

**Testimony submitted by VerifiedVoting.org to**

**The US House of Representatives**

**Committee on House Administration and Committee on Science Joint Hearing:  
*Voting Machines: Will the New Standards and Guidelines Help Prevent Future Problems?***

**July 19, 2006**

---

There is a crisis of confidence today in electronic voting systems that are widely used across our nation. It grows each day as the public gains awareness of the inadequacies and vulnerabilities of those systems. The concern is perhaps greatest among those who have the most technical understanding of the computing systems that form the basis for the voting equipment.

The concerns that led to this crisis are not new, but no set of standards alone has been or will be sufficient to erase them.

There will be those who say the crisis is not the fault of inadequate systems but rather the fault of those who shed light on the inadequacies – a “shoot the messenger” approach to restoring the public’s sense that they can be sure their votes will count. They are wrong. They might be able to bury their own heads in the sand, but asking the public to take it on faith that there’s no such thing as a machine malfunction or someone who might want to tamper with an election is simply not good enough, and a simple review of historical fact belies that belief.

There will be those who say that *system* problems can be solved with a set of *procedures*. This too is a false fix, akin to directing the public to watch while we attach a big lock on the front door of the bank, while leaving the back door unlocked and the safe wide open. Good procedures are necessary, as are technical features that support system security, reliability and usability. However, sometimes one needs mechanisms to prevent specific acts that doesn’t depend on humans to follow rules. A procedural fix cannot alone solve a system problem.

Guidelines, regardless of how well written, do not matter at all if they are not enforced. At present, mechanisms are not in place to halt the electoral process or address the problem if the Guidelines are violated or circumvented, nor even to scrutinize the process to ensure Guidelines are not violated nor circumvented. The Guidelines instead become mere fig leaves strategically draped over the never-ending problem of voting systems that cannot be made secure without the essential safeguard of a voter-verified paper record (VVPR) of every vote, and mandatory random checks of the paper records to ensure accuracy of the vote count.

Seventy percent of the states believe – regardless of the existence of any Guidelines – that voter-verified paper records are necessary.<sup>1</sup> Over half of the members of the U.S. House of Representatives have reflected that majority position by sponsoring legislation that would make

---

<sup>1</sup> 28 states have enacted rules or legislation requiring voter-verified paper records: AZ, AK, AR (partial req.), CA, CT, CO, HI, ID, IL, ME, MI, MN, MO, MT, NC, NV, NH, NY, NJ, NM, OH, OR, SD, UT, VT, WI, WV, WA. Another 8 states are deploying voter-verifiable equipment statewide even without a requirement: AL, MA, MS, NE, ND, OK, RI, WY. For details see <http://verifiedvoting.org>

VVPR mandatory in all states. While only 13 states currently require random manual audits of the voter-verified paper records,<sup>2</sup> many more have the tools to conduct those audits today.

Unless and until these practices (the use of voter-verified paper records and mandatory manual audits of those records) are adopted nationwide, the crisis of confidence will continue to grow. The current set of Guidelines, despite the efforts of those who worked on them, do not resolve this current crisis, for several reasons.

--First, they are inadequate: the current process for voting system certification is wholly insufficient for security, and resolutions of the Technical Guidelines Development Committee to include open-ended research on possible attacks were omitted from the guidelines.

--Second, they will never be adequate for security, if separate and apart from a voter-verifiable voting system and robust random manual audits. This is not to say the VVSG on security shouldn't exist, but rather that it must be understood they can only serve as a potential enhancement to mitigate risks, and cannot ever be strong enough alone.

--Third, the most significant thing the current VVSG could have done to help bolster the public's confidence was not done: On January 18, 2005, Professor Ron Rivest introduced a resolution (#13-05) to require voter-verified paper records at the TGDC meeting. Professor Rivest is the member of the TGDC with by far the greatest expertise in computer security. That resolution was voted down, by members of the committee who know less about computer security than the person who introduced the measure. Just as the Food and Drug Administration would not approve of a pharmaceutical based on a vote where accountants out-voted physicians, **it is important that decisions affecting technical requirements are made by people that are technical experts.**

--Finally, as the lion's share of HAVA equipment funding has been spent on systems that were not designed to those standards, the current VVSG can serve only as a theoretical or philosophical guideline for what you would want in a voting system, if one were going to buy a new one today... but almost no one is buying now. As safeguards for the systems we use today and for the foreseeable future, or as insurance that those systems are accessible and usable as possible—the VVSG are the horse lagging behind its voting-system cart.

