

# **Summary of Public Comment on the 2005 Voluntary Voting System Guidelines**

## **A Center for Correct, Usable, Reliable and Transparent Elections (ACCURATE)**

**Presented by Avi Rubin  
March 20, 2006**

### **I. INTRODUCTION**

Voting systems must ensure security, privacy, transparency, usability, accessibility and equality. Through the 2005 Voluntary Voting System Guidelines (the Guidelines) the Election Assistance Commission is responsible for translating these diverse values into specifications and requirements that reliably instill these values in voting systems. To accomplish this task there must be (1) consensus on the meaning of the values listed above, (2) a concerted effort to determine how the Guidelines will drive system design to align with these values, and (3) a sophisticated understanding of how to assess compliance with these requirements and, in a broader sense, of whether the requirements ultimately further the values that inspired them.

In section II, we identify fundamental problems with the process that the EAC has set forth for certifying and evaluating voting systems, and suggest solutions to those problems. First, we call for increased transparency throughout the EAC's processes and the certification and testing process. Second, we call for a reorientation of the VVSG away from its current overwhelming focus on functional testing to discipline-specific approaches to certification and evaluation. Third, we call for a systems approach to voting system certification and evaluation which importantly includes capturing, learning from, and responding to experiences with voting systems at the polling place. Fourth, we recommend that the EAC develop a more nimble and timely approach to updating the VVSG and requiring voting system compliance with new guidelines. In sections III through VII, we further discuss these overarching recommendations and recommend both short term fixes and long term goals in the specific subject areas of transparency, security, human factors, certification and evaluation, and incident feedback.

### **II. ESTABLISHING A SOUND FRAMEWORK FOR VOTING SYSTEM ASSESSMENT**

The proposed Guidelines fail to address central structural flaws of the 1990 and 2002 standards that resulted in an election process with unacceptable levels of incidents and vulnerabilities. Four fundamental structural flaws impede the EAC's ability to deliver sound voting systems: a lack of transparency throughout the process; an over-reliance on functional testing; the failure to harvest and learn from field data; and an avoidable lag in updating and applying new guidelines.

#### **A. The Process Of Certification And Evaluation Of Voting Systems Must Be Transparent**

The testing and certification of election systems must be transparent. The current lack of transparency exacts unacceptable costs in terms of system performance and public trust. The process must incorporate a meaningful period for public comment. The

EAC should require that the technical data packages which are reviewed by the Independent Testing Authorities (ITA) are made available to the public, or at the very least, to independent experts who either agree to sign non-disclosure agreements or who are hired by the government (federal, state or local) for the purpose of evaluation. Furthermore, Independent Testing Authorities should not be paid or selected by the vendors whose systems they are testing.

**B. The Certification And Evaluation Of Voting Systems Must Reflect The State Of The Art In Applicable Disciplines**

Security and system functionality dictate different requirements and require completely different forms of evaluation. Critical system security evaluation—as implemented in academia, industry, and government—always includes adversarial analysis. Adversarial analysis encompasses threat assessment, security evaluation, code review, architectural review, and penetration analysis. Security evaluation includes evaluation by outside agents and by insiders with full information about the system. Such evaluation is integral to ensuring security and is routine practice across industries for which security is mission critical.

Given that voting technology must be usable by the entire U.S. population, is infrequently encountered, and must be intuitive, simple and efficient for this diverse population, user testing must be a priority. To date the Guidelines have not addressed the principle of equality—that every vote be counted and have equal weight. The Guidelines must move away from a simple reliance on functional testing and embrace a more sophisticated and nuanced evaluation regime that is primarily designed to assess whether a systems’ performance meets established goals.

**C. A Systems Approach To Voting System Analysis Must Be Adopted That Includes Investigating And Acting On Field Data**

Voting technology must be informed by experiences in the field that are routinely captured, analyzed and fed back into the Guidelines’ development, certification and evaluation processes. Polling places should include log books in which poll workers record all failures, glitches and other anomalies. The Guidelines must require vendors, testing labs and standards-setting bodies to investigate the field data and institute corrective actions in a timely, transparent manner so that the same or related problems do not recur. Additional crucial information contained in data collected from the field concerns whether failures are concentrated in particular districts or jurisdictions largely comprised of a particular race or socioeconomic class of voters. Such data can illuminate issues with equality between voting systems.

