ACCURATE

A CENTER FOR CORRECT, USABLE, RELIABLE, AUDITABLE, AND TRANSPARENT ELECTIONS

Public Comment on the 2005 Voluntary Voting System Guidelines

Submitted to the United States Election Assistance Commission

September 30, 2005

Prepared by the Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley

ACCURATE Principal Investigators

Aviel D. Rubin
ACCURATE Director
Department of Computer Science
Johns Hopkins University
rubin@cs.jhu.edu
http://www.cs.jhu.edu/~rubin/

Dan S. Wallach
ACCURATE Associate Director
Department of Computer Science
Rice University
dwallach@cs.rice.edu
http://www.cs.rice.edu/~dwallach/

Dan Boneh
Department of Computer Science
Stanford University
dabo@cs.stanford.edu
http://crypto.stanford.edu/~dabo/

Michael D. Byrne
Department of Psychology
Rice University
byrne@rice.edu
http://www.ruf.rice.edu/~byrne/

Drew Dean
Computer Science Laboratory
SRI International
ddean@csl.sri.com
http://www.csl.sri.com/users/ddean/

David L. Dill
Department of Computer Science
Stanford University
dill@cs.stanford.edu
http://verify.stanford.edu/dill/

Douglas W. Jones
Department of Computer Science
University of Iowa
jones@cs.uiowa.edu
http://www.cs.uiowa.edu/~jones/

Peter G. Neumann
Computer Science Laboratory
SRI International
neumann@csl.sri.com
http://www.csl.sri.com/users/neumann/neumann.html

Deirdre K. Mulligan
School of Law
University of California, Berkeley
dmulligan@law.berkeley.edu
http://www.law.berkeley.edu/faculty/profiles/facultyProfile.php?facID=1018

David A. Wagner
Department of Computer Science
University of California, Berkeley
daw@cs.berkeley.edu
http://www.cs.berkeley.edu/~daw/

ACCURATE Affiliates also endorsing this Comment

Robert Kibrick, Legislative Analyst, the Verified Voting Foundation
Kim Alexander, President & Founder, California Voter Foundation
Cindy Cohn, Legal Director, and **Matt Zimmerman**, Staff Attorney, Electronic Frontier Foundation

PUBLIC COMMENT OF ACCURATE

ON THE

2005 VOLUNTARY VOTING SYSTEM GUIDELINES

TABLE OF CONTENTS

PUBLIC COMMENT OF ACCURATE

ON THE

2005 VOLUNTARY VOTING SYSTEM GUIDELINES

PREFACE

A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE),[1] a multi-institution, interdisciplinary, academic research project funded by the National Science Foundation's (NSF) "CyberTrust Program,"[2] is pleased to provide these comments on the Voluntary Voting System Guidelines (the Guidelines) to the Election Assistance Commission (EAC). ACCURATE was established to improve election technology. ACCURATE is conducting research aimed at investigating software architecture, tamper-resistant hardware, cryptographic protocols and verification systems as applied to electronic voting systems. Additionally, ACCURATE is evaluating system usability and how public policy, in combination with technology, can better safeguard voting nationwide.

With experts in computer security, usability, and technology policy, and knowledge of election technology, procedure, law and practice, ACCURATE is uniquely positioned to provide helpful guidance to the EAC as it attempts to strengthen the specifications and requirements entrusted with ensuring the functionality, accessibility, security, privacy and equality of the machinery of our democracy.

We welcome this opportunity to assist the EAC and hope this process marks the beginning of collaboration between the EAC and independent, academic experts that will vastly improve election systems and their use.

[1] http://accurate-voting.org/
[2] National Science Foundation Directorate for Computer & Information Science & Engineering, Cyber Trust, *at* http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=13451&org=CISE.

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. As past elections and past standards amply illustrate, the distillation of these broad core democratic values into workable voting system requirements that can be effectively evaluated is a complicated, continuous process. 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

We recognize the complicated nature of this task and are pleased to have the support of the National Science Foundation, allowing us to turn our intellectual and institutional resources to efforts such as assisting the EAC in meeting this challenge.

ACCURATE's comments provide several levels of advice and direction to the EAC. 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. The Appendix provides a detailed chart capturing our recommendations as well as section-specific changes to the Guidelines.

II. ESTABLISHING A SOUND FRAMEWORK FOR VOTING SYSTEM ASSESSMENT

We commend the EAC's candid acknowledgement of the past failures of the 1990 and 2002 voting standards and the broader focus of the proposed 2005 Guidelines on the "critical topics of accessibility, usability, and security."[3] However, 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. Secure, private, usable, accessible and equitable voting systems are only possible through a transparent process that embraces a systems perspective, discipline-specific approaches to certification and evaluation, and updates and applies guidelines that respond to known vulnerabilities at reasonable intervals. Our recommendations are aimed at producing such a process.

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

To support meaningful government and public oversight of elections, the process of developing the Guidelines and, to an even greater degree, 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.[4] The EAC must address this issue on several fronts. Formalizing and regularizing the development of the Guidelines—for example, by bringing the process in line with standard administrative procedures such as Notices of Proposed Rule Making (NPRM)—is an important step. Furthermore, the process must incorporate a

[3] Voluntary Voting System Guidelines Overview, Volume I, at 1 (June 2005), *available at* http://guidelines.kennesaw.edu/vvsg/vg1/docs/VVSG_overview.pdf.
[4] *See, e.g.*, *Electronic Voting: An Overview of the Problem, Before the Commission on Federal Election Reform (Carter-Baker Commission)* (April 18, 2005) (testimony of David L. Dill), *available at* http://www.american.edu/ia/cfer/0418test/dill.pdf; *Voting System and Transparency: The Need for Standard Models, Hearing on Transparency and Security Before the U.S. Election Assistance Commission Technical Guidelines Development Committee* (Sept. 20, 2004) (submission of Douglas W. Jones), *available at* http://www.cs.uiowa.edu/%7Ejones/voting/nist2004.shtml.

meaningful period for public comment. The EAC should actively seek involvement of experts from relevant disciplines. Keeping the public apprised of the opportunity to participate in the Guidelines' creation and modification will facilitate transparency and bolster public confidence.

The EAC must also facilitate greater government and public oversight of the testing and certification processes. Paper-based voting systems, with all their inefficiencies, are largely transparent to the average voter and election official. Because proprietary electronic systems hide these previously transparent functions of our election process, ensuring the integrity of the voting process requires that mechanisms be established to provide election officials and the public the information necessary to independently evaluate voting systems. To provide for such oversight, 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.[5] Furthermore, Independent Testing Authorities should not be paid or selected by the vendors whose systems they are testing. A new model for funding must be developed and implemented.

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

The EAC seeks to instill diverse values, such as security and usability, into America's voting systems. However, while the Guidelines set out specifications related to unique subjects, the approach to requirements and evaluation in each category is deeply rooted in the EAC's initial focus on testing for system functionality and feature existence.

To successfully deliver systems that incorporate the different values that currently comprise the EAC's charge, the Guidelines must appreciate the requirements and evaluation needs of each value and the methods used by professionals to assess such qualities in other contexts. For example, security and system functionality dictate different requirements and

[5] In the one instance where independent security experts evaluated the security of a voting system, serious flaws were discovered. Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, *Analysis of an Electronic Voting System*, IEEE SYMPOSIUM ON SECURITY AND PRIVACY 2004,(2004), *available at* http://avirubin.com/vote.pdf.

require completely different forms of evaluation.[6] Functionality relates to whether or not something works when it is used as planned.[7] Functionality can be tested, and the tests can be used to make predictions about the future behavior of a system.[8] Security, on the other hand, has to do with how a system behaves under unanticipated circumstances, for example when an active, dynamic adversary, possibly with inside information, tries to compromise it.[9] By definition, one cannot evaluate a system for security the way one tests for functionality or feature existence. Functionality concerns the presence of a desired behavior; security concerns the absence of undesired behavior. Tests designed to confirm functionality are inadequate tools to establish the absence of functionality, which is the cornerstone of security evaluation. Further, one cannot draw conclusions about the security of a system based on its past performance. Just because adversaries have so far refrained from attacking a system is no guarantee they will continue to so refrain.

Critical system security evaluation—as implemented in academia, industry, and government—always includes adversarial analysis.[10] 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. In sum, the Guidelines as proposed are unable to provide any assurance of security because their security evaluation process will not work. The functional testing focus of the Guidelines, combined with the structural setup of the parties involved and the technical methodologies prescribed, is essentially useless for evaluating security.