## Concerns and Recommendations

Analysis of the VVSG process to date makes clear the Guidelines are inadequate to address the current (justified) crisis of confidence in electronic voting systems. Recommendations for improvement follow.

**1. Prevent Unrecoverable Lost Votes; Mandate VVPR.** During the November 2004 election in Carteret County, North Carolina, a paperless DRE voting machine completely failed to record over 4,400 ballots cast on that machine; this failure occurred because those ballots exceeded the configured size of that machine's electronic memories. The machine failed to warn the affected voters that their ballots were not being recorded, the votes from those ballots were irretrievably

---

<sup>2</sup> AK, AZ, CA, CT, CO, HI, IL, MN, NM, NY, NC, WA, WV - for details, see <http://www.verifiedvoting.org/article.php?id=5816>

lost, and several statewide races were thrown into limbo because the margin of victory in those races was less than the number of lost votes. While this was apparently the largest number of votes irretrievably lost on a single DRE, it was not the first or only documented instance of such a loss. Two years earlier, 436 ballots failed to be recorded on a different vendor's DRE used for early voting in Wake County, North Carolina. And just last year, in Pennsylvania, cast ballots were inadvertently erased at the end of the voting day due to a set-up error.

In each case, had those DRE voting machines been equipped with a voter-verifiable paper audit trail (VVPAT) (or had those jurisdictions been using an inherently voter-verified paper ballot system, such as optical scan ballots), those votes would not have been lost. Yet despite these problems, the revised VVSG do not adequately protect against these types of problems and lack any requirement for VVPAT, despite thousands of comments submitted by the public in support of adding such a requirement.

To prevent future losses of votes due to malfunction, programming error, set-up error, or tampering, the VVSG must require voter-verified paper records. This step will also serve as an interim measure to regain some of the lost confidence in our voting system, although only in those jurisdictions that adopt the voluntary guidelines. For real impact, legislation requiring voter-verified paper records and mandatory random manual audits must be passed so that votes in all jurisdictions are protected.

**2. Accelerate VVSG Update Process.** The VVSG do not take effect until December 2007, and even then, not all states are obligated to follow them because the guidelines are voluntary. Hence, in terms of addressing the current crisis, they offer too little, too late. The lag between their development and their effective date almost ensures that they will be obsolete by the time they are in effect. The capabilities and state of the art in computerized systems changes vastly over the 24 month adoption period, and the pace of voting standards development, while slightly accelerated over what it has been, still seems glacial when seen in the light of security concerns.

Given the rate of change of technology, security-related and other standards in the VVSG should be reviewed annually, and the adoption window should be shorter than it is (e.g. 12 months rather than 24). When gravely serious security or performance problems with voting systems are uncovered as has happened in recent months, standards should be upgraded in response, and if need be, voting machines in the field re-tested for modification.<sup>3</sup> No new elections should have to be run on equipment demonstrated to be faulty or insecure.

**3. Certification Process Should Not Be Cloaked in Secrecy.** Despite some minor changes to the scheme for certifying voting systems (i.e., "qualification" has been renamed "certification", ITAs have been renamed "voting system testing laboratories", and the EAC, through NIST, will assume oversight and accreditation of the testing laboratories), the overall scheme still remains one in which private voting system vendors contract with (and pay for) private testing laboratories to carry out certification testing in secret. Public confidence in the integrity of this

---

<sup>3</sup> These recommendations echo those of Dr. Michael Shamos, Distinguished Professor of Computer Science at Carnegie Mellon University, who testified in 2004 to the Environment, Technology, and Standards subcommittee of the House Science Committee on the subject of voting system testing and certification. Cf. <http://www.house.gov/science/hearings/ets04/jun24/shamos.pdf>

certification scheme will not be achieved if this testing process continues to remain cloaked behind a veil of secrecy.

