Testimony of Ted Selker,
MIT Director of the CalTech/MIT Voting Technology Project

Election Assistance Commission
Hearing on the voluntary voting systems guidelines
July 28, 2005 hearing
Baxter hall Caltech, California.

Introduction:

The Voting Technology Project has been working since 2000 to understand how technology and processes impact voting quality. Our first published report in 2001 found that registration problems, ballot design problems, and polling place operations accounted for four to six million lost votes in 2000. We have continued to observe elections and study election forensics; we now believe that in 2004's presidential race at least one million fewer votes were lost do to those kinds of problems. Since issuing our first paper we have also tested and built technology to improve election security and ballot design; and published studies about verification as well as about accessibility for voters with special needs.

With respect to the voting technology standards, there are four main points that I want to make. **Firstly, technology is a process** and defines practices. All technology, such as that which produces iron, can be reduced to process. You start with some orange dirt and some wood that's been burned to turn it into charcoal; you put them together; take the sludge off the bottom; and that creates iron. In this way the technology is the process.

Voting orcas, ballots, boxes, machines, and databases are, in fact, attempts to systematize process. So, as with the technology of iron production, the election process *is* the technology we are improving with these standards. The process might be improved by and with mechanical, electronic and software technology. Voting technology's role in democracy is to improve the chain of custody from voter intentions to public record. But as with paper which has a legacy of potential for abuse in voting, such innovations must be controlled in order to be effective.

Secondly, mutual oversight; equipment can and should force election officials to work and think independently as they certify every step. It is crucial to design voting standards that encourage and, in fact, require that every step is qualified by more than one person without cohesion of colleagues.

Thirdly, standards should performance based and substantive; there are a very few gratuitous standards in the guidelines. For example, sanserif is the required font although it is not easier to read than serif. There is no reason to specify it, especially since most books are printed in serif, which means that most people have more practice reading it than other fonts.

Finally, methods for qualifying new technology must demonstrate improvements; audit and verification methods such as dual verification systems must show that they cannot add to fraud. When reviewing standard verification 'receipts', many voters claim to see a problem. In fact, our forensic and laboratory experiments show that many people vote for the selection adjacent to the one that they intend to choose. Today's second chance, verification devices and standards must move beyond what a person thought happened to helping everyone demonstrate what happened lest we label fraud as mistakes or mistakes as fraud

These are my preliminary comments on the standards. We at the Voting Technology Project do plan to submit public comment in the public comment period in a more detailed way.

Technological Process Defines Practices:
Looking to the physical and electronic parts of the voting technology process, many voting machines are designed to allow an unlimited number of them to daisy chain their power. I have seen where 10 machines were daisy-chained together which drew too much power and caused an outlet to fail. In some occasions, the daisy-chain was never plugged into the wall so the machines did not run off of the electrical outlet at all. I'm including a photograph, which shows a voting machine with a 'battery down' error message. This should have clued the poll worker that others were not plugged in too (should it be near a bright window)? Time constraints and pressure meant that voting officials did not check the battery.

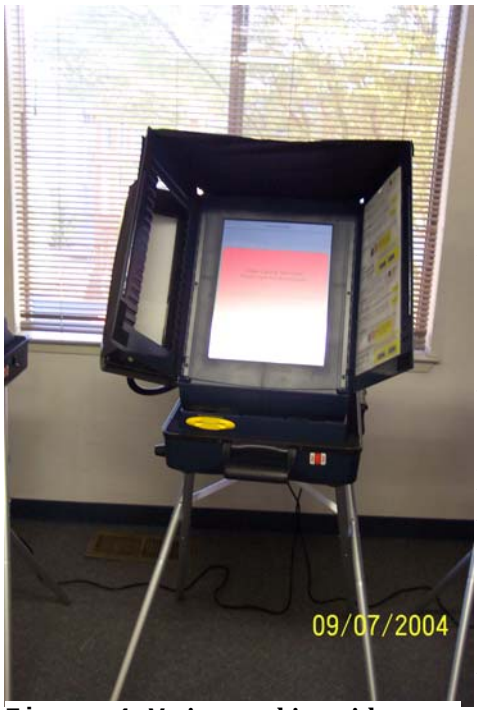

Figure 1 Voting machine with a 'battery down' error message.