Similarly, usability and its subset accessibility cannot be achieved through functional testing alone.[11] The state of the art in this field relies upon, for example, user-centered design,

---

[6] *Testimony Before the U.S. Election Assistance Commission Public Hearing on the Use, Security and Reliability of Electronic Voting Systems*, 3-4 (May 5, 2004) (testimony of Aviel D. Rubin), *available at* http://www.eac.gov/docs/Testimony%20-%20Avi%20Rubin.pdf.
[7] *Id*.
[8] *Id*.
[9] *Id*.
[10] The EAC's own Technical Guideline Development Committee adopted resolution #17-05 in January, 2005, proposing adversarial analysis. *See* http://vote.nist.gov/adopted_resolutions%202004-05.pdf.
[11] *See, e.g.*, Sharon J. Laskowski, Marguerite Autry, John Cugini, William Killam, James Yen, *Improving the Usability and Accessibility of Voting Systems and Products,* NIST Special Publication 500-256 (2004), *available at* http://vote.nist.gov/Final%20Human%20Factors%20Report%20%205-04.pdf.

heuristic testing by usability and accessibility experts and user testing—in this case by actual voters. 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. The need for user testing is heightened by the concerns raised by past election experience and independent research that suggests correlations between usability and disenfranchisement along lines of race and class.[12]

To date the Guidelines have not addressed the principle of equality—that every vote be counted and have equal weight. The Election Assistance Commission must recognize the importance of developing guidelines that embrace this core value of democracy. Translating the principle of equality into workable requirements and identifying appropriate evaluation schemes is an area of ACCURATE's research. Ensuring the usability of systems for various populations is a core component of this agenda. We look forward to providing the EAC with research and recommendations on this crucial issue.

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. The Guidelines must include procedures whereby election administrators and poll workers (or another impartial entity with appropriate expertise) are required to collect performance data from the field. For example, polling places should include log books in which poll workers record all failures, glitches and other anomalies.[13]

---

[12] *See* Michael Tomz and Robert P. Van Houweling, *How Does Voting Equipment Affect the Racial Gap in Voided Ballots?* 47 AM. J. OF POL. SCI. 46, 46 (2003), *available at* http://www.stanford.edu/~tomz/pubs/ajps03.pdf (analyzing the evidence that votes cast by black voters are rejected more often than those cast by white voters and concluding that the root cause of this racial gap is voting equipment used). *See also* Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1771, 1727 n.107-08 (2005).

[13] The recently released Carter-Baker federal election reform report makes such a recommendation. *See* Confidence in U.S. Elections, Report of the Commission on Federal Election Reform (hereinafter Carter-Baker), Sept. 2005, at 57, *available at* http://www.american.edu/ia/cfer/report/full_report.pdf.

Incident reports from the field contain valuable performance-related data that vendors and testing labs should be eager to understand and act on to improve systems. For example, the vast majority of voting systems used in the 2000 and 2004 general elections were certified to 1990 standards.[14] The absence of specific guidance on several issues resulted in avoidable failures.[15] Information regarding these types of failures should be fed back into the standards-setting process.

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. Recertification or recall of offending equipment should flow from the analysis of field data.

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.[16] Such data can illuminate issues with equality between voting systems. Evaluation procedures and certification standards that do not take into account problems experienced in the field are ultimately short-sighted and will not serve to efficiently improve voting systems. If reported problems are addressed and understood, the results can be fed back into the processes of certification and recertification so that evaluation procedures can be redesigned to minimize the chance that defective systems will be used repeatedly in the field. Such improved evaluation protocols can be incorporated into subsequent voting standards, resulting in voting systems that continually improve. In other problem areas,

---

[14] *See generally,* NASED Qualified Voting Systems, 12/05/03-Current, Aug. 30, 2005*, at* http://www.nased.org/ITA%20Information/NASEDQualifiedVotingSystems12-03-9-05.pdf.

[15] *See, e.g.,* John Schwartz, *The 2004 Election: Voting Machines; Glitch Found in Ohio Counting*, N.Y. TIMES, Nov. 12, 2001, at A12 (reporting that in Franklin County, Ohio in November 2004, an electronic voting machine injected an additional 3,893 votes to President Bush's tally in a precinct with just over 800 voters). *See also More Than 4,500 North Carolina Votes Lost Because of Mistake in Voting Machine Capacity,* USA TODAY, Nov. 4, 2004, *available at* http://www.usatoday.com/news/politicselections/vote2004/2004-11-04-votes-lost_x.htm (reporting that in Carteret County, North Carolina, over 4,500 votes were completely lost when the Unilect Patriot voting system could store only approximately 3,500 votes and over 8,000 voters used the system). Presumably, the failure in Carteret County would not have been caught by either 1990 or 2002 standards since it involved both poor error notification and the ability for a poll worker to reset the error condition.

[16] *See* Tomz and Van Houweling, *supra* note 12. *See also* United States Election Assistance Commission, *A Summary of the 2004 Election Day Survey, How We Voted: People, Ballots, & Polling Places*, Sept. 2005, *available at* http://eac.gov/election_survey_2004/pdf/EDS%20exec.%20summary.pdf; Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1763 (2005) (evidence shows that there are some intrastate racial disparities in the usage of voting equipment); *Id.* at 1726-27 (discussing evidence showing that blacks were "far more likely" to have their votes rejected than non-blacks) (citing Allan J. Lichtman, *Voting Irregularities During the 2000 Election*, Report on the Racial Impact of the Rejection of Ballots Cast in the 2000 Presidential Election in the State of Florida, U.S. Commission on Civil Rights, 2001).

such feedback loops are universally used and relied on for improving the performance and safety of a vast array of products and services, ranging from aviation to consumer products.

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 proposed Guidelines are only the third iteration of federal voting standards since their establishment.[17] Voting standards must be regularly updated as problems are identified and as technical capabilities improve. It is unacceptable that archaic and flawed systems are used in the most important aspect of our country's democratic process.

Along these lines, we acknowledge the existence of a draft of a National Institute of Standards and Technology (NIST) document, entitled VVSG Version 2, suggesting future changes to the Voluntary Voting System Guidelines.[18] That draft, scheduled to be presented to the EAC by late 2005 or early 2006,[19] may be moving in a direction consistent with this Comment. In addition, 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).[20] This effort by EAC is a good example of the analysis needed to identify and fill existing gaps in the standards. Without such gap analyses and correlated guidelines, poor standards will continue to undermine the integrity of our voting systems.

Unless the Guidelines remedy these deep structural flaws, they will not fully accomplish the EAC's stated goal— "to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility,

---

[17] The Federal Election Commission published the *Performance and Test Standards for Punchcard, Marksense and Direct Recording Electronic Voting Systems* in 1990. This was followed by the *Voting Systems Standards* in 2002. Voluntary Voting System Guidelines Overview, Volume I at 1 (June 2005), *available at* http://guidelines.kennesaw.edu/vvsg/vg1/docs/VVSG_overview.pdf.

[18] *See* Voluntary Voting System Guidelines Version 2, Draft (April 13, 2005), *available at* http://www.vote.nist.gov/VVSG2%20final.pdf.

[19] *See* Fact Sheets from NIST *at* http://www.nist.gov/public_affairs/factsheet/voting_symposium.htm (last updated June 2005).

[20] How To Determine If A Voting System Is Compliant With Section 301(a)—A Gap Analysis Between 2002 Voting System Standards And The Requirements of Section 301(a), EAC Advisory 2005-04, United States Election Assistance Commission ,(July 20, 2005), *available at* http://www.eac.gov/docs/EAC%20Advisory%2005-004%20(%204%20page%20fit%20).pdf.

and security capabilities required of voting systems"[21]— nor succeed in translating the broader set of values of security, privacy, transparency, usability, accessibility and equality required by our democratic ideals into our voting systems.

OVERVIEW OF THE GUIDELINES' FOUR CENTRAL STRUCTURAL LIMITATIONS

1) The process of establishing Guidelines and certifying and evaluating systems must be transparent.
2) The Guidelines must move away from functional testing and embrace a more sophisticated, discipline-specific, performance evaluation.
3) The Guidelines must take a systems approach that is informed by and responds to data about equipment failures, inequalities and other problems experienced at the polling place.
4) The establishment of Guidelines must become a process of continual improvement and timely adherence to updated Guidelines must be demanded.

[21] Notice of Proposed Voluntary Voting System Guidelines and Request for Comments, United States Election Assistance Commission 70 Fed. Reg. 124 (June 29, 2005).

III. TRANSPARENCY AND PUBLIC OVERSIGHT

The process for establishing voting technology must be reformed to provide transparency. Transparency is the extent to which the process and technology used in elections is open for inspection by members of the public, no matter what their situation or background. 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. Secretaries of State, elected officials, parties, candidates, and the general public must be able to assess, at some level, and validate the trustworthiness of voting systems. Thus, a core goal of the 2005 Guidelines and future voting standards should be to encourage transparency.

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.[22] Certification reports that indicate only whether a system passed are inadequate.[23] For example, four major studies by leading computer security experts documented the failures of current DRE systems that were previously certified.[24] 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. Voter confidence cannot be sustained by hiding

[22] Deirdre Mulligan & Joseph Lorenzo Hall, *Preliminary Analysis of E-Voting Problems Highlights Need For Heightened Standards and Testing,* Submission to the National Research Council of the National Academies (2004), at 7, *available at* http://www7.nationalacademies.org/cstb/project_evoting_mulligan.pdf) (stating the certification process is completely closed to the public and other third parties, there is no indication as to what specific tests are conducted to verify that a system fulfills the standards and there is no publication of problems encountered during testing).

