.

Meanwhile, voting systems purchased even a decade ago, and the many purchased even earlier, are **aging** – and deteriorating rapidly. Jurisdictions seeking to replace their systems may wish those systems to meet newer, better standards, but **unless new standards are officially adopted, voting system vendors may be reluctant to build systems that encompass them, and the EAC may not test to them**. As a result, states and counties are increasingly concerned about their ability to replace their aging systems.

In the next section, we note most states rely in some measure on federal testing and certification. Even states that do not require federal testing may look to the EAC for its role in promulgating up to date voting system standards. With an uncertain wait to get new voting systems that incorporate the proposed improvements, states can only move ahead if they do not require the VVSG or federal testing, and can cause a voting system to be built to its own specifications and standards. The question arises: **will this logjam have a negative impact on the security and reliability of voting systems? Will states move to alternatives like expanding state testing with better standards to ensure the viability of their counties' systems?**

STATE TESTING AND CERTIFICATION

Sixteen states have no Federal testing or certification requirements for voting systems:[19] AK, AR, FL, HI, KS, ME, MI, MS, MT, NE, NH, NJ, OK, TN[20], VT and WV.

Nine states and the District of Columbia require testing of voting systems "to Federal standards": CT, DC, IN, KY, MN, NV, NY, OR, TX, and VA.

Another thirteen states require that voting systems be tested by a federally approved or accredited testing laboratory: AL, AZ, IL, IA, LA, MA, MD, MO, NM, PA, RI, UT and WI.

Finally, twelve states, including California, statutorily or through rules, require prior Federal certification before a voting system can be used in the state: CA, CO, DE, GA, ID, NC, ND, OH, SC, SD, WA and WY.

Some states, like California, carry out extensive testing, though the description of a state's program in statute may be vaguely worded. Most states that require any state-level testing or certification do so specifically to ensure that state election requirements can be met by the voting system being examined. Requirements could include the capability of a voting system to operate within a "top-two primary" or "straight-ticket voting" or "ballot rotation" or other unique variables. Checking these capabilities may be done through a mock election on the voting system(s) being tested. Some require a vendor to provide references from other jurisdictions to show prior successful operation of the voting system.

The EAC has compiled a report covering the elections code or other regulations for each state describing most of their certification requirements.[21] Surveys of state requirements have been published previously by The Century Foundation[22] and by electionline.org[23]. Since those were published, few states have modified their requirements in this area. For example, in 2011-2013 to date, no legislation has passed in any state about testing and certification.[24] California's SB 360 (Padilla), under consideration in the legislature at present, is the most comprehensive bill addressing voting system certification.

California's State Testing and Certification Program

"Under California law, a voting system and any modification to a voting system must be approved by the Secretary of State before it can be used in any election. Electronic voting systems must be certified at the federal level by the U.S. Election Assistance Commission (EAC) before they can be submitted to the Secretary of State's office for review.

"When a voting system is brought to California for review, the Secretary of State conducts a thorough examination and review of the proposed system that includes:

- Review of the application and documentation;
- End-to-end functional examination and testing;
- Volume testing under election-like conditions of all voting devices used by the voter;

- Security testing that includes a full source code review and penetration testing;
- Accessibility examination and testing; and
- Public hearing and public comment period." [25]

As in other states that require both federal and state tests, the state tests complement rather than duplicate federal testing conducted by the EAC. This chart illustrates:

	EAC	California
Application & Documentation	A technical data package (TDP) is submitted by the vendor to the EAC. The TDP identifies the voting system design, operation, functionality, hardware, software, security, maintenance, and other system requirements.	The same technical data package is submitted to the Secretary of State, along with the EAC certification number.
Software	Examines system source code for its compliance with the EAC's Voluntary Voting System Guidelines (VVSG).	Examines system source code solely for voting system security purposes.
Security	Determines if the system can detect, prevent, log and recover form a broad range of security risks.	Conducts penetration testing to identify any security or accuracy vulnerabilities.
Hardware	Evaluates whether the voting system hardware can withstand exposure to environmental conditions, including varying and extreme temperatures, humidity, vibrations, and inconsistent voltage.	Does not conduct environmental testing of the hardware.
Functional	Determines if the voting system can perform each function required by federal law.	Determines if the voting system can perform each function required by California law. Volume testing under election-like conditions is conducted to ensure the systems can perform in real world election conditions, not just in the laboratory.
Accessibility	Requires vendor to provide the EAC with results from third-party accessibility testing.	Independently contracts with third-party accessibility experts to conduct accessibility testing.

California also approves ballot printers and finishers,[26] including a county, if that jurisdiction produces its own ballots rather than using another approved commercial printer. The Secretary of State can also **decertify** equipment under specific conditions.