Could the warning have been clearer than a large red image on the screen? Audio indicators would have prevented numerous problems that I have witnessed while watching many tasks associated with the administration of voting-machines. These redundant, accessible alerts would make voting machines less mysterious for many people.

A small speaker should be included in any electronic voting apparatus for multimodal verification of administrative functions. The inclusion of some sort of audio or separate modality for each possible human error will make voting machines easier for people with special needs as well as able bodied voters to successfully operate.

Anything done to a voting machine that changes the way it works should be indicated by both a redundant, multimodal, i.e. visual and an audio alert. For example, when we turn it on it should give an audio alert as well as show a screen display that indicates that the voting machine is booted up. When a voting machine is running out of batteries it should give audio as well as visual warnings a few minutes before shutting down. In any way that a voter or voting official can do something to a voting machine that machine must offer feedback in order to allow people to verify that an action was taken.

Another problem I have frequently seen in voting machines is sockets that don't have any affixment. For example, without any tools someone could accidentally just pull out the power cord in the Sequoia VVPAT printers. All connectors should be affixed. Power plugs have in the past and should in the future have tabs that allow them to be screwed to the middle cover screw of a power outlet. EPROM and other programmable electronics shouldn't have ways of being used without notice such as visible ultraviolet light reprogramming windows and unsecured jumpers (which I have seen on some machines). I have also witnessed problems with life counters that can be changed or unplugged without notice. Anything like a life counter should require some sort of visual indicator that will make it obvious if they have been tampered with. Machines should be required to keep records of any action taken on them, including the all too common act of opening the ballot box during an election. All connectors and sockets within the electronic part of these machines should have some sort of a kiss-and-tell arrangement such as fingernail polish on them. I've never seen that on a voting machine, however, it is frequently used by manufacturers of delicate electronic equipment like TV's to insure that the calibration t changes are noted if only for warrantee purposes..

Also, process evaluation is crucial for technology. For example, while XML was a fine way to write up how ballot logics were distributed on a system that I tested, leaving the only copy of what ballot modules had been programmed and distributed on one computer, which was supposed to be on a network, not a good idea. Backing that information up on a CD and storing a copy off-site to secure that XML file should have been an essential element to securing the ballot inventory. Well-conceived processes together with technology make elections secure.

Voting systems must require independent checks for each place votes can be affected:

The standards should require two people to think separately as they certify any aspect of voting equipment or results. I have not seen ballot creation, technology and use specifically discussed in the guidelines. However, I've observed frequent mistakes with the distribution of ballots for use with Optical Scan, Direct Record Electronic and punch-card voting equipment. The photograph shows many people who were unable to vote on some races in the Reno / Sparks, NV September, 2004 election because they were accidentally issued provisional ballots.

Figure 2 many people who were unable to vote on some races in the Reno / Sparks, NV September, 2004 election because they were accidentally issued provisional ballots.

Mistakes are easily made when only one poll worker is present to operate and oversee ballot creation and distribution at a ballot creation module, or writes down a voter's information, and gives the person the ballot without any double-checking by a second pair of eyes. Problems could be eliminated if the voter was required to verify that the ballot is the correct one for them, either by looking at it directly, looking at it on a display or hearing that the right ballot was being dispensed. The ballot creating module might say:" Ted Selker, Democrat, Precinct 703" (all public information). I might be required to view a display to accept the ballot or a separate voting official might have to corroborate that it is the correct ballot for me... Systematic verification that correct ballots are delivered to voters appears to be missing in the standards.

I have observed people recording voting records with a pencil. A pencil should never be allowed; nor should erasers, which I have also witnessed used on election materials. But if one official single-handedly writes down the settings from twenty machines, as shown in the photograph below, who's to say that person didn't make a mistake? Even when double-checking is legally required, it can seem redundant and almost confrontational to have a second person verifying a polling official's work. However, if each member of a two-person team had wrote on different sides of the same piece of paper with a distinct color of ink, they couldn't so easily be coerced (accidentally or on purpose) to forgo their independent notations easily which seems to often be the case; the procedure would encourage cooperation and make discrepancies easy to spot.

