# Voluntary Voting System Guidelines Companion Document for the Election Official Community

## for the TGDC's

## VVSG Recommendations to the EAC of August 31, 2007

April 2008

# Table of Contents

# Chapter 1: Introduction

This document is an overview to the Voluntary Voting System Guidelines (VVSG) Recommendations to the Election Assistance Commission (EAC) of August 31, 2007, herein referred to simply as “the Recommendations.” This overview contains summary and background information about the Recommendations and summaries of its major topics.

## 1.1 Purpose and audience

The Recommendations are by nature technical and require readers to have some knowledge of voting system design, development, and testing procedures, as well as various aspects of election conduct. While the Recommendations are constructed primarily as a technical reference for voting system manufacturers and voting system test labs, the language used is intended to be accessible to all audiences without the loss of technical content.

The Recommendations are currently available from the Election Assistance Commission (EAC) for public review. So that election officials without a technical information technology (IT) background can better understand major topics and thus participate more effectively in the public review process, the EAC requested that staff at the National Institute of Standards and Technology create an overview of the Recommendations using less-technical language.

## 1.2 Scope

This companion document summarizes major topics from the VVSG Recommendations to the EAC of August 31, 2007, and no other version. It focuses primarily on those topics that are new or that represent significant changes from VVSG 2005. Many other aspects of the Recommendations are purposely not covered in this document as they were deemed to be less significant updates from material already in VVSG 2005. Members of the EAC’s Standards Board recommended the topics for this companion document.

While every effort has been made to ensure the information in this companion document is accurate, it should not be used as the sole basis for understanding any one aspect of the Recommendations. The Recommendations should be viewed as the authoritative document, and content conclusions should be drawn from that document only.

## 1.3 Structure

This companion document contains the following sections:

## 1.3 Structure

- Chapter 1, Introduction;
- Chapter 2, Introduction to the Recommendations;
- Chapter 3, Major human factors topics;
- Chapter 4, Major security topics; and
- Chapter 5, Major core requirements topics.

# Chapter 2: Introduction to the Recommendations

This chapter contains background on the Recommendations including an overview and executive summary, and how the Recommendations relate to previous voting standards.

## 2.1 What are the VVSG Recommendations?

The Recommendations are a new set of technical guidelines intended to make future voting systems more secure, reliable, and easier for voters and election officials to use, operate, and maintain. They include a detailed series of requirements that voting systems would have to meet by passing tests conducted by accredited voting system test labs. They were developed by the EAC's Technical Guidelines Development Committee (TGDC) working in conjunction with staff from the National Institute of Standards and Technology (NIST). Whereas NIST staff performed technical research and supported the TGDC, the TGDC made the final Recommendations. The VVSG Recommendations were submitted in a 598-page report to the EAC on September 4, 2007.

The Recommendations constitute a complete examination and rewrite of the VVSG 2005 guidelines proposed by the TGDC in May 2005 and adopted by the EAC in December 2005. Their development was conducted in an open and transparent process through a series of public meetings, numerous working teleconferences, the production of various TGDC resolutions, and white papers that laid out research for requirements.

This material is available in its entirety from:

- ♦ http://vote.nist.gov and
- ♦ http://vote.nist.gov/vvsg-report.htm (VVSG Recommendations in PDF, MS-Word, and HTML)

The EAC is conducting a series of public reviews of the Recommendations. More information can be obtained from the EAC at:

- ♦ http://www.eac.gov

The following sections present an executive summary of the Recommendations and describe the history of its development, the role of the TGDC, and the Recommendations' relationship to earlier versions of voting system standards.

## 2.2 What is contained in the Recommendations?

The Recommendations contain three volumes or “Parts” for different types of requirements and information:

**Part 1: Equipment Requirements**, contains requirements that apply to voting equipment. Part 1 contains eight chapters:

1. Overviews and changes from VVSG 2005;
2. Conformance-related information and requirements;
3. Usability, accessibility, and privacy requirements;
4. Auditing and records-related requirements;
5. Security-related requirements;
6. Core requirements;
7. Requirements arranged by voting activity; and
8. Reference models: process model, vote-capture device state model, and logic model.

**Part 2: Documentation Requirements**, contains documentation requirements that apply to the voting equipment as well as to manufacturers and test labs. Part 2 contains seven chapters:

1. Overviews and changes from VVSG 2005;
2. Manufacturer requirements for quality assurance and configuration management documentation provided to test labs;
3. Manufacturer requirements for documentation to be included in the Technical Data Package (TDP) provided to test labs;
4. Manufacturer requirements for voting equipment user documentation provided to users, i.e., customers (a copy of the voting equipment user documentation is included in the TDP);
5. Requirements for the voting system test plan by the test lab;
6. Requirements for the test report by the test lab; and
7. Requirements for test results-related documentation to be made available to the public in a Public Information Package (PIP).

**Part 3: Testing,** contains requirements applying to the conformity testing to be conducted by test labs. Requirements in Part 1 and Part 2 reference sections in Part 3 to indicate the general methods for how the requirements are to be tested. Part 3 contains five chapters:

1. Overviews and changes from VVSG 2005;
2. Overview of the conformity assessment process and related requirements;
3. Overview of general testing approaches;
4. Requirements for documentation and design reviews; and
5. Requirements for different methods for testing.

## 2.3 What are the major improvements?

The major changes and improvements are:

**Capability to audit voting system records independently from the voting system's programmed logic and conduct meaningful recounts:** Known as Software Independence, this requires that voting systems produce records in such a manner that they can be audited without the use of software to detect the possibility of fraud or error in the voting system's recording of votes. Currently this would require independent voter-verifiable records such as used in optical scan or Voter-verified Paper Audit Trail (VVPAT) systems; however, future systems could rely on emerging technologies.

**Improvements to voting system reliability and operation, and ease of use by poll workers:** Many requirements from VVSG 2005 have been clarified to ensure that voting systems will operate with greater reliability and integrity and have fewer failures or problems that could disrupt elections. There have been improvements to many basic software and mechanical workmanship requirements and improvements to the ways in which voting systems report vote totals and other election information.

**Improvements to ensure voting systems are easier to use for voters and accurately record the voter's intent:** Requirements for the usability of voting systems both for voters and poll workers have been updated from VVSG 2005 so that all voters, including those with disabilities or those requiring alternative languages, can vote more easily, accurately, and independently. New requirements to improve the readability, accuracy, and completeness of voting system documentation have been added. The Recommendations call for usability performance benchmark tests that permit vendors more freedom to design while still ensuring that test voters cast ballots accurately.

**Improvements to voting system security and to the integrity of voting system software and records:** Security-related requirements from VVSG 2005 have been updated and expanded to make voting systems more secure and, at the same time, easier to manage securely. Digital signature technology has been added (a) to ensure that only properly authorized voting system software can be loaded and run on voting systems, and (b) to protect the integrity of voting system records. At the tabulation center, election officials will be able to track voting system records to specific voting equipment and to reliably detect if voting records have been changed or are missing.

**Improvements to techniques for testing voting systems while constraining costs:** Voting systems will be tested according to various benchmark tests that set performance goals for reliability and accuracy based on data obtained from the National Association of State Election Directors (NASED). The testing will be combined to ensure complete coverage while at the same time holding down costs. An expert security review known as Open-Ended Vulnerability Testing will find problems not caught in other testing so that fielded systems remain secure.

Two other major improvements to the Recommendations are:

**An improved standards architecture:** The Recommendations have been reorganized to bring them in line with applicable standards practices of the International Organization for Standardization (ISO), the World Wide Web Consortium (W3C), and other standards-creating organizations. As voting systems likely change and new techniques emerge, the Recommendations will accommodate the addition of new types of voting devices or voting variations. The Recommendations will be easier and less expensive to maintain and periodically updated.

**Improved clarity in language and requirements:** The Recommendations make strict use of specific terminology so that manufacturers and testers will have a common understanding of requirements. The requirements are more precise than in previous versions, further reducing ambiguity. The Recommendations should reduce time wasted from misunderstandings or the potential need for interpretations.

## 2.4 What are the major benefits for election officials?

Election officials will benefit in a number of ways from the improvements represented by the Recommendations. Some of the major benefits that stem from these improvements are:

**There will be less voter confusion over voting system operation:** Voting systems will be easier to use, instructions will be more clear and easier to read, and voters will have more confidence that their ballots are being captured correctly.

**Voting system setup and operation will be easier:** Documentation for election officials will be of higher quality. The secure operation of voting systems will be simpler and potentially require fewer compensatory procedures. Poll workers will encounter fewer problems in setting up and operating voting systems.

**There will be fewer failures and equipment problems:** Equipment will be more reliable and if there are problems, recovery will be more manageable. Election Day problems as a result of equipment malfunctions will occur less often.

**Election reports will be more usable, precise, and complete:** Reports from voting equipment will contain more precise information that can be used more easily to reconcile and tabulate results. Digital signatures protect the integrity of the records. Records will be in a common format that will make them easier to aggregate.

**Audits have the capability to be more precise:** Audits will detect whether problems with the voting system have affected the accuracy of its records. Systems will be able to be meaningfully recounted. As a result, there should be fewer questions about the accuracy of elections and the need for recounts.

Ultimately, voting systems will be of higher quality, easier to use by voters, and easier to manage by election officials.

## 2.5 Cost issues

While the Recommendations were written to provide a secure foundation for the next generation of voting systems, efforts were made to hold changes to existing systems to only what the TGDC deemed minimally necessary. The improvements to security in the Recommendations were made to be consistent with standard accepted IT practices in government and industry. As much as was possible, cost was considered during the development of the Recommendations.

