Testimony of David L. Dill

Professor of Computer Science, Stanford University and
Founder of the Verified Voting Foundation and VerifiedVoting.org

Before the Election Assistance Commission, July 28, 2005 Hearing, California Institute of Technology, Pasadena, California

Chairman Hillman, Vice-Chairman DeGregorio, and Commissioner Martinez, thank you for inviting me to comment today on the Voluntary Voting Systems Guidelines (VVSG).

I would like to start by stating some principles that should, in my opinion, underly EAC action on voting standards.

First, the legitimacy of elected officials comes not from fair and accurate elections, but from the people *knowing* that the elections are fair and accurate. There is no hope of demonstrating the accuracy of an election to skeptical candidates and their supporters unless the technology storing and counting the votes can produce the reliable evidence.

Second, a vital role of the EAC should be to protect the integrity of our elections. The guidelines for equipment and procedures established by the VVSG should be sufficient for the public to have unqualified confidence in the accuracy of election results. The EAC has a responsibility to demonstrate that the guidelines ensure the accuracy and security of the voting system.

Third, decisions need to be based on the best available information from the most reliable sources. The true independent experts on technical questions must be consulted, and, at least when there are disagreements, their answers weighted according to the quality of the source.

Finally, flexibility of the standards is not as important as the trustworthiness of the voting system. Technical approaches should not be allowed unless we know they can be used accurately and securely. When new approaches are proven, the standards can be updated.

Unfortunately, the draft guidelines are totally inadequate to provide us with trustworthy election results. Under these guidelines, voting technology can and will be certified that can be completely subverted, undetectably, by small groups of people. Consequently, election results cannot be trusted even when conducted by the *most competent election officials* using *the best possible election procedures.*

The 24-month implementation period is a big problem. My understanding is that these guidelines were written to be implemented by 2006, with more stringent guidelines to be developed for the near future. The guidelines are weak because many compromises were made so they could be implemented rapidly. The 24-month implementation time means that we will have no protection, other than the very inadequate FEC 2002 guidelines, until 2008; then these weak guidelines, which were only intended to be a "quick fix," will finally be implemented. We can do better.

The guidelines fail to require independent, accessible, voter-verified audit trails. If voters cannot confirm that their votes have been accurately recorded for post-election audits or recounts, there *is no evidence available that can be used to prove the accuracy of an election.* When an election yields an unexpected result, no one will ever know whether the outcome was accurate, or resulted from error or fraud.

Perhaps we wouldn't need voter-verified audit trails if there were some way of establishing that computer systems were trustworthy. Unfortunately, the state of the art does not yet allow this, and may never, since the problems grow continuously with the increasing complexity of computer systems. As I pointed out in the December 2003 NIST Voting Standards Symposium, there are three problems no one knows how to solve with surety: we don't know how to eliminate all errors in computer systems; we don't know how to make computer systems secure; and, we don't know how to ensure that the systems that deployed are the same ones that were certified. There have been many advances in each of these areas, but the problems are getting harder so fast that we can't even keep up. An especially hard problem in computer security is how to deal with "insider attacks" by people with privileged access, such as employees of the vendor.

Electronic voting is a uniquely hard problem because of the secret ballot. If a voter votes for candidate A and a machine stores an electronic for candidate B, while displaying a vote for A, the voter will not know. After the voter walks away from the machine, no one else can know who he or she intended to vote for. All they will see is a vote for candidate B.

The only solution is to make sure the voter can check an indelible record of his or her vote, and that record is saved securely. The records also must be used, in a recount or (better) during random audits. With voter verified records and routine mandatory audits of randomly-selected precincts, any widespread discrepancies between the votes that are recorded and the intended votes will most probably be caught. We can then have justified confidence in the accuracy of our elections. This is basically the concept of "Independent Dual Verification," except that it has been relegated to an "informative appendix" of the VVSG, where it has no force.

So far, I have deliberately avoided saying "paper." However, at this time, paper records are the only workable way to implement "Independent Dual Verification." The people who know computers best are generally unwilling to trust their votes to paperless e-voting machines. The Association for Computing Machinery, which is the largest association of computing professionals in the U.S., adopted a position in favor of requiring e-voting systems to produce a physical record (such as paper) for inspection by the voter, after a poll of their membership showed that 95% supported that position.

Unfortunately, the commission is not going to hear this message from its advisory committees, which fail to represent many stakeholders and often do not have needed technical expertise. In particular, election technology is extremely dependent upon computer technology, yet there are few genuine experts on computer security on the Commission's Technical Guidelines Development Committee (TGDC).

