1

# Draft VVSG Recommendations to the EAC

**May 2007 DRAFT**

**VOLUME 1:**

**INTRODUCTION**

OVERVIEW TO VOLUMES 2-5

# VVSG Draft 20070524

May 24, 2007

This document has been prepared by the National Institute of Standards and Technology at the direction of the Technical Guidelines Development Committee (TGDC). It may represent preliminary research findings and does not necessarily represent any policy positions of NIST or the TGDC.

The Technical Guidelines Development Committee is an advisory group to the Election Assistance Commission (EAC), which produces Voluntary Voting System Guidelines (VVSG). Both the TGDC and EAC were established by the Help America Vote Act of 2002. NIST serves as a technical adviser to the TGDC.

# Volume 1 Table of Contents

## Volume 2 Table of Contents

# Volume 3 Table of Contents

# Volume 4 Table of Contents

# Volume 5 Table of Contents

# Volume 1: VVSG Introduction

# Chapter 1: Overview

This version of the VVSG is a complete rewrite of VVSG 2005, with new material and considerable updates. The requirements are more precise, directly testable, and clearer to voting system vendors and test laboratories. The language throughout is written to be more readable and usable to all audiences.

This next version of this volume overview will be considerably fleshed out to include summaries of how the VVSG is to be read, the requirements structure, and new material.

## 1.1 Document Structure

Following Volume I, the Voluntary Voting System Guidelines includes:

- A terminology standard (Volume II) defining terms used in the foregoing;
- A product standard (Volume III) defining requirements that apply to voting systems that vendors produce;
- Standards on data to be provided (Volume IV) defining requirements that apply to documentation, reports, and other information that vendors and test labs deliver; and
- A testing standard (Volume V) defining test methods and protocols that test labs implement.

## 1.2 Scope and Applicability

Volume I, Guidelines Overview introduces this document from both a historical and a legislative framework. All members of the election community should obtain useful background information here for the requirements that follow in the succeeding four volumes. Volume 1 also outlines the structural changes from VVSG 2005 with the rationale that these recommended standards will be applicable to the next generation of voting systems.

Volume II, the Terminology Standard, covers Terminology for standardization purposes that must be sufficiently precise and formal to avoid ambiguity in the interpretation and testing of the standard. Terms are defined to mean exactly what is intended in the requirements of the standard, no more and no less. Volume II has a narrower scope than that of VVSG 2005 in that terms not specifically relevant to the VVSG requirements have been removed, and most of those that remain have been redefined to better serve the purpose of clarifying the VVSG.

Volume III, Product Standard, provides guidelines for vendors to produce voting systems that are secure, accurate, reliable, usable, accessible, and fit for their intended use. Volume III sets a precedent where requirements in VVSG 2005 that were ambiguous have been clarified. In those cases where no precise replacement could be determined and no testing value could be ascribed, requirements have been deleted.

Volume IV, Standards on data to be provided, is a new section containing documentation requirements separate from functional and performance requirements applying to the voting equipment itself. It contains requirements applying to the Technical Data Package, the Voting Equipment User Documentation, the Test Plan, the Test Report, the Public Information Package, and the data for voting software repositories.

Volume V, Testing Standard, contains requirements that apply to the national certification testing to be conducted by non governmental certified testing laboratories. It has been reorganized to focus on test methods and avoid repetition of requirements from the product standard. The hardware testing vs. software testing distinction is no longer a guiding principle in the organization of the Guidelines. Although different testing specialties are likely to be subcontracted to different laboratories, the prime contractor must report to the certifying authority on the conformity of the system as a whole.

## 1.3 Audience

The VVSG is intended primarily as a critical reference document for:

- Designers and manufacturers of voting systems;
- Test labs performing the analysis and testing of voting systems in support of the national certification process;
- Software repositories designated by the national certication authority or by a state; and
- Test labs and consultants performing the state certification of voting systems.

In addition, the goal of VVSG Volume l is to provide all members of the election community including the public, elected officials, and representatives of advocacy groups with a useful and usable introductory guide to the VVSG.

# Chapter 2: VVSG Background

## 2.1 Governing Legislation

The Help America Vote Act of 2002 (HAVA) established the Technical Guidelines Development Committee (TGDC) to assist the Election Assistance Commission (EAC) with the development of voluntary voting system guidelines. HAVA directed the National Institute of Standards and Technology (NIST) to chair the TGDC and to provide technical support to the TGDC in the development of these guidelines. The TGDC's initial set of recommendations for these guidelines were presented to the Election Assistance Commission in May 2005, in accordance with HAVA's nine-month deadline. After a public review process, the EAC formally adopted voluntary voting system guidelines in December 2005.

## 2.2 History of Federal Voting System Standards and Guidelines

In 1975, the National Bureau of Standards (now the National Institute of Standards and Technology) and the Office of the Federal Elections (the Office of Election Administration's predecessor at the General Accounting Office) produced a joint report, Effective Use of Computing Technology in Vote Tallying. This report concluded that a basic cause of computer-related election problems was the lack of appropriate technical skills at the state and local level to develop or implement sophisticated Standards against which voting system hardware and software could be tested. A subsequent Congressionally-authorized study produced by the FEC and the National Bureau of Standards detailed the need for a federal agency to develop national performance Standards that could be used as a tool by state and local election officials in the testing, certification, and procurement of computer-based voting systems.