However, voting systems that are easier to use, that are more reliable and secure, and that are tested more rigorously will likely be more expensive. Some criticism has been levied that these improvements will make voting systems “too expensive” and that as a result, certain requirements in the Recommendations should be reconsidered. Some critics maintain that improved security requirements as well as the requirement for software independence are not justifiable without a rigorous cost-benefit analysis.

Such a cost-benefit analysis was outside of the scope of the TGDC’s effort to write the Recommendations. As well, no analyses to show that fewer improvements to security are warranted due to mitigations such as election procedures throughout the United States were available to the TGDC. To assist any future cost-benefits analysis, this document contains a high-level overview of threats and vulnerabilities to voting systems and pointers to where the addressing requirements reside in the Recommendations (see Section 4.5 of this document). Any future analysis of cost-benefit will also need to consider and quantify the many benefits and improvements for voters and to elections that these Recommendations represent.

## 2.6 When will tests for the Recommendations be ready?

NIST is currently developing tests for the requirements, and test development will continue into 2008 and 2009. These tests will be made available incrementally to test labs as they are completed. At the time the Recommendations are ultimately approved by the EAC, it is expected that test labs will have a complete set of tests.

## 2.7 History of the Recommendations

This section presents an overview of previous voting system standards efforts and the Help America Vote Act of 2002 (HAVA). It contains information about the role and membership of the TGDC, the development of VVSG 2005, and the justification for the subsequent development of the Recommendations.

### 2.7.1 Initial NIST involvement

In 1974, the National Bureau of Standards (now the National Institute of Standards and Technology) began a research project, funded by the Office of Federal Elections of the General Accounting Office. This project resulted in a 1975 NBS Interagency Report, later reprinted as NIST SP 500-30, *Effective Use of Computing Technology in Vote-Tallying*. The report provided findings and conclusions about improving the accuracy and security of the vote-tallying process, about improving the management of the election preparation process, and about institutional factors affecting accuracy and security. The report also pointed out the lack of systematic research on election equipment and systems, and on human engineering of voting equipment, and it concluded that the setting of national minimum standards for federal election procedures would serve a valuable function.

### 2.7.2 The 1990 VSS

In 1984, Congress appropriated funds for the Federal Election Commission (FEC) to develop voluntary national standards for computer-based voting systems. The FEC formally approved the Performance and Test Standards for Punchcard, Marksense and Direct Recording Electronic Voting Systems in January 1990, which became known as the 1990 Voting Systems Standard, or 1990 VSS.

The national testing effort was developed in 1994 and overseen by the National Association of State Election Directors (NASED) Voting Systems Board, which is composed of election officials and independent technical advisors. Many voting systems or components of voting systems have gone through the NASED testing and qualification process. In addition, many systems have subsequently been certified at the state level using the VSS in conjunction with functional and technical requirements developed by state and local policymakers to address the specific needs of their jurisdictions.

### 2.7.3 The 2002 VSS

As the qualification process matured and qualified systems were used in the field, the Voting Systems Board, in consultation with the test labs, identified certain testing issues that needed to be resolved. Moreover, rapid advancements in information and personal computer technologies introduced new voting system development and implementation scenarios not contemplated by the 1990 VSS.

In 1997, NASED briefed the FEC on the necessity for continued Commission involvement, citing the importance of keeping the VSS current in its reflection of modern and emerging technologies employed by voting system manufacturers. Following a requirements analysis released in 1999, the Commission authorized the Office of Election Administration to revise the VSS to reflect contemporary needs of the elections community. This resulted in the 2002 Voting System Standards, or 2002 VSS.

### 2.7.4 HAVA and VVSG 2005

In 2002, Congress passed the Help America Vote Act (HAVA), which created a new process for improving voluntary voting system guidelines. A new federal entity was created, the Election Assistance Commission (EAC), to oversee the process. The EAC established the Technical Guidelines Development Committee (TGDC) in accordance with the requirements of Section 221 of HAVA and according to the Federal Advisory Committee Act, 5 U.S.C. App. 2. The objectives and duties were to act in the public interest to assist the EAC in the development of the voluntary voting system guidelines. The membership, as defined by HAVA, includes:

- The Director of the National Institute of Standards and Technology (NIST) who serves as its chair;
- Two members of the EAC Standards Board;
- Two members of the EAC Board of Advisors;
- Two members of the Architectural and Transportation Barrier, and Compliance Board (U.S. Access Board);
- A representative of the American National Standards Institute (ANSI);
- A representative of the Institute of Electrical & Electronics Engineers (IEEE);
- Two representatives of the NASED selected by such Association who are not members of the Standards Board or Board of Advisors, and who are not of the same political party; and
- Four individuals with technical and scientific expertise relating to voting systems and voting equipment.

(See http://vote.nist.gov/tgdcmem.htm for a list of current TGDC members.)

The TGDC first met in July 2004. Operating as a federal advisory committee, the TGDC formed three working subcommittees:

1. Security and Transparency (STS);
2. Human Factors and Privacy (HFP); and
3. Core Requirements and Testing (CRT).

The three subcommittees researched and recommended requirements for adoption by the full Committee at public plenary sessions. The TGDC's initial set of Recommendations, VVSG 2005, augmented the 2002 VSS by including the following major updates:

- Improved conformance criteria and requirements structure;
- A glossary of terms;
- Security measures for software distribution and setup;
- Security measures for wireless communications;
- Improvements for the accessibility guidelines and usability design guidelines for voting systems; and

- Requirements for Voter-Verifiable Paper Audit Trail voting systems.

The VVSG 2005 was delivered to the EAC in May 2005, nine months after the formation of the TGDC as laid out by HAVA. It was adopted by the EAC after modifications, a public review, and subsequent updates by the EAC. The final version of the VVSG 2005 is located at:

- http://www.eac.gov/voting%20systems/voting-system-certification/2005-vvsg

### 2.7.5 The VVSG Recommendations to the EAC of August 31, 2007

The HAVA-mandated schedule for completing the initial updates to the 2002 VSS was extremely aggressive (nine months) and, as a result, the improvements made by the TGDC were incremental as opposed to comprehensive. The TGDC thus recommended that the VVSG 2005 be updated with a far-reaching guideline that would address in-depth security, performance-based guidelines for usability testing and an overhaul of the standards and test methods to meet the future's more rigorous needs for electronic voting systems. The Recommendations, the subject of this companion document, apply to the next generation of voting equipment and address those needs.

### 2.7.6 Relationship of HAVA and the Recommendations

Although both HAVA and the Recommendations contain requirements, the scope and application are quite different in the two cases. HAVA is a federal law that, among other things, provides to the states financial aid for the purchase of new voting equipment. In Section 301, it also sets forth broad functional *standards* for voting systems as used in federal elections. That is, it governs the systems as actually deployed in polling places throughout the country. Violation of these standards may result in adverse action by the Department of Justice against a state or other voting jurisdiction. The standards encompass procedures as well as equipment, e.g., the requirement that each state adopt a uniform definition of a "vote."

The Recommendations are a set of highly detailed technical requirements in support of the broad goals of HAVA. These requirements apply only to voting equipment, not to procedures in the polling place. If a *type* of voting system (i.e., a particular make and model) meets all of the Recommendations requirements (as determined by conformance testing conducted by an accredited laboratory), then that type is eligible to be *certified* as being compliant with the Recommendations. Thus the Recommendations are addressed to manufacturers of voting equipment, not to states. Finally, although many states will purchase only equipment that has been certified, the guidelines are *voluntary* in that states are free to purchase and use noncertified systems, as long as they comply with the HAVA standards.

**Table 2-1 Comparison of HAVA and the VVSG Recommendations**

| CHARACTERISTIC | HAVA | VVSG |
|---|---|---|
| Status | Federal Law | Federal Guidelines |
| Scope | Voting Systems and Procedures | Voting Equipment |
| Primary Audience | States | Equipment Manufacturers |
| Enforcement | Dept of Justice | EAC |
| Phase of Life Cycle | Procurement/Deployment | Conformance Testing |
| Level of Specification | Broad/Functional | Detailed/Technical |

# Chapter 3: Major HFP Topics

This chapter contains overviews of the major Human Factors and Privacy (HFP) topics in Part 1, Chapter 3 of the Recommendations. These are as follows:

- Usability performance requirements;
- Usability for poll workers;
- Alternative languages;
- Ballot casting notification;
- Privacy;
- Plain language;
- Legibility of paper;
- Timing issues;
- End-to-end accessibility throughout the voting session; and
- Accessibility of paper records;

The first three areas discussed represent significant upgrades from VVSG 2005.

## 3.1 Usability performance requirements

This section discusses new material in the Recommendations for measuring the usability of voting systems based on how accurately test voters cast ballots. This section starts with an overview of the types of requirements in the Recommendations so that readers can better understand the performance-related aspects of the usability requirements and tests.