In Detail: California's Volume Testing

Why do it: Volume testing uncovers the kinds of problems that can arise during a busy election, by simulating use of the systems under high volume conditions. Federal testing for any systems, with the exception of central count ballot scanners used for tabulating vote-by-mail or other ballots at the county level, may not provide enough ballots voted in election-like conditions to provide needed insights. Volume testing in California started under Secretary of State McPherson and continued under Secretary of State Bowen. California initiated the volume test in the state because there was no requirement at the Federal level. [New draft federal draft guidelines include standards for volume testing adapted from California's model. However, this draft has not yet been adopted by the EAC.]

> "States ask us about it; none have come in yet to team up, but it has been discussed. Some states allow re-use of testing conducted in other states, so we have reached out."[27]

How it works: The testing is done under election-like conditions, using temporary workers as actual voters, in a lab set up like a polling place. The testers are given a script and vote a quantity of ballots each, using predetermined choices on the script so staff can track the results. The whole process is videotaped; it is noted when voters deviate from the script.

> "We verify the rate of paper jams; misprints; skewing; other problems. We can get a sense for the rate at which the jurisdiction can expect problems to start popping up, finding out whether it is a tolerable rate for use. With ballot marking devices, we can find misalignments, where the paper skews and the ballot is marked outside of a voting target. Does the system handle it correctly? Are the tolerances in the scanner picking up the vote information in that case? How often does it happen? Are error messages working correctly?"[28]

Worth the cost: Though many states do not conduct volume testing, California's Office of Voting Systems Technology Assessment (OVSTA) feels it is worth the cost. Further, though volume testing wasn't intended or designed as a usability test, the OVSTA indicates they learn a great deal about usability of the system, and are able to identify issues for voters and for poll workers who are tasked with setting up the equipment.

> "It is most beneficial when there's going to be extensive use of a system, for example if it is the primary voting system in use in all the polling places. Testing of devices or systems used less frequently is still important to ensure they work when voters do need them."[29]

Transparency: If any representatives of a jurisdiction or members of the public want to observe the volume testing, they can. Not many jurisdictions come to observe functional testing, but with volume testing of a voting system, counties considering the purchase of that system come to observe nearly every time. The Office of Voting Systems Technology Assessment provides reports of findings when all testing is complete, and posts those with at least 30 days advance notice of a hearing that is also open to the public.

Penetration Testing

Penetration tests, commonplace for software systems and network security (but not routine for voting systems), involve looking for security gaps or vulnerabilities (sometimes called "white hat" attack because the good guys attempt to break in or penetrate the system's defenses). California law allows the Secretary of State to review voting systems at any time. The California **Top to Bottom Review** in 2007 of voting systems already in use, carried out extensive penetration testing and source code evaluation.[30] The review led to strengthened security requirements, and use requirements for some of the voting systems tested. Retaining in statute the provision that allows such in-depth reviews is important; without it, even where there are known problems that have arisen, election officials may be powerless to take remedial steps and strengthen requirements.

A good investment: When Colorado implemented a network based statewide voter registration system, known as SCORE (State of Colorado Registration and Election management system), including penetration testing in its system review was a natural step. More than a state list, SCORE manages some election procedures and contains information on the political districts people live in and the ballot style they would receive. It manages the issuance of mail ballots with barcoding on the outside of the envelope, and it is capable of scanning and comparing voter signatures. CO also offers an online voter look-up tool, where voters using a standard web app may enter information known only to them, and obtain information about their political district, registration and so on. Voters can register online, change their address or party affiliation, request a mail ballot, and more. This improved app expanded on the look-up features to make it possible to "initiate" or "change" registration.

The system is centralized, with several data center sites. The Secretary of State's system has an ISO rating and sends staff regularly to technology conferences such as RSA. "*We do annual cyber security training for our staff. We make them take a test and they have to get a passing grade. We pay attention to computer security standards for hardening our systems, and industry best practices. Security is an important part of our job. Apart from making ourselves a hard target, with firewalls, not accepting traffic on non-standard ports and other front door management efforts, we also have detection systems to block port scanning hacking attempts, or heavy traffic from a range of IP addresses, and so on.*"[31]

Where systems are dependent on networks, it's important to take care of the basics, but a best practice is to make sure all the protections put in place actually work. "*We have a standing contract with a white hat attacker to do vulnerability testing. First level look at the system is assessment: poke and prod, find where some holes might be, try to identify where vulnerabilities may occur. The next step is* ***penetration testing****; not just trying to find the cracks in the wall, but trying to get through them.* ***It's not necessarily cheap, but doing penetration testing is very useful: we have definitely found vulnerabilities.***

"Engaging before the bad guys do, the white hats will point out where problems are and give advice on how those gaps can be successfully closed. It's a great investment."[32]

Independent Third Party Support for Security and Testing

In some states, election officials contract with independent entities for voting system testing and certification in part or in whole, rather than carrying out some or all of the voting system testing within the election official's department. The state may use an entity:

- to carry out a specific portion of the testing and certification function or to review testing practices;
- to manage the process for the state; or
- to examine elements of the voting system as a whole which are not part of the regular testing process (e.g. consumables, such as memory cards, or peripherals such as electronic poll-books).