[23] *Id*. (Currently, testing results from the Independent Testing Authorities provide a qualification report to the National Association of State Election Directors (NASED) and the Election Assistance Commission (EAC), which is the basis for being "NASED qualified").

[24] *See, e.g*., RABA Innovative Solution Cell, Trusted Agent Report: Diebold AccuVote-TS Voting System, Jan. 20, 2004, at 15-22, *available at* http://corporate.raba.com/news/TA_Report_AccuVote.pdf ; Science Applications International Corporation, Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes, Sept. 2, 2003, at 12-15, *available at* http://www.dbm.maryland.gov/dbm_publishing/public_content/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf; Compuware Corporation, Direct Recording Electronic (DRE) Technical Security Assessment Report, Nov. 21, 2003, *available at* http://www.sos.state.oh.us/sos/hava/compuware112103.pdf; Kohno, *et al., supra* note 5, at 7 (Johns Hopkins University analysis of the flawed source code used in DRE machines).

problems from the voting public. This "veil of secrecy" encourages questions regarding tampering and errors. Voters must know that problems are being identified and addressed. Detailed information regarding a system's performance and the exact certification tests performed must be made available for inspection.

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

Currently, source code of voting systems is not generally available for public scrutiny—in particular, to examination by impartial expert analysts. 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, including system documentation, change logs, manuals, procedures, and training documents. The independent panel of experts should be tasked with producing a public report stating and justifying their conclusions as to the security and performance of a voting system. The panel must present convincing evidence that the voting system as a whole meets its requirements for security.[25]

[25] A lack of evidence of insecurity does not mean the system is secure.

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. Election officials must not certify, purchase, or deploy voting equipment until independent security reviewers are confident that the technology will function as required.

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. Despite vendors' push-back due to potential revelations of trade secrets, protecting vendors' intellectual property must be accomplished in ways other than by sacrificing election transparency.[26] For example, experts can review certification results and source code under protection of non-disclosure agreements. Copyrights and patents owned or licensed by vendors to protect their intellectual property would still be fully enforceable. The use of open source can discourage theft of trade secrets between voting equipment vendors as vendors will have to remove such secrets from their code base or agree to release any trade secret protection. It is accepted principle among computer security professionals that "security through obscurity" is neither secure nor obscure.[27] As an illustration, portions of Diebold's source code were leaked onto the internet, despite attempts to keep it secret.[28] 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.

[26] *See* Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1771, 1794 (2005) (Vendors have claimed that their software is a trade secret and thus have guarded against any attempts to make their source code publicly available (citing Michael Ian Shamos, *Paper v. Electronic Voting Records – An Assessment* § 3.2 (April, 2004), *at* http://euro.ecom.cmu/people/faculty/mshamos/paper.htm).)
[27] *See* Wikipedia: The Free Encyclopedia, *available at* http://en.wikipedia.org/wiki/Security_through_obscurity (last accessed Sept. 28 2005). *See also* Tokaji, *supra* note 26, at 1794 (Stringent limitations on access to source code severely diminishes the opportunity to expose vulnerabilities or malfeasance (citing Eric A. Fischer, Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues, Congressional Research Service Report for Congress, Order Code RL 32139 at 26 (Nov. 4, 2003)).)
[28] *See* Kohno, *et al., supra* note 5, at 7.

IV. SYSTEM ASSESSMENTS THAT DELIVER ENHANCED SECURITY

A. Building Security Into Voting Systems

To substantially improve system security, the 2005 Guidelines must fully redesign the security evaluation process. 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.[29] A system is functional when it works while being used as planned.[30] Functionality can be tested and the tests can be used to make predictions about the future behavior of a system.[31] Security, on the other hand, has to do with how a system behaves under unanticipated circumstances.[32] By definition, one cannot evaluate a system for security in the same manner used to test for functionality.[33] It is incorrect to draw conclusions about the security of a system based on its past functional performance.[34]

The reliance on functional testing has allowed voting systems certified to 1990 and 2002 standards to enter the field with numerous security and integrity problems.[35] Failures in certified systems have clearly illustrated that the testing procedures specified by the prior standards have been woefully inadequate, as have the standards themselves (e.g., substantively incomplete). 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,[36] after the same feature was criticized by researchers at the University of Iowa almost ten years ago.[37] This fundamental security flaw was never caught in certification testing by ITAs.[38]

The completion of a checklist of functional tests alone will not result in a secure system. For example, in Volume I, Section 2.2.1 (Security), a list of items or tasks is provided "to

---

[29] *See* Rubin, *supra* note 6.
[30] *Id*.
[31] *Id*.
[32] *Id*.
[33] *Id*.
[34] *Id*.
[35] *See* Mulligan & Hall, *supra* note 22, at 3-5.
[36] *See* Kohno, *et al., supra* note 5, at 14-15.
[37] *See Problems with Voting Systems and the Applicable Standards: Hearing on Improving Voting Standards Before the U.S. House of Representatives' Committee on Science*, 107th Cong. (May 22, 2001) (testimony of Douglas W. Jones), *available at* http://www.cs.uiowa.edu/~jones/voting/congress.html; D.W. Jones, *The Case of the Diebold FTP Site* (2003), *available at* http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html.
[38] *See* D.W. Jones, The Diebold AccuVote TS Should Be Decertified and What This Tells Us About the Certification Process, presented at the Usenex Security Symposium, Washington, D.C.(Aug. 6, 2003), *available at* http://www.cs.uiowa.edu/~jones/voting/dieboldusenix.html (stating that the Diebold AccuVote TS system had passed tests imposed Voting System Standards promulgated by the Federal Election Commission many times).

ensure" system security. Many of the terms in this list are not well-defined, and isolated performance of each task cannot possibly "ensure" system security. Further, in Volume I, Section 6.4.5, the requirements for registering and checking software are described. Registering and checking a software package do not in any way demonstrate that the software can be trusted. Similarly, in Volume II, Section 5, software testing is reduced to requirements regarding the construction of the code, rather than the substance of the code.

The proposed 2005 Guidelines do little to address many known problems and inappropriately rely on functional testing.[39] We urge the EAC to move toward more appropriate evaluation schemes and ensure that guidelines are designed to eliminate or mitigate known problems.

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 that will be promulgated by the proposed Guidelines results in a simple pass/fail determination. The analysis lacks threat analysis, code review and penetration testing. Without these features it is all but certain that security will not be an integral part of the engineering and development process.

Moving forward, an overall security evaluation of a voting system must be required and some threshold criteria for passing determined. Functional testing alone, without threat analysis, code review, architectural analysis and penetration testing, will result in fundamentally insecure systems.

1. Threat Assessment

Reorienting security certification and evaluation should be a core goal of the Guidelines. In order to engineer security, the adversaries' capabilities need to be defined so that security requirements can be set to prevail against those capabilities. 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.

[39] *See supra* note 24.

In practice, when data is corrupted, it may be impossible to discern whether the error was caused by a malicious act or malfunction. 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, for example, where a bug caused a vote for one choice to be misinterpreted or misrecorded as a vote for a different choice. Each form of compromise must be analyzed and reduced so that security requirements and evaluation can be designed to test resilience against such attacks.

For security threat assessment, the burden of proof should be on the vendors. First, requirements for all voting systems need to be established. These requirements, most likely supplied by NIST or another independent entity that can assemble a representative group of experts, should specify the properties the system must provide, the threats it must tolerate, and the level of assurance required. 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.

One example of a scheme where the burden of proof is on the vendor to prove the system is secure, rather than on the evaluation lab to prove it insecure, is the Common Criteria Evaluation and Validation Scheme currently being developed by NIST and the National Security Agency (NSA) under the National Information Assurance Partnership (NIAP).[40] The Common Criteria scheme proposes to evaluate the security of a system on several axes representing performance criteria. However, 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.[41] The voting standards-setting body, assisted by security experts, could set a requirement for a minimum rating for each axis (i.e., performance criterion) and vendors would be required to demonstrate that their system can meet at least that rating. If a vendor can show a superior rating on any axis for a system, that vendor's system would be at a competitive

[40] *See* The Common Criteria Evaluation and Validation Scheme *at* http://niap.nist.gov/cc-scheme/aboutus.html. *See also* Poorvi L. Vora, Benjamin Adida, Ren Bucholz, David Chaum, David L. Dill, David Jefferson, Douglas W. Jones, William Lattin, Aviel D. Rubin, Michael I. Shamos, and Moti Yung, *Evaluation of Voting Systems*, 47(11) COMM. OF THE ACM 144 (November, 2004).

[41] *See* The Common Criteria Evaluation and Validation Scheme, Frequently Asked Questions, *at* http://niap.nist.gov/cc-scheme/faqs.html#eval-product-faq (stating that vendors ("sponsors") specify a security target and select a CCTL (Common Criteria Testing Laboratory).

advantage. Thus, such a rating system fosters innovation and provides incentives for vendors to improve various security features, rather than to simply achieve a "pass" rating.