**Table 3-1 Major HFP topics**

| HUMAN FACTORS TOPIC | DESCRIPTION |
|---|---|
| Usability performance requirements | New section to measure usability of voting systems using test subjects and measuring how accurately they cast ballots. |
| Usability for poll workers | Addresses usability for poll workers as well as for voters. Manufacturers are required to perform usability testing of system setup, operation, and shutdown.  System safety is addressed. |
| Alternative languages | This entire section has been expanded and clarified from VVSG 2005. |
| Ballot casting notification | Requirements to notify the voter whether the ballot has been cast successfully. |
| Privacy | Requirements to ensure privacy of ballot choices is preserved throughout the voting session and to ensure accessibility features or use of alternative |

| | |
|---|---|
| | languages also preserve privacy. |
| Plain language | Requirements for the use of plain language when the voting system communicates with the voter. The goal is to make the instructions for use of the system easier to understand and thus improve usability. |
| Legibility of paper | Legibility for voters with poor reading vision has been strengthened from a recommendation to a requirement. |
| Timing issues | Requirements on the timing for interactive systems. Addresses the response time of system to the user (no undue delay) and mandates that systems issue a warning if there is lengthy user inactivity. |
| End-to-end accessibility | New requirement to ensure accessibility throughout the entire voting session. |
| Accessibility of paper records | Requirements address the need for accessibility when the system uses paper records as the ballot or for verification. In particular, an audio readback mechanism is required to ensure accessibility for those with vision problems. |

### 3.1.2 What are performance requirements?

There are three kinds of requirements in the Recommendations:

1. **Design Requirements** specify something about the static structure of the system. For example, "Any control buttons on a voting system must be at least one inch apart."
2. **Functional Requirements** specify that the system is capable of performing a certain action. For example, "The system shall allow the voter to cast a straight party-line vote."
3. **Performance Requirements** specify not only that the system is capable of performing a certain action, but also sets a benchmark for how well it performs. For example, "The voting system shall provide visual feedback within one second when the voter makes or changes a choice within a contest."

While performance requirements have long been accepted for the “mechanical” aspects of system operation (e.g., maximum error rates for optical scanners), there has been a question whether such requirements could be applied to the usability of a voting system. Based on research, the TGDC believes that formulating usability performance requirements and the closely associated test procedures is both feasible and valuable. This section presents a broad description of the proposed approach to measuring usability performance. For a more detailed technical report on the Recommendations performance requirements, please see:

- http://vote.nist.gov/meeting-08172007/Usability-Benchmarks-081707.pdf

Generally, performance requirements for usability are preferable to design requirements because:

- First and foremost, performance requirements directly address the “bottom-line” usability properties of the system, such as how accurately voters can cast ballots, whereas design requirements do so only indirectly.

- Second, performance requirements are technology-independent – they provide impartial metrics of usability that are applicable across various types of voting systems: Direct Recording Electronic (DRE) systems, Electronic Ballot Markers (EBMs), Precinct Count Optical Scanners (PCOSs), etc.
- Finally, because they are technology-independent, the use of performance requirements allows voting system manufacturers to develop innovative interfaces without being overly constrained by design requirements.

### 3.1.3 Performance metrics

Usability is defined generally as a measure of the effectiveness, efficiency, and satisfaction achieved by a specified set of users with a given product in the performance of specified tasks. These three broad areas are interpreted as follows within the voting context.

First, effectiveness for voters is the ability to accurately record their intended choices. Second, efficiency is measured as the time taken to complete and cast the ballot. And finally, satisfaction is measured as the degree of confidence expressed by the voter. The TGDC has decided that only effectiveness metrics will be used as pass/fail criteria. Speed and confidence will be measured as part of the testing process, and the results will be reported, but there will be no actual performance requirements associated with them.

Effectiveness is itself further broken down into three subcomponents:

1. **Total Completion Score** – the proportion of users who successfully cast a ballot (whether or not the ballot contains erroneous votes). Failure to cast a ballot might involve problems such as a voter simply “giving up” during the voting session because of an inability to operate the system, or a mistaken belief that one has successfully operated the casting mechanism. Note that such a failure is very serious in that it voids all the votes cast by that voter.
2. **Perfect Ballot Index** – the ratio of the number of cast ballots containing no erroneous votes to the number of cast ballots containing one or more errors (either a vote for an unintended choice or a missing vote). The purpose of this metric is to catch systematic errors that affect a large number of voters, even if it causes them to make only one mistake each. E.g., if a particular contest were laid out in a confusing way, it might cause a large number of ballots to be “imperfect.”
3. **Voter Inclusion Index** – a measure of overall voting accuracy. Even if most voters cast a perfect ballot, it might be that the system presents serious difficulties for a certain number of voters who go on to commit a large number of errors.

The result of applying all three of these effectiveness metrics is that a voting system will pass the test only if a relatively small number of voters commit a relatively small number of errors.

### 3.1.4 Setting performance benchmarks

This last statement immediately raises the question of what constitutes “small.” In order to answer this question, NIST has been conducting experiments on a wide variety of voting systems to determine the typical range of performance. This research has elicited two important findings. First, one can indeed measure the performance of systems reliably. When one retests the same system, one gets (approximately) the same result. Second, the tests are sensitive enough to distinguish among various systems. Certain systems are consistently measured to be significantly more effective than others.

Based on the measured performance, the TGDC has proposed certain benchmarks (i.e., a pass/fail cutoff point) for performance. The rationale is that since some systems are capable of a given degree of effectiveness, it is reasonable to require that no system be significantly worse than this demonstrated level.

### 3.1.5 Purpose and interpretation of performance metrics

The performance requirements are supported by a precisely defined test procedure, namely the Voting Performance Protocol (VPP). One point needs to be emphasized: the purpose of the VPP is *to measure objectively the effect of the voting system on the performance metrics* described above. This implies that the VPP is to be a controlled experiment in which “everything else” is held constant, and the voting system itself is the only variable. “Everything else” includes:

- The demographic profile of the test participants;
- The instructions and tasks assigned to the participants (including whom to vote for);
- The logical structure of the test ballot (contests and candidates); and
- General environmental factors, such as lighting, ambient noise, etc.

The point, of course, is that by controlling other variables, one can confidently attribute differences in outcome to the only factor that does change between tests, namely the voting system being tested. Thus the VPP gives us a reasonably robust measure of the *relative performance* of various voting systems.

Note that the VPP is not designed for any of the following purposes:

- As a way to determine the effect of any factors other than the voting system on performance;
- As an open-ended assessment of the usability strengths and weaknesses of a given system;

- As a diagnostic tool to improve the design of the system being tested; or
- As a way to make “real-world” estimates about voter performance (speed, accuracy, etc.). While the particular scenario embodied by the VPP was chosen as typical of actual voting and to cover many common subtasks, it cannot represent the entire range of voting activities that arise throughout the country. Moreover, voters are not given a list of instructions to follow as they vote, whereas for testing one must specify the choices in order to measure the errors consistently.

The TGDC believes that the application of performance tests will be a powerful tool to promote the development of demonstrably more usable voting systems.

## 3.2 Usability for poll workers

The Recommendations address usability for poll workers more explicitly than past versions.

**Setup** includes all the steps necessary to take the system from its state as normally delivered to the polling place, to the state in which it is ready to record votes. It does not include ballot definition.

**Polling** includes such functions as:

- Voter identification and authorization;
- Preparing the system for the next voter;
- Assistance to voters who wish to change their ballots or need other help;
- System recovery in the case of voters who abandon the voting session without having cast a ballot; and
- Routine hardware operations, such as installing a new roll of paper.

**Shutdown** includes all the steps necessary to take the system from the state in which it is ready to record votes, to its normal completed state in which it has captured all the votes cast and the voting information cannot be further altered.

Since the details of these tasks are almost completely system-dependent, one can formulate only a general requirement for poll worker usability (3.2.8.1-A, Ease of normal operation). There are supplementary requirements, however, stipulating that:

1. Messages and documentation intended for poll workers must be reasonably easy to understand and provide clear direction (3.2.8-A and 3.2.8.1-C);
2. The equipment must be certified as safe to operate (3.2.8.2-A); and
3. The manufacturer must perform and report on usability tests for poll workers (3.2.8.1-B).

## 3.3 Alternative languages

Part 1, Section 3.2.7, on Alternative Languages has been considerably enhanced and clarified. It is now stated explicitly that the manufacturer declares the set of languages supported by the system, and it is for this set that the system is tested and certified. Furthermore, support for an alternative language must include:

1. The ability of the voter to select among languages, and to change languages within a voting session;
2. Presentation of complete information (including instructions, warnings, and messages) in the chosen language; and
3. Usability testing by the manufacturer for voters employing the alternative language.

Finally, requirement 3.2.7-A.3 specifies that all records designed to support auditing shall be intelligible to English readers, i.e., no knowledge of non-English languages is required to conduct an audit.

## 3.4 Other usability requirements

The addition of requirements for usability performance and in support of poll workers and the clarification of alternative languages were the major changes in the general usability section of the Recommendations. The rest of the section includes a variety of functional and design requirements in support of the voter.

### 3.4.1 Functional issues and ballot casting notification

The functional requirements cover the basic operations available to the voter. Many of these (such as the ability to correct a ballot) are mandated directly by HAVA.  The proposed Recommendations define a class of systems called Voter-Editable Ballot Devices (VEBDs). These are systems such as DREs and EBMs that present voters with an editable interface, allowing them to easily change their votes prior to final casting of the ballot. By contrast, systems using manually marked paper ballots are not considered to be in the VEBD class.

The functional requirements in Part 1, Section 3.2.2, apply to all systems and include notification of the effect of overvoting, ability to undervote, ability to correct the ballot (whether interactively or not), and notification of ballot casting.

The functional requirements in Part 1 Section 3.2.2.1, apply to VEBDs and detail some of the specific editing operations (such as the ability to navigate among contests) that such systems must support.

The functional requirements in Part 1, Section 3.2.2.2, generally address precinct-count optical scan (PCOS) systems. Although such systems cannot “help” voters as they fill out the ballot, they must still be able to provide certain kinds of feedback (such as warning of attempted overvoting) when the ballot is submitted.