Three examples shed light on this interesting practice, in each case from states that require testing to federal standards as well as their own state certification.

New York: The New York State Technical Enterprise Corporation (NYSTEC) is a private nonprofit, set up in NY to function in a similar fashion to how the National Institute for Standards and Technology (NIST) does for the federal government. The State's contract with NYSTEC allows any state agency to hire it without going through a public bidding process, and NYSTEC can serve as technical consultants on a contract.

> "*We used them as our tech consultant to review the independent voting system testing lab, and also to review the people doing the source code review. They have been excellent!*" [33]

Some concerned advocates initially raised the issue that NYSTEC didn't have technical experience specific to voting or election equipment. However, according to Co-Chair of the NY State Board of Elections Doug Kellner, NYSTEC brought instead experience from other fields without bias from all the issues that had gone before them in voting system certification testing. "*That neutral perspective turned out to be a positive*." In the course of their work, they identified problems with the federal testing lab not actually testing to all of the required standards.[34] The test lab subsequently lost its federal accreditation. [35]

Indiana: The state developed its own testing system to remedy a situation that allowed equipment to be purchased that didn't meet statutory election requirements. The Voting System Technical Oversight Program (VSTOP) is part of Ball State University. VSTOP, funded by the Indiana Secretary of State's office, was established in 2008 with the proceeds resulting from a lawsuit filed when a purchased voting system that didn't function according to state code. Although IN doesn't require EAC certification, if a system is EAC approved, it serves as a baseline and then testing is done just to state specific standards.

> "*Most of our state requirements are now incorporated in the 2005 VVSG, although the code requires only 2002 VSS compliance; so there are some redundancies in testing, but we do so to make sure we don't have the same problems of old*." [36]

VSTOP's charge includes recommending systems for state certification, creating a database inventory of voting systems, conducting periodic inventory audits, and monitoring system advisories. The process as described by VSTOP:

> *"We require all the paperwork EAC does (most that come to us recently are approved by EAC) and we look over technical bulletins and documentation. We review the material from the vendor, but we also examine the test results that have anything to do with our specific state standards or code. We then bring the machines in for a hands-on test, and evaluate it ourselves. Particularly at that point we're looking at accessibility. We have an attorney who is a specialist in the ADA who comes in and evaluates. We forward our report to election division and IN Election Commission*."

VSTOP also examines changes for previously approved voting systems. Recently a bill was passed that will require state testing and certification of electronic poll books, devices that fall outside of the testing purview in most states, in part because they are not tested at a Federal level, and there are no VVSG standards for e-poll books. Collaboration with an entity like a university can provide the technology expertise necessary to develop a testing protocol for such a system in state.

Connecticut: The Office of the Secretary of the State partnered with the University of Connecticut Center for Voting Technology Research (VoTeR Center), whose mission is to advise state agencies in the use of voting technologies by investigating voting solutions and equipment and developing safe use election procedures. The Center continuously tests voting machines, and conducts conformance testing, acceptance testing and technological auditing.

Skeptical that certification should be merely a one-time process, CT does what can be called "*rolling certification*."[37] Rather than rely on standardized certification for security, their approach seeks to provide continuous technical oversight and to anticipate issues before they come about. When vulnerabilities are discovered, state procedures can be adjusted to safeguard against problems that could result. For example, VoTeR Center examines the memory cards used in the ballot scanners in the states' towns during each election[38], finding that approximately 10% of the cards fail on average – a large percentage for digital systems. These cards hold the election definition and the votes, so their proper functioning is crucial to each election. Noteworthy is that the memory cards don't fall under the category of things that are usually tested and certified. They are typically consumables programmed for each election by an outside vendor. As a result of audits uncovering vulnerabilities in the cards, the State now uses procedures to ensure there are enough functioning cards for each town's equipment every time.

Local Level Testing

Testing equipment "where the rubber meets the road" – in the real world, where Election Day conditions will have an impact, is one of the most important phases of testing. For each election, local level testing is done to check the functioning of the voting systems, as

well as the correctness of the ballot. The goal of the pre- and post-election testing and reconciliation is to identify failings, where they occur, and whether there was an impact. There are variations in how these pre-election tests are carried out; some jurisdictions test every single machine and some do not. The following two examples describes such logic and accuracy (L&A) testing in two jurisdictions; one where both pre- and post-election L&A are done, and the other where L&A is done as a multi-phase process for best results.