**D. Voting Standards And Technology Must Be Continually Updated**

The establishment of Guidelines must become a more organic process of regular feedback and response, and existing technology must be updated to meet new Guidelines. The EAC, in its Advisory 2005-004, dated July 20, 2005, identified technical gaps between standards put forth in the Help America Vote Act of 2002 (HAVA) and the 2002 Voting System Standards (VSS). This effort by EAC is a good example of the analysis needed to identify and fill existing gaps in the standards.

**III. TRANSPARENCY AND PUBLIC OVERSIGHT**

The move to electronic voting has placed limits and barriers on the ability of election officials and the public to monitor elections. This “enclosure of transparency” must be resisted.

## **A. Transparency In Certification**

The current certification process occurs behind the closed doors, leaving the interested public with no information about the process and no basis to trust the integrity of voting systems. Failing to make certification results available to computer security experts and other members of the public contributes to both the misconception that certified voting systems are state-of-the-art, secure, accurate and fair and the belief that voting machines cannot be trusted.

### **LONG-TERM GOALS:**

- All voting system source code, design documents and security analysis should be made available to the public.
- Move away from purely binary pass/fail certification to include a quantifiable certification process with publicly-accessible results.
- Greater government and public oversight over the testing and certification processes.

### **VVSG 2005 STOP-GAP RECOMMENDATIONS:**

- Certification results regarding a system's performance and the exact tests performed must be made available to computer security experts and other members of the public.

## **B. Source Code Transparency**

The Guidelines must require vendors to make source code and related information available for review by a panel of independent experts, not just by the ITAs or NIST. The independent experts making up a review panel should be given full and unfettered access not only to source code, but to all material relevant to an exhaustive evaluation. Vendors should bear the burden and cost of providing evidence to an independent review panel that their voting product is safe, rather than inspection bodies bearing the burden to show the system is not safe. The 2005 Guidelines lack any provisions that would require vendors and ITAs to open the certification process or source code to public scrutiny and understanding. Through the voting standards, the EAC should put vendors on notice now that they will be required to publish their source code by a specified year, in order to give vendors time to comply.

### **LONG-TERM GOALS:**

- Open the certification process to public scrutiny and understanding.
- Vendors must publish source code for public review.

### **VVSG 2005 STOP-GAP RECOMMENDATIONS:**

- Source code and related information must be available to review by independent experts.

## **IV. SYSTEM ASSESSMENTS THAT DELIVER ENHANCED SECURITY**

### **A. Building Security Into Voting Systems**

Security must be built into the engineering process itself. It cannot be achieved by patching flaws. The reliance on functional testing is misplaced. Security cannot be equated with functionality. A system is functional when it works while being used as planned. Security, on the other hand, has to do with how a system behaves under unanticipated circumstances. By definition, one cannot evaluate a system for security in the same manner used to test for functionality. To illustrate, an elementary and serious flaw in key management in the Diebold AccuVote-TS machines was found by researchers at Johns Hopkins University and Rice University two years ago, after the same feature was criticized by researchers at the University of Iowa almost ten years ago. This fundamental security flaw was never caught in certification testing by ITAs.

## **B. The Framework For Security Evaluation**

The security of a voting system is best measured by its level of resistance to fraud, manipulation, corruption, malfunction and insider attacks. The security evaluation process in place today lacks threat analysis, code review and penetration testing. Functional testing alone, without threat analysis, code review, architectural analysis and penetration testing, will result in fundamentally insecure systems.

### **1. Threat Assessment**

As with all computer-based systems, security breaches in voting systems can arise from a number of sources, including weak or malicious code, programming errors, malfunctioning equipment, personnel involved in equipment or system setup, voting administrators, and poor data storage or handling procedures. For example, malicious code inserted into a system could be capable of stealing an election by displaying a voter's choice in an apparently "correct" manner, but recording the vote as other than the voter intended. A system bug could result in the same error.

Requirements for all voting systems need to be established. Second, the requirements must provide a comprehensive list of attacks that any security analysis must address. Third, vendors must provide comprehensive evidence that their system is secure through evaluation performed by Independent Testing Authorities. Finally, this evidence needs to be made available to independent security experts and analysts for review. In contrast to the Common Criteria model, vendors for voting systems should not be able to choose the evaluation lab, nor should evaluation labs be paid directly by vendors.