What happens if a voter attempts to cast a ballot (either electronically or by submitting a paper ballot to a scanner) and the system fails to correctly accept and record it? How does the voter or poll worker know whether a ballot was successfully cast or not? In order to ensure that ambiguous situations do not arise, Part 1, Section 3.2.2, has been enhanced to make it clear that the system is required to report the results of attempted ballot casting in either case (see 3.2.2-D, 3.2.2.1-F, and 3.2.2.2-F). The voter must be notified when the ballot is successfully cast, and also when there has been an unsuccessful attempt (such as a misfeed of a paper ballot).

### 3.4.2 Privacy

The requirements for voter privacy begin with the basic mandate that, during the voting session, the system must prevent anyone other than the voter from seeing or hearing ballot information. In particular, warnings from the system to the voter must preserve privacy. Finally, the system must not issue receipts to the voter that would allow someone else to find out the ballot choices.

After the voting session, the so-called “cast vote record,” if electronic, must not preserve information about alternative formats used during the voting session, such as non-English languages or accessibility features. The point here is that if there are only a few voters who use a certain format, their ballot privacy could be compromised. In the case of paper ballots, there seems to be no system feature that could solve this problem. E.g., if only one voter in the polling place uses a paper Chinese ballot, the preservation of privacy will depend on appropriate procedures, rather than on system features.

### 3.4.3 Cognitive issues and plain language

Part 1, Section 3.2.4, addresses cognitive issues that may affect usability. The basic requirements are that the system must present complete instructions to the voter as to how to use the system and that there must be a provision for assistance (such as a “Help” button) to the voter by the system. Of course, a voter may at some point need to ask for poll worker assistance, but the goal is to maximize voter independence.

There are new requirements (3.2.4-C and its sub-requirements) for the use of plain language when the voting system communicates with the voter. The goal is to make the instructions for use of the system easier to understand. The sub-requirements are based on careful study of “best practice” guidelines for human/machine interaction.

There are also requirements (3.2.4-E and its sub-requirements) for good ballot design as it applies to the voting system, again based on accepted best practices.

### 3.4.4 Perceptual issues and legibility of paper

Part 1, Section 3.2.5, addresses perceptual issues that may affect usability. Note that this section addresses certain minor but common disabilities, such as color blindness and poor reading vision.

Since many aspects of the presentation of the ballot may be adjustable (e.g., font, volume), there are requirements to ensure that, first, the system must reset to a “standard” default state between voting sessions (so that one voter does not “inherit” the settings of the previous voter), and second, that there is a feature to allow the voter to reset the system during the session.

The ability to adjust font size and contrast is mandated for all systems using an electronic image display, whereas in VVSG 2005, this adjustability was required only of the accessible voting station.

Legibility of paper has also been upgraded from a recommendation to a requirement (see 3.2.5-G). The requirement specifies two techniques (font size or magnification) whereby this may be accomplished. Note that this requirement applies to all voting systems, not just those designed for voters with disabilities. As the U.S. population ages, it becomes more important to accommodate a wide range of voter capabilities, such as variations in vision.

Finally, the Recommendations require that systems accommodate color blindness, and that systems may not rely solely on color to convey information.

### 3.4.5 Interaction issues and timing

Part 1, Section 3.2.6, addresses interaction issues that may affect usability. Page scrolling is prohibited as potentially confusing. There must be good feedback as voters make their selections, so that there is no misunderstanding about ballot selections. System features must be designed to minimize accidental activation of controls by the voter.

Part 1, Section 3.2.6.1, clarifies a number of timing issues associated with the interaction between voting systems and voters. There are two aspects of this issue: how quickly must the system respond to voter actions, and what should the system do in the event of prolonged voter inactivity? In the first case, it is desired that the system be fast enough that the voter never gets the sense of dealing with an unresponsive or "dead" system. In the second case, the system must issue an alert after a specified period of inactivity to help poll workers handle the situation of a “fled voter.”

## 3.5 Accessibility requirements

The accessibility section covers the extra features required of the “accessible voting station.” Two general points should be made about this section, as they are often misunderstood. First, the section is organized according to the type of disability being addressed, and for each type, certain appropriate design and functional features are specified. Note, however, that a feature intended primarily to address one kind of disability may very well assist voters with other kinds. For example, even though the required audio interface is specified under the subsection covering blind voters, this interface may well be useful to others, such as those with cognitive disabilities or those who do not read English well.

The second point is that the requirements that this section puts on the accessible voting station are *in addition* to those of the general usability section, not instead of them. Many of these general requirements (e.g., for legibility of paper) are quite relevant to voters with various disabilities as well as to nondisabled voters.

Most of the accessibility material is similar to that in VVSG 2005. In two areas, however, the Recommendations add significant requirements.

### 3.5.1 End-to-end accessibility throughout the voting session

Requirement 3.3.1-A mandates that the system as a whole must support good accessibility procedures, and that the manufacturer document the recommended procedures. This is to guard against the possibility that, while a system may implement all of the specific features mandated elsewhere within the accessibility section, these features do not work together smoothly to provide true accessibility.

### 3.5.2 Accessibility of paper records

The Recommendations mandate the use of independently voter-verified records (IVVR) as a security measure to guard against undetected errors within the voting system itself. As a practical matter, this means that voters will be using paper records either to verify their ballots or as the ballot itself. While paper records generally provide a simple and effective means for technology-independent vote verification, their use can present difficulties for voters with certain types of disabilities, especially visual disabilities.

In order to ensure that all voters have a similar opportunity for vote verification, requirements 3.3.1-E and E.1 specify that paper records must be made accessible, and, in particular, that the system must provide audio readback of the contents of the record. Audio access to paper reconciles the need for security and accessibility.

### 3.5.3 Other accessibility requirements

This section presents a very general overview of the accessibility requirements.

Manufacturers are required to perform usability for certain specific disabilities, namely low vision, blindness, and dexterity disability. This is to encourage realistic testing of various features to make sure that they are truly usable and not just technically correct.

## 3.5 Accessibility requirements

The accessible voting station must provide complete information in the alternative formats presented and must not require the voter to bring along any personal assistive technology. The point is for the system to present a “complete” voting interface.

For **low vision** voters, the Recommendations mandate the ability to adjust color and require that buttons and controls be distinguishable by both shape and color, so as to give as many perceptual cues as possible. Also, the system must support synchronized audio and video presentation of the ballot. The voter can control which modes of presentation are used.

For **blind** voters, the system must support a full-featured audio interface. Functionally, the interface must allow navigation within the ballot, and must also support repetition and pause-and-resume to ensure comprehension of ballot choices. There are requirements for audio quality *per se,* including volume and speed control, guaranteed range of frequency, and general intelligibility.

For voters with **dexterity** disabilities, the main requirement is for a mechanism supporting nonmanual input (e.g., mouth sticks and sip-and-puff switches). For those with limited use of their hands, the Recommendations require that the controls be reasonably easy to manipulate.

For voters with limited **mobility**, the Recommendations specifies precise and detailed design requirements (e.g., size of obstructions, knee clearance, and the like) to ensure that they can easily see and reach all the relevant displays and controls.

For voters with **hearing** disabilities, in addition to the audio requirements specified in the section for blind voters, the Recommendations requires that visual cues must accompany sound cues, and that the system must not cause electromagnetic interference with assistive hearing devices.

There are no required features that are specific to voters with **cognitive** disabilities. However, many of the features designed primarily for other disabilities and for general usability are also highly relevant to these voters, e.g., synchronized audio/video and plain language instructions.

Voters who have **limited proficiency in reading English** may take advantage of the audio interface as described for blind voters.

And finally, for voters with **speech impairments**, the Recommendations mandates that speech not be required in order to use the voting system.

# Chapter 4: Major Security Topics

This chapter summarizes major security topics in the Recommendations. These are as follows:

- Software Independence, Auditing, and Independent Voter-Verifiable Records including accessibility;
- The Innovation Class;
- System Integrity Management & Cryptography;
- Access Controls;
- Open-Ended Vulnerability Testing (OEVT); and
- Threat Summary used in developing the security-related requirements.

This material is found in Chapters 4-5 of Part 1; OEVT is in Chapter 5 of Part 3.

## 4.1 Software independence

It is necessary to be able to audit voting systems in order to ensure that they are working correctly. In December 2006, the TGDC passed a resolution requiring that voting system be "software independent." Software independence (SI) means that an undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results. All voting systems must be software independent to conform to the Recommendations.

**Table 4-1 Major security topics**

| SECURITY TOPIC | DESCRIPTION |
|---|---|
| Software independence | Requirement for voting system to produce records such that audits can detect problems with voting system software. |
| The innovation class | Proposed method for facilitating the testing of new, innovative, emerging voting technologies. |
| Open-ended Vulnerability Testing (OEVT) | Requirements for an expert security review to find problems not caught in other testing. |
| Cryptography | Requirements that address the use of cryptography in voting systems, e.g., use of U.S. Government Federal Information Processing Standards (FIPS). Voting devices must contain hardware cryptographic modules to sign election information. |
| Setup inspection | Requirements that support the inspection of a voting device to determine that: (a) software installed on the voting device can be identified and verified; (b) |

## 4.1 Software independence

| SECURITY TOPIC | DESCRIPTION |
|---|---|
| | the contents of the voting device's storage containing election information can be determined; and (c) components of the voting device (such as touch screens, batteries, power supplies, etc.) are within proper tolerances, functioning properly, and ready for use. |
| Software installation | Requirements that support the secure installation of voting system software using digital signatures. |
| Access control | Requirements that address voting system capabilities to limit and detect access to voting system components in order to guard against loss of system and data integrity, availability, confidentiality, and accountability in voting systems. |
| System integrity management | Requirements that address operating system security, secure boot loading, and system hardening. |
| Communications security | Requirements that address the integrity of transmitted information and protect the voting system from communications-based threats. |
| System event logging | Requirements that address system events to be logged and protection of the information logged to assist in voting device troubleshooting, recording a history of voting device activity, and detecting unauthorized or malicious activity. |
| Physical security | Requirements that address the physical aspects of voting system security including locks and tamper-evident seals. |

The concept of software independence is based on a longstanding problem in computer science, namely, verifying that complex software (such as in voting systems) does only what it is supposed to do and nothing else. In practical terms, this is considered beyond the state of the art in computer science without resorting to great expense.