In 1984, Congress appropriated funds for the 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.

The national testing effort was developed and overseen by the National Association of State Election Director's Voting Systems Board, which is composed of election officials and independent technical advisors. NASED's testing program was initiated in 1994 and more than 30 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 Standards in conjunction with functional and technical requirements developed by state and local policymakers to address the specific needs of their jurisdictions.

As the qualification process matured and qualified systems were used in the field, the Voting Systems Board, in consultation with the testing 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 Standards.

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

In 2002, Congress passed the Help America Vote Act, which created a new process for improving voluntary voting system guidelines. A new federal entity was created, the Election Assistance Commission, to oversee the process. The EAC established the Technical Guidelines Development Committee in accordance with the requirements of section 221 of HAVA pursuant 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 shall serve as its chair,
- Members of the Standards Board,
- Members of the Board of Advisors,
- Members of the Architectural and Transportation Barrier, and Compliance Board (Access Board),
- A representative of the American National Standards Institute,
- A representative of the 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
- Other individuals with technical and scientific expertise relating to voting systems and voting equipment.

The TGDC first met in July 2004 and delivered its initial set of recommendations to the EAC in April 2005. Operating as a Federal Advisory Committee, the TGDC formed three working subcommittees: Security and Transparency (STS), Human Factors and Privacy (HFP), and Core Requirements and Testing (CRT). The three subcommittees in collaboration with NIST recommended requirements for adoption by the full Committee at public plenary sessions. The TGDC's initial set of recommendations augments the VSS 2002 by including security measures for auditability, wireless communications and software distribution and set up, and improvements for the accessibility guidelines and usability design guidelines for voting systems. The TGDC also recommended that the VSS 2002 should be replaced 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 today's more rigorous needs for electronic voting systems. This document, applied to the next generation of voting equipment, addresses those needs and is meant to as technical guidance to the EAC for adoption of the next iteration of the VVSG.

## 2.3 Relationship of HAVA and the VVSG

Although both HAVA and the VVSG contain "requirements", the scope and application are quite different in the two cases.

The Help America Vote Act (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 Voluntary Voting System Guidelines (VVSG) is 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 VVSG requirements (as determined by conformance testing conducted by an accredited laboratory), then that type is eligible to be *certified* as being compliant with the VVSG. Thus the VVSG is addressed to vendors 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 non-certified systems, as long as they comply with the HAVA standards.

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

# 2.4 Approval and Adoption Procedures

In compliance with the Federal Advisory Committee Act, the three working subcommittees of the TGDC oversaw the development of the recommended voluntary requirements in this document through public teleconference meetings with NIST staff held between September 2005 and July 2007. In addition, during the same time period the full TGDC reviewed and approved this document at public plenary sessions convened at NIST.

These recommendations for the next iteration of the VVSG will be delivered to the EAC in July 2007 for a formal public commenting process to be noticed in the Federal Register. In addition, the EAC's Standards Board and Board of Advisors will review the document and report back to the EAC. Once the EAC has considered the input from the Standards Board, Board of Advisors and the public, the Commission will vote to adopt the next iteration of the VVSG. The EAC will also determine and publish the effective date for implementation of these guidelines. Before the implementation date for the next VVSG, local and state election officials; voting system manufacturers; and certified testing laboratories should refer to the 2005 VVSG for official guidance on current voting systems.

# Chapter 3: New Material & Significant Changes from VVSG 2005

The VVSG have been reorganized to bring them in line with applicable standards practices of ISO, W3C and other standards-creating organizations. This includes expanding the conformance clause that was added in VVSG 2005 [6], identifying testable requirements, and defining classes, which allow requirements to vary as needed to accommodate variations in voting equipment.

Preferably, requirements should specify what (the desired performance), not how (a design to accomplish that). For example, a requirement that reads "single-bit errors shall be detected" is preferable to one that reads "products shall use memories with parity bits." Classes are created to resolve the conflict that occurs when the what depends on the how. For example, the unstated assumption that the voting equipment would have an electronic memory at all requires placing the preceding example in a subclass for electronic voting equipment.

Design-constraining requirements are controversial because vendors would like the freedom to provide the desired qualities / performance in different ways. However, in cases where vendors are unable to determine for themselves whether or not a given design is conforming, they may welcome design constraints as a way to avoid repeated failures and costly retesting of their products. Moreover, in cases where the desired quality is difficult to define abstractly, an enumeration of conforming cases may be the only practical alternative, particularly if there is only one design approach that is ever actually usable in practice. Some pragmatism is required.

A vendor who is submitting a system for testing must make an implementation statement that identifies exactly which classes the system is asserted to support. Conformity assessment activities are catalogued according to which requirements they exercise. The set of conformity assessment activities appropriate to that system may then be determined automatically. Upon passing those tests and reviews, the system may be certified for only the claimed classes. There is no provision for certification of voting systems that do not conform to the requirements.