“To keep vendors and [the VSTLs] 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.”<sup>4</sup>

**4. Stronger Security Testing Needed.** The VVSG scheduled to take effect in 2007 do not mandate the type of vigorous security examination needed to uncover security weaknesses (e.g., the several Hursti hacks<sup>5</sup>, plus additional vulnerabilities discovered by California’s Voting Systems Technology Assessment Advisory Board [VSTAAB]) of the sort discovered due to the inquisitiveness and concern of local election officials (e.g., Ion Sancho, Supervisor of Elections, Leon County, Florida; Bruce Funk, Emery County Clerk, Utah). These vulnerabilities could be successfully exploited without leaving any trace. Any certification system that subjects voting systems to hundreds of hours of "testing" and which takes many months and hundreds of thousands of dollars to complete and yet fails to discover grave security vulnerabilities which can be successfully exploited in a manner of minutes is completely ineffective.

“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”). Any new iteration of the VVSG should incorporate the TGDC Resolution #17-05 which called for such an approach.”<sup>6</sup>

**5. Proprietary Interests Should Not Outweigh Security and Performance Requirements.**

The current (and future) certification scheme based on the current (and future) VVSG appears to be biased in favor of maintaining the proprietary interests of voting machine vendors rather than ensuring the integrity of the voting systems being evaluated.

An example is the inclusion of wireless networking, which opens up security threats while facilitating vendor interests. The inevitable consequence of allowing wireless, even with special guidelines about its use, is that machines with wireless capability will be certified, even though they will not and cannot be secure. Worse, even if a jurisdiction wanted to ban wireless capabilities locally, it is possible under the current certification scheme that they would be unable to determine whether such capability was already “on-board” in their existing systems. First, they'd need the technical ability to check their hardware (and if a wireless component was found, to examine the software to ensure that the software will not support it). Second, warranty and maintenance agreements often consider things like "unauthorized" opening of the case of a voting system to violate or void the warranty. So, more than likely, a jurisdiction would have to

---

<sup>4</sup> Testimony of Dr. David Dill, Professor of Computer Science, Stanford University and Founder of Verified Voting, before the Election Assistance Commission, July 28, 2005 hearing, Pasadena, CA <http://www.eac.gov/docs/Dill.pdf>

<sup>5</sup> Finnish computer security expert Harri Hursti discovered two distinct classes of vulnerabilities in the Diebold AccuVote voting systems: a) Vulnerabilities associated with the use of interpreted AccuBasic code on the removable memory card used to store vote totals and/or ballot images (for details see [http://www.ss.ca.gov/elections/voting\\_systems/security\\_analysis\\_of\\_the\\_diebold\\_accubasic\\_interpreter.pdf](http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf)); and b) vulnerabilities associated with boot loader software and flash memory (<http://www.blackboxvoting.org/BBVreport.pdf>).

<sup>6</sup> Testimony of Dr. Dill July 28, 2005, *ibid*.

ask the vendor if there was wireless capability and take their word for it or ask permission to examine the system to assess whether or not wireless functionality was shipped and armed.

Wireless networking is unnecessary and inherently unsafe, and should be banned outright. Further, The VVSG should define procedures under which local election jurisdictions can reliably verify the absence of such wireless capability in any voting systems equipment that they purchase or lease.

**6. Encourage (Secure) Usability Advances.** The current practice of certifying whole voting systems has the potential to stifle the independent development of add-ons to existing voting systems that can greatly enhance usability and especially accessibility. For example, this practice has impeded deployment of accessible ballot-marking devices which are designed for, and capable of, working with any legacy optical scan voting system, because those devices must be re-submitted for testing with each such voting system, a process in which vendors have yet to cooperate. Accessibility advocates describe a wish for systems with a broad spectrum of capabilities and features, yet typically no one system currently addresses all those needs. Jurisdictions lack the resources to obtain more than one system for accessibility, but even if they had the resources, interoperability between competing systems is lacking.

There is a need to provide for interoperability between such existing and potential modular devices made by different vendors. Yet it is important not to sacrifice the performance and security benefits that end-to-end system testing brings.

The VVSG should look to develop a better solution for inter-operability such as testing a proposed subsystem, and having well-defined, standard interfaces between sub-systems that comprise a voting system. For example, a standardized schema for defining the layout of optical scan paper ballots should be developed to enable the interchange of ballot layouts between voting systems developed by different vendors, so that an optical scan ballot printed by vendor X could be marked by a ballot marking device manufactured by vendor Y and scanned by an optical scanner built by vendor Z. Each vendor would be responsible for providing conversion software to translate between their proprietary ballot layout definition files and the standardized schema.