In order to compensate for this problem, computer systems support various kinds of audits. Given that the software cannot be entirely trusted, SI requires that audits of voting systems not rely entirely on software; it must be possible to audit voting systems to verify that ballots are being recorded and counted correctly without the use of software.

Software independence addresses these problems by requiring voting systems to have the ability to be audited independently of the software, that is, an audit that can be verified by hand. The Recommendations do not mandate that states perform hand audits, but require that equipment have the capability to support a hand audit.  SI does allow for much of the work of an audit to be done using automated means.  In addition to supporting a hand audit of vote totals, the Recommendations list several other types of general election audits that must be supported in order to achieve a fully auditable system.

Currently, there are only two major types of voting systems that meet the definition of SI: Voter-verified Paper Audit Trails (VVPAT) and optical scan. Both systems use paper records that can be examined by the voter and that can be used by election officials to audit vote totals without relying on software.

In the Recommendations, the requirements to support software independence are divided into three parts:

1. Requirements on the system as a whole to support auditing: Part 1, Section 4.1;
2. Requirements for independent voter-verifiable records: Part 1, Section 4.2; and
3. Requirements for electronic records: Part 1, Section 4.3.

### 4.1.2 Making systems auditable

For audits to be meaningful, the voting systems must be technically capable of providing records sufficient to support the audits and designed such that the audits are practical to carry out. The auditing process imposes requirements on the voting system in several ways, including:

1. Some audit procedures need specific information or behavior from voting systems in order for an audit to be possible or practical. For example, hand auditing the correspondence between paper and electronic records is possible only if the voting system produces paper and electronic records that include the same information.
2. Some audit procedures require certain assurances about the operation of the voting devices to be meaningful. For example, the hand audit of the paper and electronic records from VVPAT systems is meaningful only because the voter is able to view and verify the paper records.
3. Some audit procedure requirements raise other potential security concerns, which must be addressed, which must be addressed. For example, records summarizing votes must be produced in a way that does not violate ballot secrecy.

The Recommendations list three types of general election audits that must be supported by voting systems, as well as an additional method for assistive technology:

1. Pollbook Audit: the ability to verify that the number of voters agrees with the totals reported by the voting devices.
2. Hand Audit of Voter-Verifiable and Electronic Records: the ability to verify that vote totals generated electronically agree with voter verifiable records.
3. Ballot Count and Vote Total Audit: the ability to verify that the electronic records from the voting device agree with the final reported totals.

4. Observational Testing: the ability to verify that assistive technology is correctly presenting information to the voter (see Section 4.1.3 of this document.)

Note: The Recommendations only require that voting systems be capable of supporting these types of audits. Various jurisdictions may use a different set of audits as defined by their local laws and needs.

### 4.1.3 IVVR and electronic records

One of the key concepts in SI is the concept of an independent voter-verifiable record (IVVR) that can be verified by the voter and used in audits. The Recommendations define this record as something the voter can directly verify – that is, without the use of software or codebooks. Furthermore, the record must also be directly readable by election officials. Note: IVVRs must also be machine-readable to support use of automated means in audits and recounts.

Clearly, paper records used by VVPATs and optical scan systems can be IVVRs. However, the Recommendations allow for paperless IVVRs. The goal of the Recommendations is to foster innovation even though there currently are no paperless IVVR systems available in the marketplace. The requirements that define IVVR were designed not to preclude paperless solutions.

In Part 1, Section 4.3, the Recommendations define requirements for both the IVVR and electronic records to support audits. This includes requirements for the content of records and for digitally signing records.

### 4.1.4 SI and Accessibility

Paper records, and possibly other IVVR records, must be made accessible to blind and low-vision voters. The Recommendations, in order to meet both security and accessibility needs, require that voting systems provide an audio readback of the IVVR rather than the ballot stored in the voting system’s memory (the electronic record). This allows for an independent verification of the IVVR. In order to ensure that the readback of the IVVR has not been compromised, the Recommendations define an audit type called observational testing where sighted voters observe their own votes to test that the IVVR and the readback are consistent. If sighted people *occasionally* use assistive features, such as audio readback, there is a means to detect if IVVRs do not reflect voters’ choices. During observational testing, no one observes anyone else’s voting session.

### 4.1.5 SI and the VVSG 2005’s IDV

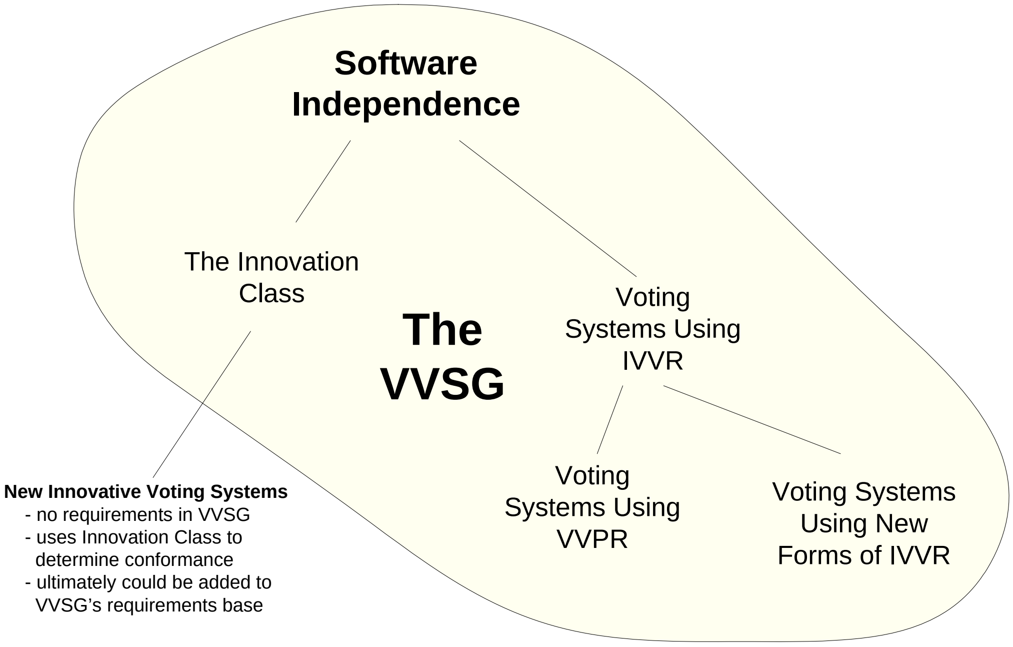
The VVSG 2005 introduced the concept of Independent Dual Verification (IDV). IDV allowed for audit by having two systems make independent records of the voter’s choices. There were four major types of IDV systems discussed: witness systems, split process (e.g., frog) systems, voter-verifiable paper (VVPR) systems (e.g., VVPAT), and end-to-end (e.g., cryptographic) systems.

VVSG 2005 included only VVPR systems, which have been expanded to IVVR. Since the goal of the Recommendations is to promote innovation in the field of auditable voting systems, it defined an innovation class to address emerging voting system technologies.

## 4.2 The innovation class

The Recommendations require that all voting systems be software independent. However, there are two paths that a voting system can follow to be software independent: *use of IVVR* or *the Innovation Class*. This is shown pictorially in Figure 4-1.

**Figure 4-1 Software Independence and the innovation class**


Software Independence
The Innovation Class
Voting Systems Using IVVR
The VVSG
Voting Systems Using VVPR
Voting Systems Using New Forms of IVVR
New Innovative Voting Systems
- no requirements in VVSG
- uses Innovation Class to determine conformance
- ultimately could be added to VVSG's requirements base

The innovation class was recommended by the TGDC as a way to encourage the development of alternate methods for achieving SI beyond IVVR. Note that the innovation class process can also be used for innovations in areas other than security such as accessibility.

The TGDC has recommended that the EAC develop procedures for submitting systems through the innovation class for federal certification. The TGDC recommends the following guidance to the EAC:

- Technologies in the innovation class must be different enough to justify using a separate certification process. In particular, it should be clear that the usual path for existing technologies towards achieving certification is not appropriate for the proposed technology.
- Technologies must advance the overall goal of fair, accurate, transparent elections. In addition, the system must meet all the requirements of the Recommendations not affected by the innovation. For example, a system with innovative security technology must still meet all usability and core requirements of the Recommendations.
- The new technology must not present an excessive burden on election administration. More generally, the technology should help rather than hinder election administrators in their goal of producing timely, accurate, and trustable election results.

## 4.3 Basic security requirements

Security is more than the ability to independently audit a system. Security must also protect the system so it can operate correctly and be resistant to tampering and various threats. Traditionally, security is described as protecting integrity, availability, and confidentiality. The integrity of the system and its data means ensuring that nothing is changed that should not be changed. Availability means ensuring the system and its data can be used when needed. Confidentiality means ensuring that data is revealed only parties that require the data.

Integrity, availability, and confidentiality are critical for voting systems. The confidentiality needs of voting systems include not linking voter choices to their identities and protecting certain data such as passwords. The general approach to securing voting system integrity and availability is by ensuring that only authorized officials and processes can make changes to the system and that all changes are logged.