Pre-Election and Post-Election Testing, Maricopa County, AZ

"I'm going to take you to a polling place you'll never see anywhere else." -- Tammy Patrick, Federal Compliance Officer for Maricopa County, AZ. During a field visit to Maricopa, staff from the EAC and one of the VSTLs were escorted by Ms. Patrick to a remote reservation village; the polling place was in a mud pack hut with dirt floors, a plywood door that did not cover the doorway, open to the elements. Temperatures outside were 105 degrees; there was dust blowing in the wind. On that day, it was not humid, but elections also occur during the "monsoon" season. *"How do you replicate these conditions in the lab? You can't."* Seeing how the system works in the real world has to be part of the whole process.

In Maricopa, machines are tested before the election to predict if they are capturing votes correctly, then tested again after the election to see if anything changed, i.e. if they can still capture votes correctly even after the jostling trip to the polling place. Post election audits are done also.

Pre-Election L&A: Maricopa runs ballots from test decks with pre-marked votes through every piece of counting equipment, and then checks totals against the known votes for accuracy. *"We test every machine, every format, every language, for both audio and print materials."*[39] The Secretary of State also conducts such pre-election testing (logic and accuracy, or L&A) on the central tabulators and on a sampling of the voting machines for use at polling places and early voting.

Poll workers run "zero reports" – requiring the voting machine to print out any vote totals cast on it, which should be zero once the machine is set up for a new election – during their set-up meeting and once again at the actual polling place, to ensure no votes were left on the machine (e.g., from the test decks).

Post-Election L&A: Maricopa does a reconciliation audit post election, prior to the canvass. *"Sometimes we'll find that folks have run ballots through twice…! If there were more votes in the total than ballots issued or voters checked in, we investigate anything outside of our variance (of 1)."*

Before the canvass of election, the SoS does a "post L&A" test on the central tabulators and a random selection of equipment. Then the county conducts a hand count **audit** as well. *"This way we can catch how it went not just in our center before the election, but also after the equipment was jostled on the way to the polling place."*

Proofing the Ballot, Travis County, TX

In a typical joint election, Travis County, TX has more than 700 ballot formats; testing every possible format, each permutation and combination, can require thousands of ballots. For a manual test, this is a high volume. The program takes several days to complete; "*it has to be well organized, and if a mistake is made you back out and start over*."[40]

What the county has learned from doing this pre-election testing over the years is that it is valuable to make a distinction between testing for "proofing the ballot" – names spelled correctly, in the right place, attributing votes to correct candidates, making sure it reads correctly – and the tallying function operating correctly. "*Many lump those together and do both at the same time, but it is very helpful to us to separate those jobs. They serve two purposes. There was a mistake in another county recently where they do not separate the two L&A processes; the error wasn't about the tallying, but about the instructions and the spelling of a person's name*."

The county asks all the jurisdictions participating on the ballot to come in, look through the ballot, and check every page before signing off, a participatory effort which the county says yields a better review. These L&A tests, regular and proofing, are listed in the newspapers so that observers may come in to see how it is done.

SOME ALTERNATIVE CONCEPTS IN STANDARDS AND APPROVAL

> *"The structure of how voting systems are designed, certified, and sold is a failed and backward system. I object to having in 2013 pretty much the same choices I had in the 90's. I object to the certification process being used rightly AND wrongly as an excuse as to why we cannot evolve our process and secure more innovative products. And, I object to the high costs of purchasing, storing, and maintaining bulky specialized, proprietary hardware."*[41]

Understanding both the benefits of testing and certification and the shortcomings of the current framework raises the question: what changes are being considered that could improve the path we take to adopting voting technology?

Changing where we obtain voting technology may change how we obtain it.

Some jurisdictions have begun to develop their own customized voting systems rather than purchase commercially available equipment. When voting systems are developed in house, rather than obtained from the existing limited marketplace, a number of benefits can occur, aside from the obvious customized design. *Testing* of a very beneficial kind can start early in the process, improving the final product; jurisdictions can require more transparency in the product, including *open source* software; and jurisdictions can require the use of *common data format*, enabling more interoperability of and modularity in voting systems (see below) and potentially in component testing in the future.

Formative Testing vs. Summative Testing: Voting technology expert and Los Angeles County Voting Systems Assessment Project (VSAP)[42] Technology Advisory Board member Joe Hall notes that we often find problems, either in testing or in actual performance, which could have been avoided with the right input while the voting system was "still on the whiteboard." "Formative" testing of the design concepts takes place early in the research and development of a product. But "summative" testing is all that we can do through the testing and certification framework now – testing done on a finished or close to finished product, "once it's already baked."[43]

An **"in-house" design process** such as what **Los Angeles** is developing, enables building in secure and usable design early in the process. The County is to be commended for establishing a Technology Advisory Board at an early phase of their concept development for this purpose. Another example is taking place in **Travis County, Texas**, where county clerk Dana DeBeauvoir pulled together a team of technical and usability experts to help develop a framework for an RFP for a completely new voting system, for the reasons she describes in the quote above.[44]

Open Source: Jurisdictions able to generate their own new system from scratch can decide to require **open source software**. As source code review is one of the harder challenges in testing voting systems, the more eyes on the code, the more opportunities there are for

finding bugs or problems. Getting commercial vendors to disclose source has been singularly difficult despite a decade or more of prodding.