2. Code Review

Voting systems must be subject to independent security reviews. Security experts have raised credible concerns about the security of today's electronic voting systems and their software.[42] For example, insiders, or those with insider-level access, can introduce malicious code. Software can contain unintentional vulnerabilities to tampering. 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 current testing performed by ITAs qualifies as neither purely independent nor effective review.

Dedicated systems should be used for voting, and all software on the system must be subject to security evaluation. 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.

Additional steps must be taken to ensure the integrity of voting code. States that have audited the use of code in voting systems have found that uncertified code is routinely used.[43] Uncertified code is another glaring gap in security. Thus, procedures are needed to ensure the integrity of voting code as it is stored, distributed, and loaded into voting machines. Requirements must be added to the standards to specify the source of code used and procedures for installing onto machines to ensure a chain of custody for that code. Periodic auditing of code running in voting machines and backend systems should be performed. In addition, backend

[42] *See supra* note 24.
[43] *See, e.g.,* Paul Boutin, *Is E-Voting Safe?* PC WORLD MAGAZINE, June, 2004, *available at* http://www.pcworld.com/news/article/0,aid,115608,00.asp; Kim Zetter, *E-Voting Undermined By Sloppiness*, WIRED NEWS, Dec. 17, 2003, *available at* http://www.wired.com/news/evote/0,2645,61637,00.htm (stating that an audit of Diebold voting systems in California revealed uncertified code in use in seventeen counties and stating that Diebold admitted wrongdoing related to these incidents).

vote-tallying should be executed on isolated machines that have never been used for other purposes.

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. To date only a few voting systems have been subject to such tests. Moving forward, penetration testing should be a routine part of voting system evaluation.[44]

It is imperative that a voting system have a high level of security that can be demonstrated to the voting public. 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. Currently, the Guidelines do not provide clear standards as to the level of security requirements. For example, in Volume I, Section 1.6.1 (National Certification Tests), the Guidelines provide: "Although some of the certification tests are based on those prescribed in the military standards, in most cases the test conditions are less stringent, reflecting commercial, rather than military, practice." Given that the integrity of our democracy is put at risk with an insecure voting system, the standards must demand security that is at least as effective as those used in the military and in industries where data integrity is mission critical.

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.

[44] *See, e.g.*, RABA Innovative Solution Cell, Trusted Agent Report: Diebold AccuVote-TS Voting System, Jan. 20, 2004, at 15-22, *available at* http://corporate.raba.com/news/TA_Report_AccuVote.pdf; Science Applications International Corporation, Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes, Sept. 2, 2003, at 12-15, *available at* http://www.dbm.maryland.gov/dbm_publishing/public_content/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf.

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[45]

Critical aspects of a secure system include the ability to audit the system and the requirement that the system's operation be transparent to voters. 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.[46] Section 301(a) of HAVA requires that all voting systems have an "audit capacity" and that they produce a "permanent paper record."[47] The 2005 Guidelines, in Volume I, Section 2.2.5, recognize that the maintenance of audit records reduces the chance of error. However, the auditability of systems must be enhanced and the Guidelines must insist on a higher level of performance and accuracy in the audit-trail capability of voting systems.

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. Privacy and secrecy concerns mandate that any audit system must not be linkable to who the actual voters

[45] We recognize that not every voter will check their ballot. Because of this fact, the term "voter-verifiable" may be a more concise description. Part of the research agenda for ACCURATE is to study ways in which to require or encourage voter verification of audit trails.
[46] Recently, the Commission on Federal Election Reform recommended that a VVPAT be required for all voting systems but neglected to recommend that the paper record be the official record of the vote and that random statistically sampled auditing of such records be performed. *See* Carter-Baker, *supra* note 13, at 27.
[47] 42 U.S.C. § 15481(a) (Supp. 2002).

were. However, voters must be able to verify with an indelible record at the time their vote is cast that their vote was cast as they intended. Otherwise, security cannot be assessed and the voting public has no rational basis on which to trust the voting system.

Lack of voter-verifiability is a central failure of most current DRE voting systems. In the current systems, when ballots are stored electronically, voters have no way of knowing whether their vote has been recorded correctly. With previous paper-based voting systems, a voter could inspect a fixed record, subject to no additional processing or manipulation except the separate act of counting, of her choices and verify its accuracy prior to casting the ballot. In today's purely electronic systems, there is no "fixed record" for voters to review, or for officials to review as a check against the system or in the case of a recount. 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.[48] There are systems available today that permit voter-verified elections. Optical scan systems allow voters to verify their ballots before casting. Voter verified paper audit trails can also be used with DRE machines. Ballot marking devices can be used to allow voters to use a touchscreen interface to select votes and then print out an inspectable paper ballot. In each of these solutions, voters can verify their vote and a permanent record is available for recount or auditing. As a result, voter-verified systems are innately far more secure than non-voter-verified systems.

In addressing the requirements for systems with VVPAT, the Guidelines fall short of providing standards for critical features of the audit trail. Even though the Guidelines include a new section establishing requirements for the currently optional Voting Verified Paper Audit Trail technology, Section 6.8, the term "Voting Verified Paper Audit Trail" or "VVPAT" is not clearly defined either the "Glossary" or in the "Definitions" section. Additionally, definitions for related terms, such as "voter-verified paper record" or "voter-verified paper ballot," that are routinely encountered in both enacted state and pending federal legislation cannot be found in the Guidelines. The lack of definitions in this area creates potential legal issues when determining the scope of technologies to which the requirements of Section 6.8 apply, as well as determining the applicability of the requirement in various states.

[48] Voter-verified paper audit trails are meant to encompass voter-verifiable ballots marked by the voter and voter-verified records that are printed out.

The use of a voter-verified paper audit trail requires the design of special procedures. 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. Once developed, procedures must be required so that the audit trail is used without fail in a manner that supports its role as auditor. These manual audits are essential for security as they provide the only means available to detect many kinds of electronic fraud. The Guidelines must also specify procedures in the instance of a mismatch between electronic and paper records. In some cases, a 100% manual recount may be required. The Guidelines include no procedures for handling such a discrepancy between VVPAT data and electronic data. (See Volume I, Section 6.8). The only requirement related to the reliability of printers to be used is the system-wide requirement that there be 163 hours mean time to failure (MTF), which is inadequate. 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. Such practices are routinely followed in accounting systems. The data management requirements set forth in Volume I, Section 3.2.8 also need to be strengthened to include audit logging and other methods to block malicious editing of audit logs.

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. End-to-end system evaluation is important to ensure that the voting system will operate as a whole. However, 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.

Because the Guidelines and their predecessor standards have no requirement for interoperability between systems or subsystems, system vendors have taken the position that their systems cannot be used to test others' software or hardware components.[49] As a result, there is no interoperability among competing systems, or among modular pieces that could be used in voting systems.[50] When vendors prohibit interoperability, states become locked-in to a particular vendor's equipment and unable to purchase updated or competing subsystems. The Guidelines need to ensure that barriers to a robust, competitive, innovative market are not built into the certification process.

Requiring interoperability across systems and between system components and subsystems can add to the security and transparency of voting systems. For example, by using modular pieces developed by different vendors in software and hardware, a system may be less vulnerable to malicious attack. Furthermore, interoperability fosters transparency since it will facilitate end-to-end testing of systems by independent outside experts. The Guidelines must include a requirement for open, standardized interfaces to enable interoperability. 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.

[49] For example, Diebold Election Systems, Inc. (DESI) recently sent a "Product Use Advisory" to various customers and a letter to Florida's Division of Elections that stated any use of a mixed system required prior written authorization from Diebold to protect their "proprietary interests." DESI "Product Use Advisory" and Letter dated July 11, 2005 from Ian S. Piper (Diebold Compliance Officer) to Paul Craft (Florida Division of Elections Chief of the Bureau of Voting Systems Certification) (on file with author). *See also* Kevin P. Connolly, *Volusia Vote-Machine Idea Runs Into Corporate Problem,* ORLANDO SENTINEL, Aug. 2, 2005, *available at* http://www.verifiedvotingfoundation.org/article.php?id=6253.

[50] For example, the Guidelines must require interoperability so that ballot scanning vendor X is required to make sufficient technical specifications for its ballot format available to ballot marking device vendor Y. Then vendor Y can ensure that its ballot marking devices do an adequate job of marking ballots that will be scanned by vendor X's ballot scanner.

E. Addressing Network Vulnerabilities

The transmission of data poses significant security risks. Data can be intercepted, lost, modified, corrupted, and the like. The security problems are magnified when a network is used to transmit data. Connecting voting machines to telecommunication systems, which has been done for many years, has recently been shown to be an extraordinarily dangerous practice.[51] In addition, the unchecked stream of security breaches of sensitive data at credit card companies, universities, and hospitals has shown that network technology today is largely insecure.[52]

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. Although the word "internet" does not appear in Volume I, except once in Appendix A, it is clear the authors of the Guidelines intend to open the door to internet voting without using the term. Internet voting should be banned for the foreseeable future because of massive vulnerabilities that have no easy resolution.[53] In addition, the possibility that a wireless connection be used, as allowed in Volume I, Section 6.7 must be removed. As is specifically admitted in Volume I, Section 6.7, wireless connections involve substantial risk. Therefore, their use cannot be tolerated. Overall, the standards must prohibit any connection of a voting system to networks that extend outside the polling place, including wireless networks, internet-connected networks, and networks connected to a public telephone system.