The basic security requirements are contained in Part 1, Chapter 5, of the Recommendations and are summarized in Table 4-1 of this chapter. The following sections present an overview of the major aspects of Chapter 5 material.

### 4.3.1 System integrity & cryptography

The Recommendations include requirements to preserve system integrity based on current and emerging best practices in the field of computer security. A key concept for voting systems is the use of cryptography, especially digital signatures, for system integrity. The Recommendations require digital signatures for software to ensure that the software is unmodified before it is installed and run by the system. In addition, digital signatures are required to ensure the integrity of electronic records such as cast ballot records. The Recommendations require a dedicated piece of hardware to perform the cryptography for every voting device to support digital signatures. These modules are standard equipment and will not add significantly to either the cost of the device or to the administration of the system. Manufacturers may be required, however, to redesign their voting applications to integrate cryptography.

These requirements provide the capability for audits to reliably trace each record back to the voting device from which it was produced. Furthermore, digitally signing the entire collection of cast vote records produced by a vote-capture device ensures that an auditor can verify whether all records are present and if any records have been deleted or added. As an example, if a voting system digitally signs all electronic records as they are exported to a removable memory device, any attempts to change the records while in transit to the central location will be detectable because the digital signature will not validate properly.

The Recommendations also define requirements for logging of voting system information, such as when software was changed and by whom. The Recommendations require that the information logged be protected from modification and deletion.

Note: VVSG 2005 contained a requirement to address system integrity though the use of inspections of the internal machine through the use of a "trusted interface." This requirement was no longer needed, since the goal of the requirement can be met through software independence and digital signatures.

### 4.3.2 Access controls

The Recommendations require several types of access control including logical access controls, user authentication, physical security, and communications security. Access control is used to restrict who and how people and programs interact with the voting system. For example, the Recommendations require equipment to be able to restrict who can authenticate (login) to the system and perform certain actions, as well as restrict the capabilities of software programs to perform certain actions.

The Recommendations specify two general methods for identifying users:

1. **Role-based**: identifying a user based on the role they play, such as administrator, central election official, voter; and
2. **Identity-based**: identifying a user based on the user's unique identity, such as the user's name.

The Recommendations require that election management systems use identity-based access controls. To allow for specialized operating systems, the Recommendations allow for other devices to use role-based authentication.

Access to wireless communications is mostly prohibited in the Recommendations. Radio frequency wireless, used in many local area networks, is completely prohibited in voting systems. Note, however, that this does not affect the transmission of unofficial results after the close of polls; this capability is still permitted. The Recommendations also prohibit connection to the Internet or any network external to the polling site. The sole exception is for electronic pollbooks that are connected to state-wide voter registration databases but are not connected to other polling place devices.

The Recommendations also define physical access controls for physical security.

## 4.4 Open-ended vulnerability testing

Open-ended vulnerability testing (OEVT) is an expert security review whose goal is to discover architecture, design, and implementation flaws in the system that may not be detected using systematic functional, reliability, and security testing. These are flaws that may be exploited to change the outcome of an election, interfere with voters' ability to cast ballots or have their votes counted during an election, or compromise the secrecy of votes.

OEVT relies heavily on the experience and expertise of OEVT team members, their knowledge of the system, its component devices and associated vulnerabilities, and their ability to exploit those vulnerabilities. The Recommendations require both security and election expertise for the OEVT team.

The Recommendations define the minimum acceptable testing effort of 12 staff weeks. Note: This does not mean that a system will itself be tested for 12 weeks, but that 12 weeks of staff time be minimally made available for the testing effort, which may include time for research and writing reports.

There are three ways that a voting system could fail OEVT:

1. Discovery that the system does not meet a requirement in the Recommendations;
2. Discovery that the system does not meet the manufacturer’s documentation. The Recommendations require that manufacturers provide documentation of how their system, used in concert with recommended procedures, mitigates significant threats; and
3. Discovery of a critical flaw for which the OEVT team can posit a plausible description, including factoring in recommended procedural controls, of how the flaw might be exploited to change the outcome of an election, interfere with voting, or compromise secrecy of the ballot.

Note: The OEVT team is not required to successfully demonstrate an exploitation of a system’s flaws.

## 4.5 Threat summary

This section focuses on explaining how major categories of IT security threats are addressed by the Recommendations. Primarily the requirements in Part 1, especially those in Chapter 4, Security and Audit Architecture, and Chapter 5, General Security Requirements, address these threats. However, many threats are also addressed by usability requirements in Chapter 3, workmanship and reliability requirements in Chapter 6, and testing-related requirements in Part 3 (in particular, the requirements for OEVT in Part 3, Chapter 5).

Threats to voting systems can be mitigated in a number of ways, including through various procedures as well as with technical security controls incorporated in the voting system.  As with all complex IT systems, the selection of which security controls is based on an assessment of:

- What kind of the threats there may be to the system;
- What types of vulnerabilities the threats may exploit;
- What types of controls are available (or could become available);
- What might happen if threats are realized; and
- How the controls may impact the cost and operational performance of the system.

The assessment of these factors is often referred to as a threat assessment. For voting systems, the kinds of problems that have been faced in the past are known – based on analyses of past elections and studies of voting systems. However, as with other types of systems, one cannot know what will happen in the future.

Current voting system studies have included traditional security threat assessments, academic studies and experiments, reliability assessments, studies of how voters use the voting systems to record their votes, and assessments of elections that experience problems.

In general, a threat is addressed through a series of controls – both technical and procedural. Controls can generally be grouped into three types:

1. Those that prevent problems;
2. Those that detect problems (so they can be addressed); and
3. Those that assist in recovering from a problem.

Many of the threats to voting systems are similar to those of other IT systems. For example, most IT systems use access controls to ensure that only authorized people can change the software or configure the system as well as cryptography to protect the integrity of data. Although voting systems benefit from these controls as well, voting systems are quite dissimilar from most IT systems in several ways that are very important with respect to security. Key differences include:

- Not only is the system not allowed to link voters to their choices, it also must not provide a way for voters to prove how they voted.
- Because of privacy of the ballot, it is not possible to perform audits in standard ways that link transactions to individuals. Financial transactions usually provide some sort of receipt or confirmation to the user about the transaction (e.g., email confirmation of an online purchase). This information is used for verification that the system is functioning correctly and can be used to analyze problems.
- Voting systems are used infrequently (with impact on both administrator and operator training as well as equipment storage and setup) but need high reliability when they are used.

- Voting systems are not generally networked outside the polling place. The Recommendations prohibit the use of wireless networking and place constraints on how electronic pollbooks can connect to central voter registries. These factors significantly reduce threats to voting systems. (Note, however, that all networking outside the polling place presents risks.)
- Voting systems do not have trusted users of the system.

Given these factors, the security controls are a mix of standard security controls and controls tailored explicitly to the voting environment.

Controls are generally classified as technical, i.e., they are a feature of the IT system, or procedural, i.e., they are something people do. The Recommendations address both types of controls: the technical features are addressed directly by the Recommendations and the procedural controls are addressed indirectly in that the Recommendations require systems to be capable of being managed with the appropriate procedural controls. For example, see the EAC Best Practices and Election Management Guidelines for descriptions of appropriate controls at

- http://www.eac.gov/election/docs/electionmanagementguidelines.pdf/attachment_download/file

Many procedural controls are completely independent of the system, but many are intertwined with the technology used. Some technical controls are completely dependent on being accompanied by appropriate procedural controls. For example, if administrative passwords are taped to the side of the box, it does not matter how well the logical access controls are designed; they have been rendered ineffective. Other procedural controls, such as auditing, require that the system be able to produce appropriate records for auditing.

Table 4-2 shows the relationship between election-specific threats and the major control categories in the Recommendations that address the threats. Note that most threats are addressed by several controls – a practice referred to as "defense in depth." There are also many supporting controls that are used to strengthen the other controls. An example of such a control is cryptography, which is necessary for other controls such as access control.

**Table 4-2 Election-specific threats addressed in the Recommendations**

| THREAT | DESCRIPTION | CONTROLS IN THE RECOMMENDATIONS |
|---|---|---|
| Loss of voter privacy including vote selling and voter coercion | Some voters willingly give up their privacy in order to sell their votes. Others are coerced to vote certain ways. If voters believe that voter privacy is compromised, they can be coerced, whether or not the | • Part 1, Section 3.2.3 Privacy<br>• Part 1, Section 4.3 Electronic Records and Part 1, Section 4.4 IVVR for specific items on ensuring that audit records |