### **2. Code Review**

Voting systems must be subject to independent security reviews. Independent security review includes penetration testing, which is required to determine whether voting systems (including both the precinct vote collection system and the central canvass systems) are secure against attack, especially attacks from insiders. The proposed Guidelines contain no such security review. The Guidelines are particularly weak in their handling of commercial off-the-shelf software (COTS). In Volume I, Sections 4.1.3 and 5.2, COTS software is specifically excluded from having to meet testing requirements. This is a gaping hole in security—for example, allowing intentional or accidental subversion of the voting system by manipulation of the underlying operating system. States that have audited the use of code in voting systems have found that uncertified code is routinely used. Uncertified code is another glaring gap in security.

### **3. Penetration Testing**

Finally, penetration testing is an important part of critical system evaluation. In penetration testing, agents simulate a malicious attack on the system, possibly knowing internal information that the system designer considers secret. Penetration testing should be a routine part of voting system evaluation. Election security is a national security issue, where the machinery we use to cast votes for elected offices and referenda must be trusted to the same degree as critical military, medical and banking systems.

#### **LONG-TERM GOAL:**

- Security evaluation to include security ratings along multiple axes.
- Security that is built into engineering and development of voting systems, instead of security based on patching flaws.

- Requirements to include security evaluation, including threat analysis, code review, architectural review and penetration testing.

**VVSG 2005 STOP-GAP RECOMMENDATIONS:**

- Independent review of system security by panel of external experts.
- Elimination of COTS loophole in security evaluation—all software in a voting system must be subject to inspection and testing.
- EAC must announce a timeline now for the elimination of the COTS loophole to put vendors on notice and allow them time to comply.
- Penetration testing as part of certification.

**C. The Quest For Auditability: An Indelible, Independent, Voter- Verified Audit Trail Must Be Required**

By allowing a record that supports voter-verified auditing to be optional, the 2005 Guidelines guarantee that the security of our voting systems will continue to be compromised.<sup>46</sup> Section 301(a) of HAVA requires that all voting systems have an “audit capacity” and that they produce a “permanent paper record.”

Effective audit systems have three main features. First, the records used for auditing must be independent from the primary voting data. That is, even if the system used to record voter input is compromised, the audit data is not subverted. Second, the audit data must be as impervious to corruption, fraud or manipulation as the primary data. Third, the only way to verify that the data in a voting system are correct is through the voters themselves. Lack of voter-verifiability is a central failure of most current DRE voting systems. If votes were incorrectly recorded by the system there is no possibility of a meaningful recount. Today, to remedy these defects, an indelible record in the form of a voter-verified paper audit trail (VVPAT) must be required for existing DREs. Optical scan systems allow voters to verify their ballots before casting.

It is critical to develop procedures to manually recount the audit trail for a random subset of precincts to check the accuracy of the electronic results. The Guidelines do not provide any standards for statistical auditing of random samples of votes. The Guidelines must also specify procedures in the instance of a mismatch between electronic and paper records. The Guidelines include no procedures for handling such a discrepancy between VVPAT data and electronic data. Volume I, Section 2.2.4.1 requires that a permanent record of audit data be maintained, but may be overridden by “authorized officials.” This is an invitation for corrupt insiders to manipulate data. Changes must be entered in an unalterable log and in such a way that the original data is kept intact.

**LONG-TERM GOAL:**

- Indelible, independent, voter-verified audit trail required for every certified voting system.

**VVSG 2005 STOP-GAP RECOMMENDATIONS:**

- Requirements for manual recounts and random sampling of audit records, including keeping of unalterable audit logs.
- VVPAT provision should be a requirement, not optional.

**D. A Call For Interoperability**

The 2005 Guidelines, as written, call for end-to-end system testing. Imposing an end-to-end requirement without requiring interoperability creates barriers against modular upgrades or additions, compatibility between systems and subsystems, and the assessment of subsystems in isolation from the rest of the system. This can stifle innovation and invites vendor lock-in. When vendors prohibit interoperability, states

become locked-in to a particular vendor's equipment and unable to purchase updated or competing subsystems. Requiring interoperability across systems and between system components and subsystems can add to the security and transparency of voting systems. Incorporating open source software into voting systems is one potential route towards ensuring this kind of transparency.

**LONG-TERM GOAL:**

- System-system and system-subsystem interoperability.

**VVSG 2005 STOP-GAP RECOMMENDATIONS:**

- The Guidelines must include a requirement for open interfaces to enable interoperability.