---

[51] *How to Hack an Election*, N.Y. TIMES, January 31, 2004, *available at* http://www.nytimes.com/2004/01/31/opinion/31SAT1.html (stating that when the state of Maryland hired experts to test Diebold AccuVote-TS machines, they were able to change cast votes remotely using a modem connected to the voting machine).

[52] *See* Privacy Rights Clearinghouse at http://www.privacyrights.org for a list of data breaches.

[53] For example, opportunities for undetectable coercion and vote selling remain problematic. This same risk applies to existing absentee ballots, and is thus not unique to Internet voting. Computer security experts have recently discredited internet voting entirely. David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner, *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*, Jan. 21, 2004, *available at* http://www.servesecurityreport.org/paper.pdf; David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner, *Analyzing Internet Voting Security; An Extensive Assessment Of A Proposed Internet-Based Voting System*, 47 COMM. OF THE ACM 59 (Oct. 2004), *available at* http://doi.acm.org/10.1145/1022594.1022624. The same risk applies to existing absentee ballots, and thus is not unique to internet voting.

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, Internet-connected networks, and networks connected to a public telephone system.

V. APPLYING A SYSTEMS PERSPECTIVE TO VOTING TECHNOLOGY

The previous 1990 and 2002 voting system qualification regimes focused on the machines as if they could be evaluated wholly separate from the conditions in which they are used.[54] 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. However, this approach should be extended to encompass many types of assessment into a voting systems evaluation approach. The Guidelines fall short of such a systems regime, conspicuously omitting voting systems' field data as performance feedback.

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. "Disenfranchisement by design" has been all too common.[55] The severity of this issue has been highlighted by recent elections, particularly since the 2000 Presidential election.[56] Usability problems are evident to the voter in the polling place. For example, during

[54] The 1990 and 2002 standards did not speak effectively to the issues of usability and auditability. United States General Accounting Office, *Elections: Status and Use of Federal Voting Equipment Standards*, GAO-02-52 (2001), at 11, *available at* http://ww.gao.gov/cgi-bin/getrpt?gao-02-52.

[55] Tokaji, *supra* note 26, at 1767, 1770 (There is unquestionably a racial gap that results from the use of at least some paper-based voting technologies. Also, the disabled are disenfranchised in that paper-based voting systems lack an audio capacity, thereby preventing people with visual impairments or those who cannot read from voting independently, and both punch-card and optical scan systems that require voters to hold an object to punch or mark the ballot prevent people with manual dexterity impairments from voting independently).

[56] *Id*. at 1727 (On November 18, 2001, the New York Times, Washington Post and Sun-Sentinel all released the results of their inquiries into the Florida election (citing Sally Kestin, *The Disenfranchised: Poor, Uneducated Rejected Most in 2000 Election*, SUN-SENTINEL, Nov. 18, 2001, at 1F; Dan Keating & John Mintz, *Florida Black Ballots Affected Most in 2000; Uncounted Votes Common, Survey Finds*, WASH. POST, Nov. 13, 2001, at

the 2004 Presidential election, voters repeatedly reported that upon reviewing their ballot before casting their vote, the votes had been misrecorded.[57] 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.[58] This was reported primarily with presidential votes "jumping" from candidate to candidate.[59] Vote jumping was also reported for non-presidential races.[60] Additionally, poll worker interaction with voting systems resulted in problems such as voting delays. For example, voters reported that voting was delayed during the 2004 elections for a considerable amount of time as poll workers brought an electronic voting machine out to a disabled person who could not enter the polling place.[61] This effectively stopped voting for all other voters in the precinct as there are procedural regulations that required a certain number of poll workers inside the polling place while voting is being conducted and two poll workers must accompany the DRE taken to the disabled person outside the polling place.[62]

While belated, we are pleased that the 2005 Guidelines address the challenges of human factors. (Volume I, Section 2.2.7) The Guidelines appropriately identify the ultimate goal of human factor assessment, stating that the requirements in Section 2.2.7 intend to "provide a voting system and voting environment that all voters can use comfortably, efficiently, and with justified confidence that they have cast their votes correctly."

However, the proposed 2005 Guidelines fall considerably short of delivering on this goal. The weaknesses of section 2.2.7 are especially problematic given that they will not go into effect until 2008.

1. Voting Systems Pose Complex Usability Issues

Usability focuses on the voter's interaction with the voting system. Voters need to be able to cast their intended votes without confusion, without error, and without losing confidence in the system itself. Voting is an intrinsically challenging human factors problem. Voting systems must be usable by citizens regardless of age, disability, education, socioeconomic status,

---

A3, Ford Fessenden, *Examining the Vote: The Patterns; Ballots Cast by Blacks and Older Voters W ere Tossed in Far Greater Numbers*, N.Y. TIMES, Nov. 12, 2001, at A17).
[57] Mulligan & Hall, *supra* note 22, at 11.
[58] Mulligan & Hall, *supra* note 22, at 11(citing election incident reports taken from the Election Incident Reporting System *at* https://voteprotect.org/epc/).
[59] *Id*. at 11-12.
[60] *Id.*
[61] *Id*. at 13.
[62] *Id*. at n. 69.

familiarity with computers, literacy level, native language, and the like. This fact makes the voting population one of the most diverse user populations anywhere. Adding to the complexity of the situation is that the user population has zero training with the voting system and voting occurs very infrequently. Further complicating the usability issue is the lack of a well-trained expert group of administrators.[63] Unlike other complex systems, 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. In fact, since the poll worker population draws heavily on the elderly, it may present a population with less relevant experience than the population as a whole.[64] Thus the human factors issues are complicated in all respects.

2. The Proper Framework For Usability Certification And Evaluation

The establishment of Guidelines to address human factors issues is a step toward recognizing that regulating voting systems requires us to consider the various needs and constraints of the individuals that interact with them. While recognizing the need for higher-level performance-based requirements, 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 2005 Guidelines must define the degree of usability that can be expected from the voting system. Because the voting system must be robust enough to perform effectively and successfully under voting conditions, the Guidelines must move away from the current reliance on functional testing and embrace a more sophisticated and nuanced evaluation regime that relies

[63] Tokaji, *supra* note 26, at 1787-88 (reports published in the wake of the 2000 election document that poll worker resources in many communities, especially urban ones, are stretched thin) (citing House Minority Caucus Report on Election Reform, *Revitalizing Our Nation's Election System* (2001)).

[64] *Id*. (Numerous reports since the 2000 elections have documented that the nation's polling places are dramatically understaffed, often by elderly poll workers. The addition of equipment that poll workers will have to deal with can be expected to complicate the election process). *See also* Whitney Quesenberg, *Oops! They Forgot the Usability: Elections as a Case Study*, UPA Voting and Usability Project (Oct. 26, 2004), at 6, *available at* http://www.wqusability.com/articles/oops-they-forgot-usability.pdf.

primarily on assessing performance against some metric of usability.[65]

The Guidelines must establish standards that ensure reliable casting of votes as a result of human interaction with the system. The design usability requirements set forth in Volume I, Section 2.2.7.3 propose to make human interaction straightforward - the voter indicates the intended votes, verifies the vote, can change the vote, and then officially casts the vote.

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.[66] No future voting system should allow the incidental casting of votes, incidental under-voting, over-voting, or any of the other inaccuracies that are products of the human/system interaction.[67] The usability problems of the past, which will likely still exist under the current 2005 Guidelines, must be eradicated by intensive testing under conditions close to those experienced during actual voting with a reasonably representative distribution of actual human voters.[68] For example, representatives across race, age, and class need to be included in the testing samples to ensure equality of voting systems. The 2005 Guidelines need to reflect this type and level of user testing.

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.

---

[65] For example, given the large number of system crashes in the past elections, the Guidelines should specify an acceptable crash rate, system capability contingencies if a crash occurs, and other standards that ensure security is not compromised during a crash, such as standards that do not tolerate lost votes.

[66] Sharon J. Laskowski & Whitney Quesenbery, *Putting People First: The Importance of User-Centered Design and Universal Usability to Voting Systems*, at 3, *available at* http://www7.nationalacademies.org/cstb/project_evoting_wq_sjl.pdf (stating that usability and the user experience should be the starting point for the design of any voting system).

[67] *See* Mulligan & Hall, *supra* note 22, n.65-67 (citing election incident reports taken from the Election Incident Reporting System, *at* https://voteprotect.org/epc/). *See generally* Whitney Quesenberg, *Oops! They Forgot the Usability: Elections as a Case Study*, UPA Voting and Usability Project , Oct. 26, 2004, *available at* http://www.wqusability.com/articles/oops-they-forgot-usability.pdf.