Figure 3 one official single-handedly writes down the settings from twenty machines

I am not aware of voting equipment that requires two people to log on separately to establish that someone was there to corroborate the running of ballot creator, selection acquiring system or counting machines. Such buddy systems should be part of standards that seek to disallow any one person from running a voting or counting operation alone.

Guidelines should be substantive: Sanserif is not well established to be better than serif for reading. As stated above but there are some graphic layout objectives that are worth noting. I disagree with the standard's statement that usability is not easily tested. People can read a left justified list much faster than a center justified list, vertical alignment of similar things helps visual scan, etc. Skip-to-next as an audio requirement, as the guidelines stipulate, will be useful if and only if feedback were also required. While I and the VTP expect to make detailed remarks on such issues, they aren't the heart of my observations concerning this document.

Electronic data should be treated as a voting record. As written, the standards indicate that electronic data is not election record; however, it is an important record that can be made archival. Electronic data is less delible than physical data in many ways. It can be placed on write once media; easily backed up to make changes much more testable/observable than with physical objects (in many cases, readable even after attempts at deleting it). The dates of recording can be established. In fact, many current forensic procedures utilize electronic data to establish important facts. Electronic data should be treated as a voting record and kept archivally for at least 22 months. Ideally it should be kept forever because electronic data can be stored in negligible physical space.

There is a requirement stipulating a mean time between failures of 135 hours. Observing paper-trail printers in use, one in twenty needed attentions sometime during the set-up or voting. I've been told of elections with worse problems than that. The mean time between failures should take the entire system into consideration and be set at an error level that is acceptable for that system. For example, if one is designing a system for LA and doesn't want to have hundreds of mistakes, then the mean time between failure for all equipment has to be low enough so that a couple of million people can vote without losing a vote.. This is only possible with excellent checks and balances on the chain of the custody of voting machines. This should be specified in the guidelines.

I've seen many, many mistakes caused by people not knowing when and how to properly open, close, or otherwise handle ballot boxes and paper verification printers (which should be treated as the same thing). In fact, I never saw one ballot box closure on any of the paper verification printers I observed in Nevada. Such closures might have orange indicators, noisemakers, blinking indicators, or otherwise obviously show voters and officials that they are in place. Unsealed boxes without such closures will be equally easy to discern. Ballot boxes should require sealed interlocks before the machines allow voting. I include a picture of an optical scan machine on November 2 2004 with envelopes of ballots which had been taken out of the machine to "reduce jams".

Figure 4 an optical scan machine on November 2 2004 with envelopes of ballots which had been taken out of the machine to "reduce jams".

.

There were some missing things in the standards that I want to remark on as well. Voters and election workers should be able to visually see that the voting machine and ballot are certified for this election. While the guidelines specify that ballots should not have any advertising or identification on them, maybe they need to have some official identification that helps people verify that it is the election's authentic and correct ballot, not a non-certified, prototype or ballot from another place or time. There are famous cases of changed ballots and voting equipment. We can prevent such mistakes or fraud in the future.

Methods for qualifying new technology must demonstrate improvements:
Verification must verify. Verification must be designed so that claims about problems matter and can be sorted out. Do and can people verify with the voter verified X audit trail system, (where X might be audio, video, paper, stone, smartcard or whatever)? Verification, mechanical reliability, accountability and accuracy levels for any system must be ascertained through experiments and demonstrations.

The process of qualifying approaches for verification and auditability technology has to be established in the guidelines. Qualification tests for architectures should be specified so that as new architectures — such as closed systems, open systems, cryptographic techniques, Byzantine architectures, dual verification systems, voter verifiable X, audit trails, etc. — will be and evaluated and considered for use when they improve the voting process. Good approaches for testing these technologies should be specified and be required... Methods and schedules for qualifying new technologies should be defined in the voting standards so that as new technologies — whether these be innovative audio ballots or new kinds of devices for accessing audio ballots -- are created, we have a method for testing and qualifying them, whether or not these technologies have previously been specified in the guidelines.