To see why this is a problem, consider the fate of resolution #13-05 to require voter-verified paper trails, introduced at the TGDC meeting on January 18, 2005. This resolution was introduced by Prof. Rivest, the member of the TGDC with (by far) the greatest expertise in computer security. That resolution was voted down. I would be interested to know what the rest of the TGDC knew about computer security that Prof. Rivest does not. The minutes of the meeting do not answer this question, since there is no meaningful debate of the technical merits of that proposal – the discussion centers around political questions.

My understanding is that the members of the Commission are not bound by the advisory recommendations of the TGDC, and that you have the power to add a requirement for accessible

voter-verified paper records to the guidelines. I would urge you to add such a requirement, or to provide a detailed explanation for why paperless DREs can be trusted. I believe that if you take an objective look at the best available information, you will come to the same conclusions as thousands of computer professionals.

Fortunately, there exists a cost-effective and highly accurate technology for voter-verified paper records (VVPR): Precinct-count optical scan, with an accessible ballot marking device for those who cannot mark ballots with a pen or pencil. Precinct-count optical scan has been widely used and thoroughly studied. A requirement for VVPR will not entail a significant financial or technological risk to states and counties.

As you know, the guidelines are lengthy. I will be submitting detailed comments later through the EAC process. However, in my remaining time, I would like to emphasize several specific aspects of the guidelines that need attention.

The optional VVPAT guidelines in the VVSG are headed in the right direction. However, the term VVPAT is undefined, and the guidelines seem to assume that state-mandated paper trail requirements will be met by DRE voting machines with attached voter-verifiable printers. Ballot marking devices for optical scan systems do not fit this model, nor do machines that simply print ballots without keeping an electronic copy. Some requirements, for example, that the voter not be able to handle the ballot, are inappropriate for ballot marking devices. The VVSG must clarify which requirements apply to which technology.

The guidelines are grossly deficient in the area of networking security. Connection to a communications network creates enormous security vulnerabilities, because so many more people (and programs) can attempt to access the system. Software defenses often have unexpected security holes. Worse, network access can be used to trigger malicious software, or obtain access through a security hole that has been deliberately installed in the software. The only prudent course is to make sure that any network links that could reach outside the polling place are *physically disconnected*. The combination of live networking during an election with paperless electronic voting is nightmarish.

Unfortunately, the guidelines refer at multiple points to the possibility that *voting machines may transfer individual ballots over public networks during an election*. This is a computer security disaster.

The guidelines also allow wireless networking, which opens up similar security threats. The guidelines require lots of documentation and justifications for the use of wireless, but the inevitable consequence of allowing it is that machines with wireless capability will be certified, even though they will not and cannot be secure. Wireless networking is unnecessary and inherently unsafe, and should be banned outright.

Another area is interoperability – the ability of equipment from different vendors to work together. For example, it should be possible to use a ballot marking device from one vendor with an optical scan system by another vendor. Right now, the requirement that whole systems be certified may allow one vendor to sabotage the use of another vendor's equipment, if the first vendor does not cooperate with the certification process.

My final comments are on the certification process. The current process is almost worthless for security. The process itself has to be made much more stringent. In particular, security evaluations

should be conducted by *experts not chosen by the vendors*, and those experts should be allowed to do open-ended research on possible attacks (such groups are sometimes called "Tiger teams"). Indeed, the TGDC passed resolution #17-05 calling for such an approach, which unfortunately does not appear in the guidelines.

There is also a severe need for more transparency in the certification process. The current process is stacked in favor of vendors, who have a huge and unfair information advantage over the rest of the public because the process is so secretive. Interested parties are not able to check whether the certification process was conducted well, or even what features the machines actually have.

Most of what we know about voting machine security comes from the analysis of Diebold's AccuVote-TS software by researchers at Johns Hopkins and Rice Universities, which was only possible because Diebold's secret software was released on a public website by Bev Harris. That analysis showed that there major flaws in the security design of the software, a fact that the public and policymakers had both a need and right to know. Now, Diebold claims to have fixed all the problems, even though many of them appear to to be unfixable without a complete rewrite of the system. It is unacceptable that only Diebold and the ITA know the truth of whether these problems have been adequately addressed.

To keep the vendors and ITAs accountable for their work, the EAC should require that, as a condition of certification, the report produced by the ITA be publicly released, along with the technical data package should be released.

In summary, the proposed guidelines do not provide essential protection for our elections. The EAC should take bold action to ensure that our elections are not only accurate, but that everyone *knows* that they are accurate – even experts in computer security. New guidelines should be in place by 2006, and more stringent guidelines should be implemented as soon after that as possible. The most important step would be to require accessible voter-verified paper records, which is can be easily achieved by any jurisdiction by using precinct-count optical scan with an accessible ballot marking device. There also needs to be much greater attention to network security issues, including a total ban on wireless communication capability. The certification process needs to be revised to make sure that stringent security evaluations occur, and there must be much more transparency in the process.

Thank you.