Standardized Protocols for Development: A goal of improvements being considered to the federal testing and certification program is speeding the time it takes to get through the process, while keeping or improving the quality of the products that come out. A proposed consideration to reduce the amount of time the process takes is **to trade some of the testing for a manufacturer's "declaration of conformity"** with standardized protocols that the manufacturer would use in the process of developing the system, such as ISO 9001.[45] However, according to a Guidelines document on certifying voting systems from the European Union, while ISO certification could be useful, it is also time limited, and usually requires re-certification to maintain the standard. [46]

Common Data Format (CDF) – The Game-Changer

> *"We want this system to have the ability to produce election results that can be downloaded in formats useful to our customers and that meet the hopefully soon-to-be-developed national standards for providing election data so that returns can be rapidly and accurately collected statewide and nationally."*[47]

The Institute of Electrical and Electronics Engineers' (IEEE) working group "P1622" which includes major vendors of voting systems, state and local election officials and others,[48] is building a standard for **more usable data formats for elections**. As noted by the P1622 working group on their website:

> "Today's election equipment generally uses proprietary data formats, thus a device from one manufacturer will not "talk" directly to another device from another manufacturer to transmit voter data from, say, a database to an election management system. …
>
> "A CDF is an enabling technology for election operations involving use of COTS devices and non-polling place equipment for interacting with voters and, without it, newer technologies are much more difficult to interface. With a CDF, electronic voting devices become **easier to use, test, analyze**, secure, and ultimately, trust that they are functioning correctly."[49]

A common theme among many that we interviewed was that being able to test components of voting systems would enable a more streamlined way of acquiring those systems. To date, we lack interoperability between the proprietary systems that are used in the field. For example, a jurisdiction using an accessible ballot-marking device from one vendor with a voting system purchased from another vendor cannot count those different ballots with their other ballots; they need to remake the ballots because the two vendors' systems don't communicate. At present, component testing would not be feasible in California[50], but there is interest in moving toward that point when it is feasible.

The adoption of the Common Data Format will be a game changer, but it's not quite ready yet. The CDF standards will be incorporated into future versions of the federal Voluntary Voting System Guidelines; it is unknown when those will be formally adopted, but a state with the size and buying power of California can certainly require the use of those standards. A completed standard can already be used for blank ballot transmission for overseas voters. Projects underway include election results reporting and transmission of voter registration and candidate database information.

> "Future standards will address interoperability among voting devices and election logging in the common format. These standards, as adopted by voting system manufacturers, will result in scenarios such as an [Election Management System] being able to provide ballot programming information for any manufacturer's voting device, and any voting device being able to export its auditing data or its cast vote ballot images in the common format."[51]

What Could Be: Evidence Based Elections

What if we could do *less* testing and certification, and at the same time have *more* confidence in the correctness of the election outcome? What if we had more regulation of the evidence trail in elections, and less regulation of equipment?

Two UC Berkeley experts from the statistics and computer science departments, propose exactly that in their paper "Evidence-Based Elections." They argue that elections should provide convincing evidence that the reported outcomes reflect how people actually voted, and that we can structure elections that way with "*a combination of software-independent voting systems, compliance audits, and risk-limiting audits. Together these yield a resilient canvass framework: a fault-tolerant approach to conducting elections that gives strong evidence that the reported outcome is correct or reports that the evidence is not convincing.*"[52]

If evidence-based elections are adopted, with required compliance audits and risk-limiting audits[53], they suggest, "*certification and testing of voting equipment can be relaxed, saving money and time and reducing barriers to innovation in voting systems—and election integrity will benefit*."

Testing will not find all programming errors or software bugs, nor prevent the introduction of malicious software into voting systems. And, by itself, the adoption of paper ballot voting systems and voter-verifiable paper records in California does not ensure we will catch software problems that can cause lost or mis-tallied votes. To maximize the security and reliability of voting systems despite the possible presence of bugs or errors, it is necessary to audit the voting system's electronic records (or election results reported by the voting system) using independent records of voter intent.

California is one of twenty-five states that perform audits regularly. It received a good rating in a recent report[54] that graded the states on whether and how well they do this essential post-election "test" or check on the outcome. After passage of legislation enabling risk-limiting audit pilots, the Office of the Secretary of State has carried out risk-limiting audit pilots in ten California counties over the past two years, under an EAC grant.[55] The state is at the forefront of post-election audit research, and uses software-independent systems statewide. It should be noted that recently introduced legislation (SB360, Padilla) calls for the risk-limiting audits as a use requirement for conditional approval of a voting system for use in a pilot election. California is in a position to **lead the nation with evidence-based elections**, especially as enabling technology advances.