**E. Addressing Network Vulnerabilities**

The transmission of data poses significant security risks. Connecting voting machines to telecommunication systems, which has been done for many years, has recently been shown to be an extraordinarily dangerous practice. All provisions, such as Volume I, Sections 1.5.4, 4.4.2 and 5, that keep open the possibility that voting systems can be networked outside the polling place for data transmission or any other purpose must be eliminated from the 2005 Guidelines. Internet voting should be banned for the foreseeable future because of massive vulnerabilities that have no easy resolution.

**LONG-TERM GOAL:**

- Networking capabilities included once security can be assured.

**VVSG 2005 STOP-GAP RECOMMENDATIONS:**

- Ban standards that permit connection to networks that extend outside the polling place, including wireless networks, Internetconnected networks, and networks connected to a public telephone system.

**V. APPLYING A SYSTEMS PERSPECTIVE TO VOTING TECHNOLOGY**

With the adoption of human factors guidelines, the EAC is taking a step towards recognizing the importance of an additional critical perspective on voting machinery performance.

**A. The Human Factors Challenge: Users Are An Integral Part Of The Voting System**

The lack of attention to voter and poll worker interaction with voting systems is a known source of problems. During the 2004 Presidential election, voters repeatedly reported that upon reviewing their ballot before casting their vote, the votes had been misrecorded. Voters reported that it took five, seven, or even nine attempts of going back and correcting their ballot choices for the proper vote to register.

**1. Voting Systems Pose Complex Usability Issues**

Voting is an intrinsically challenging human factors problem. Voting systems must be usable by citizens regardless of age, disability, education, socioeconomic status, familiarity with computers, literacy level, native language, and the like. Voting systems are staffed by individuals who are not screened or selected for their knowledge of technology. The poll worker population is nearly as diverse as the voting population.

**2. The Proper Framework For Usability Certification And Evaluation**

The 2005 Guidelines proceed to enumerate functional design requirements for usability—as they do for security— without adequately addressing a voting system's level of performance, incorporating known standards and methods for assessing

usability, or analyzing reported incidents during previous elections due to human factor considerations. The current state of the Guidelines will no more ensure voters' effective interaction with voting systems than previous voting standards. The Guidelines must move away from the current reliance on functional testing and embrace a more sophisticated and nuanced evaluation regime that relies primarily on assessing performance against some metric of usability. Usability evaluation by usability and accessibility experts and user testing with actual voters must be performed to ensure the voting system is usable instead of simply designed to meet functional requirements. Usability testing and design need to start early in the engineering process and testing needs to be repeated often.

**LONG-TERM GOAL:**

- Voting systems that are both objectively usable and perceived as usable.
- Standards that ensure reliable casting of votes as a result of a system's technical capacity and human interaction with the system.
- Guidelines supported by empirical data obtained through comprehensive research on human factors.
- Achieve optimal usability by incorporating human factors early in design of the voting system.

**VVSG 2005 STOP-GAP RECOMMENDATIONS:**

- Outreach to usability and accessibility experts to perform heuristic testing.
- Intensive evaluation under conditions close to those experienced during actual voting with a reasonably representative distribution of actual human voters.

**3. Defining The Accessibility Requirements**

Too often, voters who require assistance, because they are disabled or because they lack a full command of the English language, are forced to rely on others to help them cast their vote. This reliance leaves the voter vulnerable to intimidation and harassment that ultimately detracts from their voting rights. The Help America Vote Act of 2002 mandates that every polling place shall have at least one voting station equipped for individuals with disabilities by Jan. 1, 2006. In addition to requirements being undefined and not testable, the 2005 Guidelines set unreasonable standards for certain machine functions designed to accommodate particular kinds of disabilities. As a result, specific mandates for a particular machine function and a particular disability must be justified, since they foreclose options that may have other advantages, such as features that can make a machine more accessible to another class of individuals. Section 203 of the Voting Rights Act of 1965 mandates alternative minority-language access. The requirements set forth in the 2005 Guidelines need to be clarified and refined to effectively improve the opportunity for multi-lingual voters to effectively vote independently and privately.

**LONG-TERM GOAL:**

- Maximize the opportunity for voters to vote independently and privately, without compromising important values like system security.

**VVSG 2005 STOP-GAP RECOMMENDATIONS:**

- Include members of disabled populations in empirical research, in particular to verify vendors' claims of the accessibility benefits of electronic systems.
- Effective implementation requires clarity and precision in the definition of terms.