### 4.5 Threat summary

| THREAT | DESCRIPTION | CONTROLS IN THE RECOMMENDATIONS |
|---|---|---|
| | privacy violation is real. Similarly vote selling is also facilitated by the belief that privacy can be compromised. | do not identify voters.<br>• Part 1, Section 7.5.1 Issuance of voting credentials and ballot activation |
| Incorrect counting of voter choices including adding or deleting votes from totals | Changing the totals is often called election fraud. Although any change to the reported totals from the correct values violates the security goals, election fraud becomes more serious as the scale increases to a level where the outcome of national, state or local races is changed. | • Chapter 7, Requirements by Voting Activity, addresses correct operation of the voting system.<br>• Part 1, Section 4.2, Requirements for Supporting Auditing, Part 1, Section 4.3, Electronic Records, and Part 1, Section 4.4 IVVR, provide technical requirements to allow election officials to meaningfully audit elections and show that the voting system works correctly. |
| Incorrect capture of voter choices | Voters may accidentally select the wrong choice or the voting system could incorrectly record a selection. | • Part 1, Section 3.2, Usability, and Part 1, Section 3.3, Accessibility, address technical requirements for increasing the quality (including ease and accuracy) of the vote capture process.<br>• Chapter 7, Requirements by Voting Activity, addresses correct operation of the voting system. |
| Disruption of an election | Disrupting an election can result in preventing some large fraction of voters from voting or having their votes counted. The goal of such as attack may be to affect the outcome of the election or a form of protest. | • Part 1, Section 5.6 ,Communication Security<br>• Part 1, Section 5.8, Physical Security<br>• Part 1, Section 3.3, Accessibility |

| THREAT | DESCRIPTION | CONTROLS IN THE RECOMMENDATIONS |
|---|---|---|
| | | • Part 3, Section 5.3.3 Reliability |
| Discrediting an election | The result of a successful discrediting attack is an election in which there is substantial doubt about the correctness of its result. This is distinct from a disruption attack in that the election runs normally, but then evidence is manufactured to support a claim of fraud. Discrediting attacks can affect elected officials' ability to govern and long-term voter confidence. | • Part 1, Section 4.2, Requirements for Supporting Auditing, Part 1, Section 4.3, Electronic Records, and Part 1, Section 4.4, IVVR, provide technical requirements to allow election officials to meaningfully audit elections. |

Table 4-3 shows how the Recommendations address generic IT system vulnerabilities. These vulnerabilities could be the means by which an election-specific threat becomes a reality. These are vulnerabilities that many IT systems must address.

**Table 4-3 Generic IT system vulnerabilities addressed in the Recommendations**

| VULNERABILITY | DESCRIPTION | CONTROLS IN THE RECOMMENDATIONS |
|---|---|---|
| Malicious programming by insider (at manufacturer, test lab, election official) | It is possible to write software to change vote totals, not record certain votes, or otherwise change the results. This requires significant knowledge of how the software is programmed, how elections are run using the voting system, and requires access to the system. | • Chapter 6, especially 6.4 Workmanship<br>• Part 1, Section 4.2, Requirements for Supporting Auditing, Part 1, Section 4.3, Electronic Records, and Part 1, Section 4.4, IVVR, provide requirements to detect the effects of incorrect software<br>• Part 3, Chapters 4 and 5, especially Structural Coverage (white box testing) and Open-Ended Vulnerability Testing |

## 4.5 Threat summary

| VULNERABILITY | DESCRIPTION | CONTROLS IN THE RECOMMENDATIONS |
|---|---|---|
| Software and design errors | All software is subject to errors. | • Chapter 6, especially 6.3, Hardware and Software Performance, and 16.4, Workmanship<br>• Part 1, Section 4.2, Requirements for Supporting Auditing, Part 1, Section 4.3, Electronic Records, and Part 1, Section 4.4, IVVR, provide requirements to detect the effect of incorrect software<br>• Part 5, Chapters 4 and 5, especially Structural Coverage (white box testing) and Open-Ended Vulnerability Testing |
| Incorrect software being run and other configuration problems including viruses | Voting systems run software but also have configuration files, primarily ballot definition files, which are critical to the election. The wrong software or configuration files could be loaded onto a machine on purpose or by accident. Viruses and other malicious code are examples of incorrect software that could be run. | • Part 1, Section 5.5, System Integrity Management<br>• Part 1, Section 5.3, Software Installation<br>• Part 1, Section 5.2, Setup Inspection<br>• Part 1, Section 5.1, Cryptography<br>• Part 1, Section 5.4, Access Control<br>• Part 1, Section 5.7, System Event Logging |
| Hacker/outside attack | Any IT connected to any network is subject to hacker attacks. Attacks range from run-of-the-mill attempts to break into systems to sophisticated denial of service attacks. | • Part 1, Section 5.4, Access Control<br>• Part 1, Section 5.7, System Event Logging<br>• Part 1, Section 5.6, Communications |
| Insider sabotage | Disgruntled employees are a fact of life within any organization. In addition, as noted above, insiders are often in the best | • Part 1, Section 5.4, Access Control<br>• Part 1, Section 5.7, System Event Logging |

## 4.5 Threat summary

| VULNERABILITY | DESCRIPTION | CONTROLS IN THE RECOMMENDATIONS |
|---|---|---|
|  | position to cause damage. | • Part 1, Section 5.8, Physical Security |
| Loss of physical or infrastructure support (e.g., loss of electricity or network) and loss of IT system functionality | This vulnerability addresses external factors such as loss of power or networking as well as other physical problems such as water line breaks, storms, and transportation problems. It also includes broken equipment. | • Part 1, Section 6.3, Hardware & Software Performance<br>• Part 1, Section 6.4, Workmanship<br>• Part 1, Section 5.6, Communications<br>• Part 3, Section 5.3, Benchmarks (including 5.3.3 Reliability) |
| Compromised communications | Communications lines are the most obvious place for outsiders to attack a system. Communications security, while very advanced, is very difficult to set up and operate securely. | • Part 1, Section 5.6, Communications<br>• Part 1, Section 5.1, Cryptography<br>• Part 1, Section 4.3 Electronic records |

# Chapter 5: Major Core Requirements Topics

This chapter provides overviews of major core requirements topics in the Recommendations. This material largely comprises Chapters 6 and 7 of Part 1. The Core material is defined as “the material remaining after usability, accessibility, privacy, and security.” It includes basic requirements for device functionality, workmanship, voting variations, and so forth. The sections below contain overviews and summaries of the major core topics, as follows:

- End-to-end and volume testing;
- Reliability testing;
- Optical scanner accuracy;
- Commercial off-the-shelf (COTS) software testing; and
- Electronic pollbooks.

The core requirements material is largely an update from VVSG 2005, and many of the requirements not covered here are rather technical and detailed, having to do with electrical aspects of equipment, quality control, software design, coding standards, and so forth. However, the material is extremely important, as it entirety covers most aspects of voting equipment and operations, and will largely result in voting systems being significantly more reliable.

## 5.1 End-to-end and volume testing

End-to-end testing of voting systems for accuracy and reliability covers the entire elections process from election definition through the reporting of final results. It was not specified in previous versions of the Recommendations, which meant that some tests could bypass significant portions of the system that would be exercised during an actual election, such as the touch-screen or keyboard interface. This practice may lower testing costs or increase convenience, but the validity of the testing could be difficult to defend.

**Table 5-1 Major core topics**

| CORE TOPIC | DESCRIPTION |
|---|---|
| End-to-end testing | Requirements to ensure all aspects of voting systems are tested during all phases of voting operations. |
| Volume testing | Requirements to assess accuracy and reliability in tests simulated to mimic election conditions using typical volumes of data. |
| Reliability testing | Significant changes to requirements to assess the reliability of voting systems. |
| Optical scanner | Significant changes to accuracy requirements for optical scanners and handling |

| CORE TOPIC | DESCRIPTION |
|---|---|
| accuracy | of marginal marks. |
| Electronic pollbooks (epollbooks) | New requirements on ballot activation involving epollbooks to protect integrity and privacy of ballot activation information and to ensure records on epollbooks do not violate secrecy of the ballot. |
| COTS | Significant changes to requirements to ensure commercial off-the-shelf-software used in voting systems is tested appropriately. |

Part 3, Section 5.3, of the Recommendations lays out requirements for evaluating reliability, accuracy, and optical scan misfeed rates over the course of the entire test campaign as opposed to just during tests specifically focusing on reliability or accuracy. The rationale is:

- Reliability and accuracy are important to measure during all aspects of the test campaign; and
- This increases the amount of data available for measurements without necessarily increasing the duration of testing.

In addition, Part 3, Section 2.5.3, tightens the requirements from previous versions that permitted bypassing certain parts of the system, e.g., the user interface, during the tests.

Measuring reliability and accuracy during the course of a test that simulates actual election conditions provides more realistic, defensible measurements of actual expected reliability and accuracy rates. Thus, a “volume test" that approximates the conditions of an actual election will be part of the voting system testing. A volume test involves a large number of test voters using voting devices in conditions approximating normal use in an election. Requirement 5.2.3-D in Part 3, Section 5.2.3, specifies a volume test similar to the State of California’s California Volume Reliability Testing Protocol rev. January 31, 2006-01-31, available from

- http://www.ss.ca.gov/elections/voting_systems/volume_test_protocol_final.pdf

## 5.2 Reliability testing

In VVSG 2005, the requirement for voting device reliability specified a Mean Time Between Failure (MTBF) of at least 163 hours. This requirement received much criticism for not being sufficiently rigorous, in that it still permitted a relatively high likelihood of failure over a 15-hour period (approximately 9 percent), yet the MTBF demonstrated by the described test was even lower.

Thus, the evaluation of reliability was updated in the Recommendations to be more rigorous and comprehensive.

However, simply increasing the number of hours of testing so as to lower the likelihood of failures occurring was not practical, given the way in which the reliability tests were conducted. For example, to reduce the likelihood of failure to one percent over a 15-hour period would have required an estimated 234 days of testing. In addition, since failures are more often triggered by the activity that occurs in an election than by the mere passage of time, just adding more time does not necessarily result in a more effective test.

The approach taken in the Recommendations is first to strictly define what one means by a *failure* and then to arrive at appropriate failure rate benchmarks on a type-of-device basis, which is more realistic than the previous "one size fits all" approach from previous versions. These benchmarks are expressed in terms of the level of *activity* (e.g., number of ballots processed) rather than time. Finally, the Recommendations use a volume test and evaluate reliability over the course of the entire testing campaign. This should keep the amount of time required for testing to a manageable level, but result in a more effective test. This will also reduce costs.