[68] *See* Whitney Quesenberg, *Defining a Summative Usability Test for Voting Systems: A Report From the UPA 2004 Workshop on Voting and Usability*, Sept. 2004, *available at* http://www.upassoc.org/upa_projects/voting_and_usability/documents/voting_summative_test.pdf (creating a fully-defined protocol for a summative usability test of a voting 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

The 2005 Guidelines need to ensure the opportunity for voters to vote independently and privately. 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.[69] This reliance leaves the voter vulnerable to intimidation and harassment that ultimately detracts from their voting rights.[70]

Accessibility

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.[71] The 2005 Guidelines assert that the requirements of Section 2.2.7.1 are "meant to make the voting system directly accessible to as many voters as possible." Despite the Guidelines promising intentions, they fail to clearly and effectively establish useable standards that voting systems can be evaluated against.

Precision is needed in many of the Guidelines' sections intended to accommodate voters with visual, hearing, speech or cognitive impairments and mobility or manual dexterity limitations. For example, Volume I, Section 2.2.7.1.2.1.3 states "All voting stations using paper

[69] *See* Tokaji, *supra* note 26, at 1769 (citing Michael Waterstone, *Civil Rights and the Administration of Elections—Toward Secret Ballots and Poling Place Access*, 8 J. GENDER RACE & JUST. 101, 107 (2004) (arguing that federal voting rights laws should be interpreted to protect the right of disabled citizens to vote "in the same manner as their fellow citizens")).
[70] *Id*.
[71] 42 U.S.C. § 15481(a) (Supp. 2002).

ballots should make provisions for voters with poor reading vision." The term "provisions" is left undefined and unquestionably too broad. Furthermore, whether a system meets the requirement set forth in this section cannot be evaluated. Another example is Volume I, Section 2.2.7.1.2.2.3.9, which states "[t]he audio system should allow voters to control, within reasonable limits, the rate of speech." Again, the requirement uses language that must be defined because changes in the rate of speech can also potentially change pitch. Changes in pitch are undesirable and the requirements should reflect that pitch changes are unacceptable. Overall, the term "reasonable limits" is undefined and is not amenable to system evaluation. Additionally, the Guidelines include visual contrast requirements in Volume I, Section 2.2.7.1.2.1.4, but omit audio minimum signal-to-noise ratio requirements. In the past, audio on DRE machines was difficult to understand because this ratio was too low. These are just a few examples of similar problems throughout the new sections of the Guidelines where precision is needed.

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. For example Volume I, Section 2.2.1.2.2.4 states, "if the normal procedure is to have voters initialize the activation of the ballot, the Acc-VS shall provide features that enable voters who are blind to perform this activation." While it is, of course, desirable that voters with disabilities vote in the same ways as other citizens without additional assistance, this may not always be possible. 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.

Limited English Proficiency

Section 203 of the Voting Rights Act of 1965 mandates alternative minority-language access.[72] The 2005 Guidelines merely scratch the surface of the need to accommodate non-English proficient voters. 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

[72] Under Section 203 of the Act, a community of one of the four covered language minority groups, "American Indian, Asian American, Alaskan Natives or of Spanish heritage," will qualify for bilingual voting assistance if more than 5% of the voting-age citizen population in a jurisdiction belong to a single language minority community and have limited English proficiency (LEP) OR where more than 10,000 voting-age citizens in a jurisdiction belong to a single language minority community and are limited English proficient AND the illiteracy rate of the citizens in the language minority group is higher than the national illiteracy rate. 42 U.S.C. § 1973aa-1a (2000).

independently and privately. Where the Guidelines do address the issue of non-English proficient voters, the language used is too broad or fails to tackle important distinctions.

For example, Volume I, Section 2.2.7.1.3 states that "for literate voters, the [Alternative Language Voting Station] shall provide printed or displayed instructions, messages, and ballots in their preferred language, consistent with state and Federal law." Here, the general reference to state and federal law is too broad and at a minimum should incorporate requirements established by the Voting Rights Act of 1965.[73] Furthermore, the Guidelines fail to address which languages must be supported, for example whether all twenty-eight languages currently included in the Voting Rights Act must be supported?[74] The Guidelines also fail to address standards for languages without a written form.

Overall, the 2005 Guidelines need to be more detailed, exact and specific in terms of accessibility to be effective. In their current state, crucial gaps exist, which will make the Guidelines fall short of effective implementation at the voting station.

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.

[73] *See* 42 U.S.C. § 1973aa-1a (2000), *supra* note 72.

[74] The most recent determinations of covered jurisdictions were determined by the Census Bureau on July 26, 2002. The 28 languages, as mandated by the Voting Rights Act, include Alaskan Native (Other), Aleut, American Indian (Other), American Indian (Unspecified), Apache, Athabascan, Central/South American Indian, Cheyenne, Chickasaw, Chinese, Choctaw, Eskimo, Filipino, Japanese, Korean, Navajo, Paiute, Pueblo, Seminole, Shoshone, Sioux, Spanish, Tohono O'dham, Ute, Vietnamese, Yaqui, Yuman, Zuni. 67, Fed. Reg. 144 (July 26, 2004), *available at* http://www.usdoj.gov/crt/voting/sec_203/203_notice.pdf.

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

Voting system technology must be informed by experiences in the field. Currently, the 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. Problems need to be investigated, understood, and then fed back into the processes of recertifying (at times recalling) existing systems and establishing the next set of Guidelines. Given the numerous incident reports during the past Presidential election, voters deserve accountability and proof that these failures will not continue to taint the voting process.[75] The large volume of incident reports indicates a clear need for some kind of recall or recertification process. Although the incident reports were given over to the EAC, there is no process in place to ensure that the EAC considers the data collected.

For example, 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. This practice is accepted and used in other industries where reliable performance of products is required, for example in the National Transportation Safety Board (NTSB), pharmaceutical industries, and even in the toy industries where safety is at issue.[76] The Guidelines need to similarly follow the public reporting policies of these industries and agencies.

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.[77] In addition, the

---

[75] Mulligan & Hall, *supra* note 22, at 11 (On November 2, 2004, over 2014 individual election incidents were reported, as part of the Election Incident Reporting System, that Election Protection Coalition volunteers classified as "machine-related" election incidents.).

[76] *See, e.g.,* "Reporting An Accident To The NTSB," *at* http://www.ntsb.gov/aviation/report.htm (Federal regulations require operators to notify the NTSB immediately of aviation accidents and certain incidents).

[77] Verified Voting Foundation, *Election 2004 E-voting Incidents from the Election Incident Reporting System (EIRS)* (Nov. 18, 2004), *at* http://www.verifiedvoting.org/article.php?id=5331. *See also* David Dill & Will Doherty, Electronic Voting Systems: A Report for the National Research Council by the Verified Voting Foundation, Nov. 22, 2004, *available at* http://www7.nationalacademies.org/cstb/project_evoting_vvf.pdf. Other efforts to collect information about voting incidents include the Common Cause hotline and the Election Sciences Institute "Voter Watch" online incident reporting service. *See* Press Release, Common Cause, *Common Cause Sponsoring Non-Partisan Voter Hotline, 1-866*-MYVOTE1 (Oct. 19, 2004), *available at* http://www.commoncause.org/site/apps/nl/content2.asp?c=dkLNK1MQIwG&b=194883&ct=261142; *See* Press

House Judiciary Committee received 57,000 complaints of election irregularities.[78] These problems were reported mainly by voters, and were primarily centered around the human-machine interface of the voting machines.[79] Problems included difficulties with casting ballots, such as miscasting of votes, inadvertent vote casting, and incomplete voting.[80] Other reported problems included machines crashing or displaying error messages, out-of-service equipment, and difficulties with or malfunctioning of specialized equipment serving the disabled.[81] 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.[82] Thus, even a cursory examination of field data gives investigators strong hints as to where to look to improve equipment to reduce problems with voting. Incident reports from the field provide valuable performance-based data that vendors and testing labs should be eager to understand and act on to improve systems. The voting standards must set up procedures whereby field data is reported and investigated, and problems are corrected in a transparent manner, for example by recertification or recall of offending equipment.

Further, 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.[83] These field data again identify critical information that must be fed back into the standards-setting process. Problems are reported with such voting systems frequently, despite being labeled "certified."[84] By allowing certification of equipment to outdated standards, error-prone equipment and poor technology continue to taint election results.

Release, Election Sciences Institute, *Web Site Delivers Live, Real-Time Reporting for Voting Problems* (Oct. 29 2002), *at* http://www.votewatch.us/media/press_releases/votewatch_2002_launch.pdf.

[78] Press Release, House Committee on the Judiciary, *Government Accountability Office to Conduct Investigation of 2004 Election Irregularities* (Nov. 23, 2004), *available at* http://www.house.gov/judiciary_democrats/gaoelectionjtpr112304.pdf).