RECOMMENDATIONS and KEY TAKE-AWAYS

Today's **certification landscape is in flux**. The fact is that the certification **guidelines are limited**, more limited than the expanding voting system environment of today and tomorrow. More jurisdictions use vote-by-mail and vote centers than a decade ago. Additional ancillary systems are proliferating, such as online voter registration systems, election night reporting systems, online ballot delivery and marking systems, electronic poll books, Internet voting systems, and more. For those systems, there are **no federal standards**; current guidelines apply only to voting and tabulation equipment. Thus, there is no federal testing for such ancillary or new systems, even though some or possibly all may impact a voter's ability to access, mark and cast an effective ballot. That absence of oversight may need to change to prevent a rush to bad technology, but adding effort to an already resource-heavy certification process is complicated.

In 2011, the San Francisco Voting Systems Task Force recommended replacing the existing requirement for federal certification with a comprehensive state certification process, one that is agile, efficient and cost effective, and sound enough to ensure that any new voting system would still meet the minimum federal requirements. Such a process would enable the state to ensure that uncertain conditions at the federal level would not interfere with our counties' ability to deploy good voting systems.

Elections officials we interviewed largely agreed that it was helpful to have a federal body for developing standards that benefit all the states. There was also agreement that the EAC testing and certification function is a valuable and needed resource, particularly for states that do little or no testing and certification, but even for those that do extensive testing under their own auspices.

Finally, ensuring that there is ongoing dialogue between election administrators and technology experts, as has already begun in several places (notably Los Angeles County and Travis County), can help. **Finding a balance between "enough" testing and certification with appropriate use requirements, such as post-election audits, will be important and make a difference in how well we safeguard the validity of our elections**.

Support Evidence-Based Elections: Certification Alone Cannot Ensure Security – Systems can be modified post-certification, and certification may miss existing problems despite best efforts. For security, along with local best practices, robust **risk-limiting post-election audits** should be standard practice to reduce the chance that a wrong outcome would not be found and corrected.

Start Testing Earlier – It's easier to incorporate modifications to improve voting system design early; changes to something already built must be bolted on, not built in deeply. Encourage engagement with experts early in development for more formative testing.

Testing Should Be Ongoing – Certification is not a "set it and forget it" process. Vigilance is valuable and revisiting systems for periodic testing can help identify key vulnerabilities

or areas for improvement. The Secretary of State should retain the responsibility of periodic review.

Test Smart – Focus on usability, accessibility, and penetration testing, especially at the state level. Adopt usability benchmarks. Conduct **volume testing** at the state level. These practices help ensure **all voters have the opportunity to cast an effective ballot**.

Examine Other Systems That Affect The Voter's Ability to Vote – Testing should not be limited to voting systems. Electronic poll books, election night reporting, online ballot delivery, and other systems peripheral to voting machines and tabulators should be examined to ensure they integrate correctly with other parts of the election system, and to ensure voters are not disenfranchised by malfunctions in the technology. While standards for testing such systems don't exist at the national level, the state, counties and voting advocates could work together to identify key concerns and critical functions to check.

Test Close to the Local Level Too – While federal and state testing have clear value, it is important to have some testing controls at the local level where the rubber hits the road. Adopt best practices in local testing, such as L&A and ballot proofing. One state recommends a training process for officials to ensure consistency of testing across all jurisdictions. A state testing entity also can support local election officials by serving as a liaison for county officials and the vendor.

Voting System Test Labs Are A Valuable Resource: Team Up to Save Costs – VSTLs know more than they are asked to report about. They serve as an aid to state testing entities and can help reduce the amount of effort needed to certify systems. Integrating state level and VSTL testing done for the federal certification process means less redundancy.

Enable In-House Development of Election Systems By Jurisdictions – Testing and certification of voting systems should be designed to enable jurisdictions to build their own voting systems, rather than having to buy systems from the current commercial market.

State Certification Standards Should Be At Least As Strong As Current Federal Standards - It is important to have a **baseline** of standards, whether the locus of control for testing is primarily state or is primarily federal. While the approval of updated federal standards is uncertain, if the state controls certification, it may adopt those improvements.

Support Efforts to Develop Common Data Formats for Election Systems – CDF can be a game-changer for more transparent and streamlined election processes, including blank ballot delivery to remote voters, election night reporting, and post-election audits. CDF can enable a movement toward **modularity**, with appropriate safeguards to ensure all the voting system's parts work together. Reduce costs and increase scalability by incorporating more efficient off the shelf hardware.

Support full authorization of a re-invigorated federal Election Assistance Commission.