A *failure* is defined as an event that results in (a) loss of one or more functions, (b) degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds, (c) automatic reset, restart, or reboot of the voting device, operating system, or application software, (d) a requirement for an unanticipated intervention by a person in the role of poll worker or technician before the test can continue, or (e) error messages and/or audit log entries indicating that a failure has occurred. In plain language, failures are equipment breakdowns, including software crashes, such that continued use without service or replacement is worrisome to impossible. Normal, routine occurrences like running out of paper are not considered failures.

Part 1, Section 6.3.1, lays out estimates of election activity volume per election for voting devices, and then lays out the manageable number of failures per election per device type. The research data behind these numbers came from interactions with members of NASED (National Association of State Election Directors) through their representative on the TGDC. The estimates of volume and failures are for a mid-size county in a western state in a high turn-out election, as of 2006. According to these estimates, a county of 150,000 registered voters will have 120,000 ballots cast in a presidential election. A typical polling place will be set up to handle 2,000 voters, which equals 60 polling places in a mid-size county.

Table 5-2 summarizes the estimated volumes per device class:

**Table 5-2 Estimated volumes per election by device class**

| DEVICE CLASS | ESTIMATED VOLUME PER DEVICE PER ELECTION | ESTIMATED VOLUME PER ELECTION |
|---|---|---|
| central tabulator | Maximum tabulation rate times 8 hours | 120,000 ballots |
| EMS | 480 transactions | 480 transactions |

### 5.2 Reliability testing

| DEVICE CLASS | ESTIMATED VOLUME PER DEVICE PER ELECTION | ESTIMATED VOLUME PER ELECTION |
|---|---|---|
| precinct tabulator (e.g., PCOS) | 2,000 ballots | 120,000 ballots |
| DRE | 200 voting sessions | 120,000 voting sessions |
| EBM | 70 voting sessions | 120,000 voting sessions |
| other vote-capture device | 200 voting sessions | 120,000 voting sessions |
| activation device | 2,000 ballot activations | 120,000 ballot activations |

The following paragraphs outline the estimates of manageable failures per device type per election:

- **Central-count optical scanner (CCOS)**: No more than one machine breakdown per jurisdiction requiring repairs done by the manufacturer or highly trained personnel. Medium-size jurisdictions plan on having one backup machine for each election.
- **Election Management System (EMS):** This is a critical system that must perform in an extremely time-sensitive environment for a mid-size county over a 3-to-4 hour period election night. Any failure during the test that requires the manufacturer or highly trained personnel to recover should disqualify the system. Otherwise, as long as the manufacturer's documentation provides usable procedures for recovering from the failures and methods to verify results and recover any potentially missing election results, 1 failure is assessed for each 10 minutes of downtime (minimum 1 – no fractional failures are assessed). A total of 3 or more such failures disqualify the system.
- **Precinct-count optical scanner (PCOS):** A failure in this class of machine has a negligible impact on the ability of voters to vote in the polling place. No more than 1 of the machines in an election experience serious failures that would require the manufacturer or highly trained personnel to repair (e.g., will not boot). No more than 5 percent of the machines in the election experience failures that require the attention of a troubleshooter/poll worker (e.g., memory card failure).
- **Direct Recording Electronic (DRE) and Electronically-assisted Ballot Marker (EBM):** No more than 1 percent of the machines in an election experience failures that would require the manufacturer or highly trained personnel to repair (e.g., won't boot) and no more than 3 percent of the machines in an election experience failures that require the attention of a troubleshooter (e.g., printer jams, recalibration, etc.).
- **Ballot activator (e.g., epollbook):** The media/token should not fail more than 3 percent of the time (the county will provide the polling place with more tokens than necessary). No more than 1 of the

devices should fail (the device will be replaced by the county troubleshooter).

Using this data, the reliability of the devices will be evaluated using the volume test designed to simulate actual election conditions and throughout the entire test campaign, so that voting systems that appear incapable of performing at the level of reliability described above will receive a negative test result.

## 5.3 Optical scanner accuracy and marginal marks

The Recommendations clarify the accuracy requirements for optical scanners. Previous versions of the Recommendations required optical scanners to conform to a low error rate requirement when reading marks that were made to manufacturer specifications. This requirement has been retained, but is now supplemented by a requirement to read a standard mark made with a #2 pencil with the same level of accuracy as marks made exactly to manufacturer specifications. A related requirement to ignore "extraneous perforations, smudges and folds," which under some interpretations is unattainable with existing technology, has been adjusted to recognize that there is no mechanical way of determining whether a given mark that appears within a voting target is extraneous or not. (A machine cannot read the mind of the voter to determine if a mark was intentional or accidental; it can only read the ballot and implement some consistent policy based on that reading.)  Marks appearing outside of voting targets, on the other hand, are always extraneous—at least as far as standard behavior is concerned. Systems that support detection of circled voting targets and other marks that jurisdictions may consider to be valid votes must also support a baseline, standard mode of operation in which such marks are ignored.

The Recommendations also address marginal marks, which previously were not addressed at all. A marginal mark is a mark within a voting target (e.g., an oval on a ballot next to a candidate choice) that does not conform to manufacturer specifications for a reliably detectable vote. The word *marginal* refers to the limit of what is detectable by an optical scanner, not the margin of the page. A marginal mark is neither clearly countable as a vote nor clearly countable as a nonvote. It is an ambiguous vote, analogous to dimpled chad on a punchcard.

## 5.4 Commercial off-the-shelf (COTS) software testing

Previous versions of the VVSG were criticized for defining Commercial Off-the-Shelf (COTS) software and the resultant testing requirements in a somewhat loose fashion. Essentially, if a COTS software product is used in a voting system and it is used unmodified, then it is exempt from requirements for source code inspection. If the COTS is modified, its source code is subject to inspection and the source code is also subject to requirements for source coding standards, which involved extensive and time-consuming reformatting of the source code. In some cases, the difference between modified and unmodified COTS was not clear, and in some cases, having to reformat modified COTS source code may have been counterproductive.

It is important to note, however, that COTS has never been exempt from testing; COTS has always been tested as part of the voting system. However, it has been exempt in some cases from source code inspection.

The Recommendations now define COTS very strictly as “only unmodified,” e.g., shrink-wrapped commercial software and analogous open-source packages. It clarifies the treatment of components that are neither voting system manufacturer-developed nor unmodified COTS (so-called “modified COTS”). It also allows different levels of testing scrutiny to be applied depending on the sensitivity of the components being reviewed. In some cases, modified components do not require source code reformatting.

The result is that COTS and modified COTS are tested appropriately, but at the same time not wastefully. For example, a COTS operating system with a proven track record of performance may not require source code review, but configuration files that affect the performance of the operating system would require test lab review.

The way in which COTS is tested has also changed. The manufacturer must deliver the system to test without the COTS installed, and the test lab must procure the COTS separately and integrate it into the voting system. If the integration is successful, the COTS can safely be assumed to be unmodified.

## 5.5 Electronic pollbooks

The Recommendations now contain requirements for electronic pollbooks (epollbooks), located in Part 1, Section 7.5. These requirements were added to protect integrity and privacy of ballot activation credential information and to ensure that records on epollbooks and vote-capture devices cannot be aggregated to violate secrecy of the ballot. Epollbooks are permitted to activate the ballot while connected to an external voter registration database; various requirements on network security are included.

It is important to note that while the requirements in Part 1, Section 7.5, are fairly limited, all other relevant requirements in the Recommendations that apply to voting devices also apply to electronic pollbooks that are submitted as part of the voting system. Thus, requirements for security, reliability, accuracy, and usability also apply.

In general usage, the term *ballot activation* is sometimes used in a broad sense to cover the general activities of

1. Determining what type of ballot must be presented to the voter, and
2. Activating the voting system to present the ballot style that is appropriate for that voter.

The requirements in Section 7.5 use *issuance of voting credentials* for the first activity and “ballot activation” exclusively for the second activity.

Voting credentials are those data items sufficient for the voting system to activate the appropriate ballot for the voter. The credentials consist of an indication of the ballot style and ballot configuration as well as any additional ballot options that the voting system may be capable of presenting if selected by the voter, such as a magnified ballot for a voter with low vision.

Preserving privacy of the ballot is a paramount consideration in issuance of voter credentials and ballot activation because knowledge of the voter’s identity is involved. The requirements in this section mandate that privacy of the ballot be protected throughout the entire process of credential issuance and ballot activation, and that no information be maintained in reports or logs that could assist in identifying a voter’s cast ballot (except for provisional voting on a DRE).

Provisional voting using a DRE must, however, “violate” voter privacy because it is necessary to link the DRE’s electronic record with the voter’s identity. If an epollbook or other programmable activation device is used also for provisional voting, then it is possible that the epollbook could keep a record of provisional voters and include, with the voting credentials, an identifier associated with each provisional voter’s identification. The DRE might then associate that identifier with that voter’s record. This should only happen if the activation device and the vote-capture device are in a “provisional voting” mode; no linkage of voter identity to voter records should be possible otherwise.

There are also requirements that permit a ballot activation device to connect to an external voter registration database via a network. Network connectivity is inherently difficult to secure and make reliable; therefore, the requirements in this section mandate that the external connectivity must be enabled/disabled by an authorized election official, and that a backup mechanism be in place if the connectivity fails. A ballot activation device or DRE/EBP used as an activation device cannot be connected simultaneously to both an internal (to the voting site) network of DREs or EBPs and an external network (i.e., the ballot activation device cannot include more than one network interface).

5.5