Defining the audit data for events must be made explicit. Many events happen for a voting machine during its life, equipment runs through a power outage, falls on the floor, is turned on or off runs out of batteries, is reset, is calibrated, has its software upgraded, etc Unusual events happen for all voting equipment, therefore machines should be designed to archivally log such occurrences. In addition, procedures should be defined for where this information is to be made available to whom. Vendors and election officials have told me about many events that are never reported. In July I heard of a new case in which an optical scan voting machine stopped counting in November that was not known or reported before that. How does knowledge of this incident get transmitted, to whom, how can it help? I have been told that mechanical airplane failures can require all owners of airplanes with that mechanical configuration to be informed and have upgrades made available. It seems as though EAC, local election officials, and the Secretary of State should have records of all voting equipment events. Further, protocol for what to do if an event is found with other similar machines is important...

Testing audit data and collection is crucial and should be part of checking voting machines. Do machines record the data that they're supposed to when something is not done correctly? Electronic data must be treated as election data. In your standard it is reported that this is not necessary. As stated above, electronic data can be more indelible in many ways than physical data, and is used forensically for many, many different purposes.

Testing standards for disabled accessibility must test access directly. There are many inadequately accessible voting systems, whose shortcomings go undetected when they are evaluated merely for having buttons that go backwards and forwards (as the standards specify). Accessibility tests should require any voting technology to demonstrate that disabled people can use it to vote accurately within a reasonable amount of time. An exemplary prototype of each ballot type for a machine should be assessed for its quality. Special needs voters using the system should be shown to work with an accuracy level that is on a par with that of normal people using standard approaches.

Figure 5 Three people in a single booth on November 2, 2004.

The actual benefits of usability are not difficult to prove or measure. The standards committee must strike the statement that usability benefits are difficult to prove. There are many simple demonstrations of improvements to election accuracy, integrity and security.

Privacy:

It is a more difficult to restrict a voting booth without a curtain for use by one person at a time than one, which has a curtain. In the photograph below there are three people in a single booth… Curtains are examples of technology that can act as prosthetics to protect the secret ballot, help people vote securely and privately.

Just as they keep beginning-of-day records, etc., electronic voting machines should create internal records at the time that they are being set up. Complete records should be retrievable and available from voting machines to the ITA, the state and local certification officials at the time of an audit.

I conclude with an image of a polling place that is inside of a glass room. The polling place activity is observable and the ballots still secret. The standards in my opinion must be here to support creating, and using materials in service of a eliminating the ways votes have been lost in the past with a glance to how they might be compromised in the future.

Figure 6 a polling place that is inside of a glass room.

Thank you for your attention. I look forward to the complete and ongoing living document of the voting system guidelines and to the positive impact that they will have on elections.

Reference materials:

S. Ambler, R. Jeffries, Agile Modeling: Effective Practices for Extreme Programming and the Unified Process, (John Wiley & Sons, 2002).
B. Berard, et al. Systems and Software Verification: Model-Checking Techniques and Tools (Springe, 2001).
S. Cohen, Ted Selker, An Active approach to Verification May, 2005, http://vote.caltech.edu/media/documents/wps/vtp_wp28.pdf
T. Selker, Election Auditing is an end to end procedure, Science **308** 1873 (. 2005).
T. Selker, User Experience Magazine, Usability Professionals Association 4, 1 (Feb. 2005).
T. Selker, Presentation at Caltech/MIT Voting Technology Project Symposium, Cambridge, Ma, October 2004 (2004;http://www.vote.caltech.edu/Reports/selker.ppt)
Voting Technology: Innovations for Today and Tomorrow, Symposium, Oct. 1, 2004; http://www.vote.caltech.edu/events/2004/voting-tech
R. G. Saltman, "Accuracy, Integrity and Security in Computerized Vote-Tallying", National Bureau of Standards Special Publications, 1988, pp. 500-158
R. Sinnott et al., "Voting Machine Peripherals and Software", Irish Commision on Electronic Voting, 2004; www.cev.ie/htm/report/first_report/pdf/Appendix%202C.pdf).
S. M. Sled, Vertical Proximity Effects in Recall (2004;http://www.vote.caltech.edu/Reports/vtp_WP6r.pdf).
C. Stewart III Residual Vote in the 2004 Election, Feb. 2005; http://vote.caltech.edu/media/documents/vtp_wp21v2.3.pdf
http://www.vote.caltech.edu