ACKNOWLEDGEMENTS

The author thanks the many hard working election officials whose work is indispensable to the exercise of the democratic process. Appreciation is due to all who share their expertise and energy in pursuit of better elections in the Future of California Elections (FOCE) group. Thanks also go to the many people who provided insights about voting system testing and certification from their unique perspectives. While not all were quoted, all were extremely helpful: Matt Bishop, Doug Chapin, Dana DeBeauvoir, Efrain Escobedo, Lowell Finley, Joseph Lorenzo Hall, Brian Hancock, Doug Jones, Neal Kelley, Doug Kellner, Merle King, Dean Logan, Joe Losco, Matt Masterson, Larry Norden, Tammy Patrick, Whitney Quesenbery, Philip Stark, Alex Shvartsman, Trevor Timmons, David Wagner. Thanks are due to Kim Alexander, Susan Greenhalgh, David Jefferson, Ron Rivest and Barbara Simons for their insights and feedback. Finally, deepest appreciation goes to the James Irvine Foundation, for their support.

ENDNOTES

[1] See http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm . In the same year Ohio

[2] However, it is only for elections where votes will be cast on a DRE system, not all systems. Further, it is specific to jurisdictions with multiple DRE systems, for which CA does not currently have. Therefore, the last time parallel monitoring took place was in 2006.. Sec. 19255, California Elections Code, available at http://www.leginfo.ca.gov/cgi-bin/displaycode?section=elec&group=19001-20000&file=19250-19255

[3] Secretary of State Post Election Audit Study Working Group; Risk Limiting Audit Pilots

[2] http://www.calvoter.org/issues/votingtech/pub/CVF_voting_tech_policy_brief.pdf

[5] The EAC can also decertify equipment it had previously certified when warranted.

[6] California does not use any EAC certified equipment. All equipment used in the state was certified by NASED prior to the EAC's program becoming active.

[7] See EAC web page on quality monitoring program here: http://www.eac.gov/testing_and_certification/quality_monitoring_program.aspx

[8] Telephone conversation with Matt Masterson, Deputy Director of Elections, Office of the Secretary of State, Ohio; 4/26/13.

[9] See EAC web page on voting system reports here: http://www.eac.gov/testing_and_certification/voting_system_reports.aspx

[10] Author's transcript of comments by Joseph Losco on a panel at a recent NIST/EAC conference on voting system testing and certification in Gaithersburg, Maryland. Video of the session (Day Two, Session Four) is available here: http://www.nist.gov/itl/csd/ct/future-voting-webcast.cfm

[11] GAO Report "Elections: Federal Program for Certifying Voting Systems Needs to Be Further Defined, Fully Implemented, and Expanded," September 2008; available at http://www.gao.gov/new.items/d08814.pdf

[12] Though we are pleased to note the EAC adopted and published ballot design guidelines developed by Design for Democracy, those guidelines are not included in the VVST, voting systems are not tested for them, and they are not required for EAC certification. See "How Design Can Save Democracy," by Richard Grefe and Jessica Friedman Hewitt, NY Times, 2008, available at: http://www.nytimes.com/interactive/2008/08/25/opinion/20080825-ballot.html

[13] Rivest, Ronald L. 2008. On the notion of "software independence" in voting systems. *Philosophical Transactions of the Royal Society A2008 (*366*),* available at http://people.csail.mit.edu/rivest/pubs/Riv08b.pdf

[14] California does require the use of a voter verified paper audit trail; all systems either use a paper trail printout verifiable by the voter on a voting machine or (better) the physical ballot marked directly by the

voter either manually or through the use of an accessible ballot marking device. These features make systems used in California meet the criteria of software independence.

[15] Public Comment on the Voluntary Voting System Guidelines (VVSG) Version II, by ACCURATE – A Center for Correct, Usable, Reliable, Auditable and Transparent Elections, May 5, 2008. http://accurate-voting.org/wp-content/uploads/2008/05/accurate_vvsg2_comment_final.pdf

[16] Email exchange with usability expert Whitney Quesenbery, 4/28/13.

[17] Ibid.

[1] Comment by Merle King, presentation at NIST/EAC Future of Voting Systems, Gaithersburg, MD Feb. 2013

[19] From Election Assistance Commission's pages on Voting System Certification. http://www.eac.gov. Also in this first category are American Samoa, Guam, Puerto Rico and the Virgin Islands.

[20] Tennessee, confusingly, could fit into this first category of "no Federal requirement" or the fourth category "requiring Federal certification" depending on the component of the voting system. TN Code 2-9-110 allows for "non-standard machines" to be used; TN Code 2-9-101 describes requirements for the state but no specifications for testing nor certification; and the recently passed and modified Tennessee Voter Confidence Act (2010), TN Code 2-20-104, requires all precinct-based optical scanners to have been certified by the "election assistance commission as having met the applicable voluntary voting system guidelines." None of the equipment obtained prior to the passage of TVCA was required to be federally certified.