**B. Field Data Must Play An Integral Role In The Development Of Guidelines And System Evaluation**

Guidelines lack a process to incorporate suspected system failures or to address changing technology. In particular, the Guidelines fail to establish standards that ensure performance data from the field are used to improve systems so that the same problems do not contaminate future elections. The Guidelines should require a feedback loop wherein data is collected in the field and provided to vendors, testing labs, and standard-setting bodies that are required to investigate and address the incidents reported. There were no fewer than 23,000 voting problems reported by the Election Protection Coalition (EPC) in the 2004 Presidential election and over 34,000 to date. In addition, the House Judiciary Committee received 57,000 complaints of election irregularities. Problems included difficulties with casting ballots, such as miscasting of votes, inadvertent vote casting, and incomplete voting. Seventy-five percent of the reported problems were associated with a particular type of voting equipment (paperless voting machines) and ninety percent of all incident reports were associated with equipment from five vendors. Incident reports from the 2004 Presidential election showed that many of the equipment failures implicated systems certified to 1990 standards since the majority of the voting systems used in that election were qualified to the outdated standards.

Parallel monitoring provides field data not reported by voters that should be analyzed and acted upon. In parallel monitoring, people cast scripted votes while being videotaped. The cast votes are compared to the scripted votes and the video record. Parallel monitoring can help to expose malicious or poorly-designed code. Despite frequent failures associated with 1990-certified equipment, most systems in use today are certified to 1990 standards.

**LONG-TERM GOAL:**

- Problems with existing voting systems are identified, understood and fed back into the process of recertifying existing systems and establishing future voting standards.

**VVSG 2005 STOP-GAP RECOMMENDATIONS:**

- The critical data obtained from the incident reports of the past two Presidential elections (and other data) must be examined and fed back into the standard-setting process.

**C. Ensuring Equality Of Voting Systems: The Relationship Between Usability And Field Data**

It is particularly important to ensure the equality of different voting systems used across diverse populations. If the data reveal that failures come from jurisdictions largely comprised of a particular race or class, potential issues of equality are raised and should be further explored. It is unacceptable to allow problems of this sort to go without response and corrective action. As new technology emerges for securing systems and/or for accommodating the disabled, the non-English proficient voter, and other voters who under the current voting system require assistance, the standards should be updated to reflect the improved capabilities in a timely manner.

**LONG-TERM GOAL:**

- Standards that demand accountability and proof from vendors and testing labs that known equipment vulnerabilities and inequalities will not continue to contaminate the voting process.
- State-of-the-art tools implemented as they become available.

**VVSG 2005 STOP-GAP RECOMMENDATIONS:**

- Continued collection and analysis of voting field data and correction of inequalities.

**VI. NEEDED CHANGES IN DEVELOPMENT OF THE GUIDELINES**

The development of Guidelines must become a process of regular feedback and response. Existing technology must be updated to meet new Guidelines. It is unacceptable that archaic and flawed systems are used in the most important aspect of our country's democratic process.

#### **A. Unacceptable Results Of Delayed Implementation**

The proposed 2005 Guidelines continue to propagate delays in implementing improved standards. We recommend moving to a continuous, ongoing certification and de-certification process. Instead of certifying a system once, systems should be periodically reexamined. As standards evolve and our knowledge expands, systems that were once acceptable may no longer be.

##### **LONG-TERM GOAL:**

- The Guidelines are an organic process of regular feedback and response.
- Continuous certification and decertification process.

##### **VVSG 2005 STOP-GAP RECOMMENDATIONS:**

- The Guidelines need to be implemented prior to 2008.
- Vulnerable systems certified to outdated standards should be reexamined.

#### **B. Opportunities For Administrative Improvement**

The current process of approving the Guidelines fails to adequately incorporate meaningful public comments. The compressed time schedule effectively denies the EAC from receiving valuable input from experts. At a minimum, there should be a second review of the 2005 Guidelines so that some semblance of a discourse can occur on these critical issues.

##### **LONG-TERM GOAL:**

- The process of updating and improving the Guidelines is open and accessible.

##### **VVSG 2005 STOP-GAP RECOMMENDATIONS:**

- The Guideline creation timeline needs to include a period for public comments to be addressed, understood and implemented.

### **VII. CONCLUSION**

Past elections have eroded public confidence in the trustworthiness, fairness and accuracy of voting systems and ultimately elections. It is imperative to restore public confidence. Voters and election-related jurisprudence demand that every vote has equal weight and each vote is counted. Voters deserve to cast their votes with equal dignity without regard to disability or language. Voting systems should accurately capture voter intent, be fully auditable, secure, and transparent enough to support meaningful public oversight.