[79] *See* Verified Voting Foundation, *Election 2004 E-voting Incidents from the Election Incident Reporting System (EIRS): Election Verification Project Press Conference* Nov. 18, 2004)*, "E-Voting Problems Reported," at* http://www.verifiedvoting.org/article.php?id=5331.

[80] *Id*.

[81] *Id*.

[82] Mulligan & Hall, *supra* note 22, at 11.

[83] *See supra* note 54, *Elections: Status and Use of Federal Voting Equipment Standards*, GAO-02-52 (2001), at 2, *available at* http://ww.gao.gov/cgi-bin/getrpt?gao-02-52.

[84] *See* Mulligan & Hall, *supra* note 22, at 11 (citing voters' reports of voting systems being "down" or "broken" from the Election Incident Reporting System, *at* https://voteprotect.org/epc/).

A number of fundamental technical gaps in the standards have been identified for both DRE and paper-based systems. For example, In Carteret County, North Carolina, voters continued to cast votes using a 1990-certified system whose memory was full during early voting in 2004. Over 4,500 votes were completely lost when the Unilect Patriot voting system used could store only approximately 3,500 votes and over 8,000 voters used the system.[85] The loss of votes could not have been prevented by functional testing nor by red team testing as the system nominally performed as designed but errors were not noticed or acted on by election workers.[86] The standards need to incorporate this type of collected field data and incapable or suspect systems need to be decertified or recalled.

Additionally, 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. For example, California recently began a parallel monitoring program in response to an Ad Hoc Touch Screen Task Force to study and make recommendations on possible improvement in the security of DRE voting equipment.[87] This type of auditing comes close to mimicking the conditions of actual voting.[88] As a result, parallel monitoring can help to expose malicious or poorly-designed code.[89]

Despite frequent failures associated with 1990-certified equipment, most systems in use today are certified to 1990 standards.[90] Although this excessive regulatory time lag for adoption of updated standards may be acceptable in slow-moving industries, it is not appropriate for voting systems of any kind, in particular computerized voting systems. Rather than being certified once and allowed to operate in accordance to outdated standards, voting systems must

---

[85] *See also More Than 4,500 North Carolina Votes Lost Because of Mistake in Voting Machine Capacity,* USA TODAY, Nov. 4, 2004, *available at* http://www.usatoday.com/news/politicselections/vote2004/2004-11-04-votes-lost_x.htm.

[86] Although the system displayed error messages, these messages were not obvious and were apparently cleared as the system reset with each new voter. The error messages went unnoticed by poll workers while about 4,500 voters tried to cast their votes. *See id. See also* Janette Pippin, *Warning Light Came On, State Tests Revealed*, JACKSONVILLE DAILY NEWS, Nov. 18, 2004, *available at* http://www.jdnews.com/SiteProcessor.cfm?Template=/GlobalTemplates/Details.cfm&StoryID=27422&Section=News.

[87] *See* California General Election Parallel Monitor Program Report of Findings, Nov. 30, 2004, *available at* http://www.ss.ca.gov/elections/november2004_pmp_report.pdf.

[88] *See id.* at 12.

[89] *Id.* at 6.

[90] *See supra* note *54*, *Elections: Status and Use of Federal Voting Equipment Standards*, GAO-02-52 (2001), at 2, *available at* http://ww.gao.gov/cgi-bin/getrpt?gao-02-52).

be designed such that they are reliable, long-lived systems that can be updated quickly in a modular manner and recertified as new standards are released. For example, although the U.S. still relies on military aircraft designed and built decades ago, outdated flight-deck instrumentation is swapped out and replaced regularly to make necessary improvements. Inadequate performance of certified systems in the field and improvements in available technology both dictate that the voting standards must be updated and implemented in a timely, regular fashion to ensure the integrity of future elections.

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. Embedded in data collected from the field is important information that can indicate inequalities between voting systems. 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. Field data that indicate such problems must be understood and addressed so that inequalities can be identified and eliminated. It is unacceptable to allow problems of this sort to go without response and corrective action. Given the large number of incidents of voting equipment malfunctions during recent years, including the past two Presidential elections, the standards must demand accountability and proof from vendors and testing labs that known equipment failures and inequalities will not continue to contaminate the voting process.

In addition, the Guidelines must reflect that the best practices and state-of-the-art tools are implemented as they become available. 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. The technology used in voting systems should at least mirror the technology available to consumers. In reality, voting systems should be a level beyond considering the stakes to the individual and to the democratic system as a whole.

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

Voting standards must be updated as problems are identified and as technical capabilities improve. The proposed 2005 Guidelines continue to propagate delays in implementing improved standards. As the Guidelines' "Overview" Section states, new standards will not be implemented until 2008 (24 months following formal approval).[91] Delaying implementation

[91] EAC proposes that the Guidelines become effective 24 months after final adoption, which is anticipated to take place in October 2005. *See* Voluntary Voting System Guidelines Overview, Volume I at 1 (June 2005), *available at* http://guidelines.kennesaw.edu/vvsg/vg1/docs/VVSG_overview.pdf. *See also* Election Assistance Commission News Release "EAC Releases Voluntary Voting System Guidelines for Public Comment," (June 27, 2005), *available at* http://www.eac.gov/news_062705.asp.

until 2008 perpetuates weak voting standards. The result of this timeline is that the majority of the systems in use will be certified to 2002 or 1990 standards. The problem is exacerbated with the 2005 Guidelines as they were intentionally meant to serve as "interim" standards and incorporate only minor changes from the 2002 VSS) so that they could be implemented by 2006. By allowing the use of systems certified to outdated standards, our voting system remains vulnerable. Errors and data corruption introduced by delay and "grandfather" policies are entirely preventable and must be eliminated.

We recommend moving to a continuous, ongoing certification and de-certification process. Instead of certifying a system once, systems should be periodically reexamined. A system should be decertified at any time if it is found not to meet currently accepted standards of security, privacy, reliability, accuracy, or transparency. 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 public hearings on the new 2005 Guidelines took place just three days after the Guidelines' release.[92] There is no period for reply comments as is allowed in other rulemaking contexts, which deprives the EAC of the well-developed and articulated input produced as entities with competing and complementary points of view engage with each others'

[92] On June 30, 2005 the EAC held a public meeting and public hearing on the proposed Voluntary Voting System Guidelines in New York. Information *available at* http://www.eac.gov/Public_Meeting_Public_Hearing_063005.asp.

comments.[93] The compressed time schedule effectively denies the EAC from receiving valuable input from experts. The process of approving of the Guidelines should be handled more like a Notice of Proposed Rule Making (NPRM).[94]

Furthermore, since the Guidelines are set to be approved in October 2005, the expedited timeline provides no opportunity for the comments created during the 90-day public comment period to be addressed, understood, and implemented. This process also effectively denies any realistic chance that the public can influence the creation of the standards. 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.

---

[93] At the conclusion of the 90 day public comment period and after the consideration of comments received, EAC commissioners will vote to approve the Voluntary Voting System Guidelines. The final version will be made available to the public at that time. *See* Voluntary Voting System Guidelines Introduction, Volume I, *available at* http://guidelines.kennesaw.edu/vvsg/intro.asp.

[94] The Notice of Proposed Rule Making is published in the Federal Register to notify the public of the proposed issuance of rules and regulations. The NPRM typically gives 60 days for public comment from any and all interested parties, and an additional 30 days for reply comments. Original comments may still be filed in the reply comments window. 5 U.S.C. § 551. The Federal Aviation Administration, Federal Communications Commission, National Telecommunications and Information Administration, and Environmental Protection Agency are examples of agencies that follow NPRM procedures.

To meet the EAC's objectives, and its mandate, the 2005 Guidelines must be substantially revised. We look forward to working with the EAC to revise these guidelines.

ACCURATE researchers are available to speak with the Election Assistance Commission. Please contact Aviel Rubin at (410) 516-8177 or Deirdre Mulligan at (510) 642-0499 for further information.

Submitted on behalf of ACCURATE and listed affiliates by:
Erica Brand, Law Clinic Intern
Cecilia Walsh, Law Clinic Intern
Joseph Lorenzo Hall, Ph.D. Student, School of Information Management & Systems
Deirdre K. Mulligan, Director, Samuelson Law, Technology & Public Policy Clinic, Boalt Hall School of Law, University of California, Berkeley

APPENDIX

The following is a table outlining section-specific comments to the proposed 2005 Voluntary Voting System Guidelines. The table is organized to mirror the preceding text. Where appropriate, recommendations for additional provisions to the Guidelines and modifications to existing provisions have been included.

III. TRANSPARENCY AND PUBLIC OVERSIGHT	
A. TRANSPARENCY IN CERTIFICATION **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.**	
SPECIFIC RECOMMENDATIONS:	
New Provision	Certification results regarding the system's performance must be made available to computer security experts and other members of the public.
New Provision	Independent Testing Authorities should not be paid or selected by the vendors whose systems they are testing.
B. SOURCE CODE TRANSPARENCY **Long-term Goal:** • **Open the certification process to public scrutiny and understanding.** • **Vendors must publish source code for public review.**	
SPECIFIC RECOMMENDATIONS:	
SPECIFIC RECOMMENDATIONS:	
New Provision	Security review of voting systems by outside panel of experts required.