[21] "State Requirements and the Federal Voting System Testing and Certification Program," Election Assistance Commission, http://www.eac.gov/assets/1/Page/State%20Requirements%20and%20the%20Federal_%20Voting%20system%20Testing%20and%20Certification%20Program.pdf

[22] "Balancing Access and Integrity", The Century Foundation, July 24, 2005; available here: http://old.tcf.org/publications/2005/7/pb542

[23] http://people.csail.mit.edu/rivest/voting/reports/2004-04-30%20ElectionLine-SecuringTheVote.pdf

[24] The National Conference of State Legislatures (NCSL) election legislation database identified four bills passed from 2011-present which related to voting systems testing or security but none pertain to certification testing. The database can be found here: http://www.ncsl.org/legislatures-elections/elections/2011-2013-elections-legislation-database.aspx Language did pass in California requiring that the Secretary of State's office be able to certify ballot marking systems, but those are defined separately from a voting system.

[25] http://www.sos.ca.gov/voting-systems/cert-and-approval/vsys-approval.htm

[26] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=elec&group=12001-13000&file=13000-13006

[27] Telephone conversation with Voting System Technology Assessment, Office of the Secretary of State, California

[28] Ibid.

[29] Ibid.

[30] http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm

[31] Telephone conversation with Trevor Timmons, CIO, Office of the Secretary of State, Colorado, April 26, 2013

[32] Ibid.

[33] Telephone conversation with Doug Kellner, Co-Chair, NY State Board of Elections

[34] NYSTEC Review of CIBER Master Test Plan and CIBER Security Master Test Plan, Prepared for NY State Board of Elections, September 27, 2006
http://www.elections.ny.gov/NYSBOE/hava/CIBERSecurityMasterTestPlanReview-Version1.pdf

[35] "US Bars Lab From Testing Electronic Voting", New York Times, January 4, 2007
http://www.nytimes.com/2007/01/04/washington/04voting.html

[36] Telephone Conversation with Joe Losco, Chair, Dept of Political Science, Ball State University, and VSTOP Co-Director, 5/13/2013

[37] Telephone conversation with Alex Shvartsman, Prof. Computer Science & Engineering, University of Connecticut, Director of VoTeR Center, 5/10/2013

[38] For reports of these audits, see http://voter.engr.uconn.edu/voter/audit-reports/

[39] Telephone conversation with Tammy Patrick, Maricopa County Federal Compliance Officer, May 2, 2013

[40] Telephone conversation with Dana DeBeauvoir, April 26, 2013

[41] Remarks of Dana DeBeauvoir, Travis County Clerk, TX, at NIST meeting, February 26, 2013. Available here: http://www.traviscountyclerk.org/eclerk/content/images/pdf_tc_elections_speech_comments_for_NIST.pdf
[42] http://www.lavote.net/voter/vsap/
[43] Comments by Joseph Lorenzo Hall, NIST/EAC Future of Voting Systems, Gaithersburg, MD, Feb. 2013
[44] Remarks of Dana DeBeauvoir, Travis County Clerk, TX, at NIST meeting, February 26, 2013.
[45] ISO 9001 is a standard set by the International Standards Organization that sets out the requirements for a quality management system; see http://www.iso.org .
[46] Certification of e-voting systems; Guidelines for Developing Processes that confirm compliance with prescribed requirements and standards; Directorate General of Democracy and Political Affairs, Council of Europe, 02/16/2011, p. 7. http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_certification_EN.pdf
[47] Remarks of Dana DeBeauvoir, Travis County Clerk, TX, at NIST meeting, February 26, 2013.
[48] Telephone conversation with member John McCarthy, 05/30/2013
[49] http://grouper.ieee.org/groups/1622/faq.html
[50] Comments by Ryan Macias at NIST/EAC Future of Voting Systems conference; integration software would have to be added, and the blended systems we use, problems have arisen when a modification occurs to a single component. Common data format would make this much easier.
[51] http://grouper.ieee.org/groups/1622/WorkingDocuments/1622-2011/IEEE-P1622-Standard-1622-2011-flyer.pdf
[52] Stark, P. B. and Wagner, D. A. (2012). "Evidence-based Elections." Available at: http://statistics.berkeley.edu/~stark/Preprings/evidenceVote12.pdf
[53] A risk-limiting audit checks some voted ballots in search of strong evidence that the reported election outcome was correct – if it was. If the reported outcome is incorrect, then the audit usually will lead to a full hand count that reveals the correct outcome. By design, once the audit finds strong evidence that the reported outcome was correct, it can stop. Thus, the audit intelligently adapts to the facts of a particular election. See http://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf
[54] "Counting Votes 2012: A State by State Look at Election Preparedness," Verified Voting Foundation, Common Cause and Rutgers Law School Constitutional Litigation Clinic, 2012; available at http://countingvotes.org
[55] http://www.sos.ca.gov/voting-systems/oversight/risk-limiting-pilot.htm