**7. Scrutiny and the Need to Address Defects Discovered After Deployment:** At present, the revised VVSG and proposed certification process lack any clear mechanism for suspending or revoking the federal certification status of deployed voting systems found to contain serious defects, including security vulnerabilities, that put the public's votes and the integrity of our elections at risk. When such critical security defects are discovered in already-deployed voting systems, some fraction of impacted states issue some sort of warning or advisory, while other states take no action at all. Even when warnings or advisories are issued, most states typically take no further action to ensure that local jurisdictions comply or act on those notices, in part because the costs for implementing interim mitigation procedures fall on local election jurisdictions that lack the resources to effectively carry them out.

When defects in other types of products affect public safety, product recalls are initiated and product defects corrected at vendor expense. But when similarly serious defects or vulnerabilities are found in voting systems, we do not see federal certification revoked or products recalled. (Nor have we seen any requirement that vendors notify all their existing markets about the

problem, with recommendations for mitigation or replacement. This means the same problem can occur election after election, in county after county, despite having been likely preventable in all but the first instance.)

To help prevent voting machine problems, new Guidelines must provide a mechanism for scrutiny to ensure that its standards are maintained and enforced, especially when problems with the design of a voting machine are discovered after it has completed federal qualification and been deployed for use in elections.

The revised VVSG should include mechanisms for suspending or revoking federal qualifications when serious defects in voting machines are discovered after initial qualification, and should require notification and mitigation by the vendor involved to all jurisdictions where the voting system is deployed.

### **Need for Prompt Action**

Slightly over 2 years ago, on June 24, 2004, the Environment, Technology, and Standards subcommittee of the House Science Committee held hearings on the subject: "Testing and Certification of Voting Equipment: How can the process be improved".<sup>7</sup> In his testimony<sup>8</sup> before that committee, Dr. Michael Shamos stated in part:

*I am here today to offer my opinion that the system we have for testing and certifying voting equipment in this country is not only broken, but is virtually nonexistent. It must be re-created from scratch or we will never restore public confidence in elections....*

*... We need a coherent, up-to-date, rolling set of voting system standards combined with a transparent, easily-understood process for testing to them that is viewable by the public. We don't have that or anything resembling that right now, and the proposal I have heard are (sic) not calculated to install them.*

*...I propose that standards for the process of voting be developed on a completely open and public participatory basis to be supervised by the EAC, with input from NIST in the areas of its demonstrated expertise, such as cryptography and computer access control. Members of the public should be free to contribute ideas and criticism at any time and be assured that the standards body will evaluate and respond to them. When a problem arises that appears to require attention, the standards should be upgraded at the earliest opportunity consistent with sound practice. If this means that voting machines in the field need to be modified or re-tested, so be it. But the glacial pace of prior development of voting standards is no longer acceptable to the public.*

Unfortunately, two years after the Sub-committee heard these concerns in testimony, little has changed. Instead of recreating the testing and certification system "from scratch" and making that process "transparent, easily-understood" and "viewable" by the public, the revised VVSG does little to address any of these concerns. Rather, the revised VVSG makes some tweaks to the "arcane technical standards" (Guidelines) and the accreditation of the testing labs, but otherwise

---

<sup>7</sup> <http://www.house.gov/science/hearings/ets04/index.htm>

<sup>8</sup> <http://www.house.gov/science/hearings/ets04/jun24/shamos.pdf>

leaves intact the existing opaque and secretive system which Professor Shamos describes as "grotesque". That system can continue no longer, and must be made transparent.

Beyond accepting public input to the revised VVSG, the "standards body" must show greater evidence that it has heard the overwhelming majority of that public input and must provide a meaningful response to key concerns raised by the public (e.g., concerns regarding the urgent need for VVPR and for the elimination of wireless technology from voting systems).

When gravely serious security problems with DREs are uncovered as they were during this past year, standards must be upgraded in response, voting machines in the field modified and re-tested, and the pace of voting standards development must accelerate to address usability, performance and especially security concerns.

It is time for Congress to act to safeguard our elections. Tweaking the voluntary Guidelines (not even yet in effect) will not address the public's urgent concerns about the integrity of our voting system. Immediate passage of a requirement for voter-verified paper records and mandatory random manual audits will.