New Provision	Source code and related information must available to review by independent experts.

IV. SYSTEM ASSESSMENTS THAT DELIVER ENHANCED SECURITY

A. BUILDING SECURITY INTO VOTING SYSTEMS

SPECIFIC RECOMMENDATIONS:

Security: **2.2.1**	A list of items or tasks is provided "to ensure" system security. Many of the terms in this list are not well-defined. Isolated performance of each task cannot possibly "ensure" system security.
Software Security: 6.4.5	The requirements for registering and checking software are described. Registering and checking a software package do not in any way demonstrate that the software can be trusted.

B. THE FRAMEWORK FOR SECURITY EVALUATION

Long-term Goals:

- **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 and parallel monitoring.**

SPECIFIC RECOMMENDATIONS:

New provision	Independent review of system security by panel of external experts with access comparable to that of fully-informed insiders.
New provision	Adversarial analysis as part of certification including threat assessment, security evaluation, code review, architectural review, penetration testing and parallel monitoring.
New provision	Decertification procedures for malfunctioning or incapable equipment.
Application of the Guidelines and Test	"Although some of the certification tests are based on those prescribed in the military standards, in most cases the test

Specifications: 1.6.1 (National Certification Tests)	conditions are less stringent, reflecting commercial, rather than military, practice." This provision is misleading and does not provide a clear standard that can be followed.
Scope: Exclusions: 4.1.3 and 5.2 (Design, Construction, and Maintenance Requirements)	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 manipulations of the underlying operating system. Dedicated systems should be used for voting, and all software on the system must be subject to testing.

C. THE QUEST FOR AUDITABILITY: AN INDELIBLE, INDEPENDENT, VOTER-VERIFIED AUDIT TRAIL MUST BE REQUIRED

Long-term Goals:

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

SPECIFIC RECOMMENDATIONS:	
New Provision	Indelible, independent, voter-verifiable audit trail required.
New Provision	A voter-verified audit trail should not be optional.
New Provision	Create procedures to manually recount the audit trail.
New Provision	Create standards for handling a discrepancy between audit data and electronic data.
New Provision	Software testing in Section 5 is currently reduced to requirements regarding the syntax of the code. The Guidelines must contain requirements for the substance of the code.
DRE System Requirements: 2.2.4.1	This provision requires that a permanent record of audit data be maintained, but it 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.
System Audit: 2.2.5	This provision recognizes that the maintenance of audit records reduces the chance of error. However, the auditability of

	systems must be enhanced and the Guidelines must insist on a higher level of performance and accuracy in the audit-trail capability of voting systems.
Performance Requirements: 3.2.8 (Vote Data Management Requirements)	The data management requirements set forth in this Section need to be strengthened to include secure audit logging and other methods to block malicious editing of audit logs.
Requirements for Voter Verified Paper Audit Trail (Optional) 6.8	Specific requirements related to the reliability of the printers to be used should be provided.
D. A CALL FOR INTEROPERABILITY **Long-term Goals:** • **System-system and system-subsystem interoperability**	
SPECIFIC RECOMMENDATIONS:	
New Provision	Requirement for open interfaces to enable interoperability.
E. ADDRESSING NETWORK VULNERABILITIES **Long-term Goals:** • **Networking capabilities included once security can be assured.**	
SPECIFIC RECOMMENDATIONS:	
Telecommunication Requirements: 5.0 [Also 6.5.4 (Telecommunications & Data]	All sections 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.
Wireless Requirements: 6.7	The possibility that a wireless connection be used, as permitted by this Section must be removed. Wireless connections involve risk and cannot be tolerated. The standards must prohibit any connection (hard wire or wireless) of a voting system to a

	network at all times.
V. APPLYING A SYSTEM PERSPECTIVE TO VOTING TECHNOLOGY	
A. THE HUMAN FACTORS CHALLENGE: USERS ARE AN INTEGRAL PART OF THE VOTING SYSTEM	
1. Voting Systems Pose Complex Usability Issues	
2. The Proper Framework For Usability Certification And Testing **Long-term Goals:** • **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.**	
SPECIFIC RECOMMENDATIONS:	
New Provision	Outreach to usability and accessibility experts to perform usability evaluation.
New Provision	Intensive testing under conditions close to those experienced during actual voting with a reasonably representative distribution of actual human voters.
3. Defining The Accessibility Requirements **Long-term Goals:** • **Maximize the opportunity for voters to vote independently and privately.**	
SPECIFIC RECOMMENDATIONS:	
New Provision	Include members of disabled populations in empirical research, in particular to verify vendors' claims of the accessibility benefits of electronic systems.
New Provision	Effective implementation requires clarity and precision in the definition of terms.
New Provision	For auditory interfaces which present a list of options, the user

	should receive a message when the end of the list is reached, indicating where they are. The message should state that "the end of the list has been reached and the next advance command will return to the beginning of the list." This avoids frustrating and time-consuming scrolling up a long auditory list.
New Provision	Displayed text should be presented in mixed case (as opposed to all-uppercase) as this is more legible.
New Provision	For DRE systems that allow users to use an inverse or negative video option to control contrast (e.g., white-on-black instead of black-on-white), the inverse video presentation should require a font change to a stroke width optimized for such presentation.
Human Factors: 2.2.7.1.2	"An Acc-VS shall provide accessibility to voters using their own personal assistive device." Examples should be provided. The provision needs a "Comment" that this may not always be possible as there are multiple hardware protocols for various assistive devices (e.g. PS2, USB), but that vendors should strive to accommodate as many as possible.
Human Factors: 2.2.7.1.2.1.3	"All voting stations using paper ballots should make provisions for voters with poor reading vision." The term "provisions" is undefined.
Human Factors: 2.2.7.1.2.1.4	Requirements must include minimum audio signal-to-noise ratio requirements. If this ratio is too low on DRE machines, the audio is difficult to understand.
Human Factors: 2.2.7.1.2.2.3.1	"The ATI shall provide its audio signal through ... a 3.5mm stereo headphone jack." There are two industry standards for headphone jacks: 3.5mm (also 1/8 inch) and 6.5mm (also 6.3mm or 1/4 inch). An adapter should be made available for those users with 1/4 inch connections.
Human Factors: 2.2.7.1.2.2.3.9	"The audio system should allow voters to control, within reasonable limits, the rate of speech." The term "reasonable limits" must be defined because changes in the rate of speech

	also can change pitch.
Human Factors: **2.2.7.1.3**	"For literate voters, the [Alternative Language Voting Station] shall provide printed or displayed instructions, messages, and ballots in their preferred language, consistent with state and Federal law." The general reference to state and federal law is too broad and at a minimum should incorporate requirements established by the Voting Rights Act of 1965.
Human Factors: **2.2.7.2.2.4**	"If the normal procedure is to have voters initialize the activation of the ballot, the Acc-VS shall provide features that enable voters who are blind to perform this activation." 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 make a machine more accessible to another class of individuals.
Human Factors: **2.2.7.5.4**	There are currently no guidelines addressing input method for DREs. The currently dominant forms are touchscreen, scroll wheel and older button-matrix machines. There are potential issues with touchscreen calibration and accuracy (e.g., misrecordings because of double-touching when the "off" hand is inadvertently rested on the edge of the touchscreen) which are not mentioned. There should be guidelines in place for users to report touchscreen miscalibration and for the complexity of the recalibration process.
B. FIELD DATA MUST PLAY AN INTEGRAL ROLE IN THE DEVELOPMENT OF GUIDELINES AND SYSTEM EVALUATION **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.**	
SPECIFIC RECOMMENDATIONS:	
New Provision	The Guidelines must include procedures whereby vendors,

	testing labs, and standards-setting bodies are required to collect and investigate performance data from the field and institute corrective actions in a transparent manner.
New Provision	Establish clear procedures for recertification or recall of offending equipment.

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

Long-term Goals:

- **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.**

Specific Recommendations:

New Provision	Use field data to identify and eliminate inequalities between voting systems.
New Provision	Continued collection and analysis of voting field data and correction of inequalities.

V. Needed Changes In Development Of The Guidelines

A. Unacceptable Results Of Delayed Implementation

Long-term Goals:

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

Specific Recommendations:

New Provision	The Guidelines need to be implemented prior to 2008.
New Provision	Vulnerable systems certified to outdated standards should be reexamined.
New Provision	Voting standards must be regularly updated as problems are identified and as technical capabilities improve.

B. Opportunities for Administrative Improvement

Long-term Goal: • **The process of updating and improving the Guidelines is open and accessible.**	
SPECIFIC RECOMMENDATIONS:	
New Provision	Active participation from experts from relevant disciplines should be actively sought.
New Provision	Formalize the development of the Guidelines—for example, by bringing the process in line with standard Notice of Proposed Rule Making (NPRM) administrative procedures.
New Provision	The Guideline creation timeline needs to include a period for public comments to be addressed, understood and implemented.