Identified requirements and a classification mechanism in the VVSG facilitate traceability from state standards to the VSS. States may define their own profiles over the VVSG, adding requirements they deem necessary without excessive repetition and revision of VVSG text.

## 3.1 Volume 2 Changes

The scope of concern for this terminology standard has been narrowed from that of the Glossary of [6]. Terms that were not needed to disambiguate VVSG requirements have been removed, and most of those that remain have been

redefined to better serve the purpose of clarifying the VVSG. Please see the discussion in Volume II Section 1.2 about the intended use of these definitions.

## 3.2 Volume 3 Changes

### 3.2.1 Supplemental Guidance

Throughout the Product Standard are informative subsections titled "Procedures required for correct system functioning." The requirements in these subsections provide context for what the functional requirements specify or, more often, for what they omit. These requirements do not pertain to the voting system and are not tested by an accredited test lab.

### 3.2.2 Conformance clause

The conformance clause has been expanded to define classes of voting systems and devices. Classes are an evolution of the notion of voting system "categories" that appeared in previous Guidelines. Those categories were paper-based, DRE, precinct count and central count.

The categories were too coarse-grained for the purpose of scoping requirements. In many cases it was unclear whether a given requirement applied holistically to the entire voting system, individually to every device in the voting system, or individually to every instance of a particular type of device. Consequently, it was unclear how to apply requirements to today's voting systems, which may blend DRE equipment with optical scan equipment and otherwise fail to meet the assumptions that were inherent in the old Guidelines.

Classes make it possible to scope requirements more precisely so that systems blending different technologies can be tested and certified.

### 3.2.3 Core requirements

The core requirements for voting systems to define elections and to collect, count, and report votes have been expanded to specify what functionality must be provided in order to claim support for the many jurisdiction-specific voting variations such as cumulative voting, straight party voting, etc. In previous versions of the Guidelines, vendors were required to identify which variations were supported and to document how those variations were supported, but the Guidelines lacked any functional requirements on the variations. The new requirements define a baseline of functionality for each of the voting variations.

The requirements have been broadened to cover Electronically-assisted Ballot Markers (EBMs) and Electronic Ballot Printers (EBPs). These devices' combination of a DRE-like interface with a paper-based method of recording votes was something that previous Guidelines did not handle.

The metric for reliability has been changed from Mean Time Between Failure to a failure rate based on volume that varies by device class and severity of failure. The metric for accuracy has been changed from ballot position error rate to report total error rate, and separate requirements referring to specific, low-level operations have been replaced with a single, general, end-to-end accuracy requirement. The metrics for multiple feed and rejection of ballots that meet all vendor specifications have been merged into a single "misfeed" metric. In each case, revised benchmarks have been derived from input from the Technical Guidelines Development Committee and election officials.

Significant changes have been made to the accuracy requirements for optical scanners. Previous Guidelines required optical scanners to conform to a low error rate requirement when reading marks that were made to vendor 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. 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. This ties into the well-known problem of voter intent. 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.

Requirements and discussion on the handling of marginal marks have been added. See Volume III Section 1.4.4.

Requirements on the content of vote data reports, which appeared in several places and in different ways in previous Guidelines, have been unified, harmonized, and clarified. Required contexts for reporting have been specified, and the concepts cast ballot, read ballot and counted ballot have been clearly distinguished. The quantities to be included in vote data reports have been formally defined using a logic model.

Other changes include

- Made compatible with early voting.
- Clarified that the redundant records stored by DREs are for recoverability purposes, and not to be confused with independently auditable records as specified in Dangling ref: PleaseAddReference_STS_Auditability.
- Clarified and generalized the prohibition on counter overflow.
- Specified that voting systems should flag any discrepancies in vote data reports that are detectable by the system.
- Added "should" requirements for reporting the count of blank ballots and for combined precinct reporting.
- Separated election administration concerns from product requirements.

- Replaced the term ballot format, which was inherited from [1], with the term used in modern practice, ballot style.

### 3.2.4 Marginal marks

A marginal mark is a mark within a voting target that does not conform to vendor 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. Marks that are outside of voting targets are called extraneous marks.

A marginal mark is neither clearly countable as a vote nor clearly countable as a non-vote. It is an ambiguous vote, analogous to dimpled chad on a punchcard.

The voter should always be instructed to make an ideal mark, which in a typical optical scan system means completely filling the oval with a #2 pencil. To allow for variations in the marks that diligent voters actually make when trying to follow this instruction, the accidental use of non-approved marking utensils, et cetera, optical scanners are configured to accept a relatively wide range of marks as votes (Requirement III.6.8.5-D). Marginal marks are below this range. They happen when voters do not follow instructions or the instructions are inadequate.

Although the criteria are not necessarily simple, vendors are required to specify what constitutes a reliably detectable mark versus a marginal mark (Requirement IV.3.1.2-A.2). If this cannot be accomplished, then the voting system is counting votes using a mystery algorithm. Such a system is not certifiable.

A ballot that was marked with an EBM should never contain marginal marks. If it does, an equipment malfunction has occurred, and it should be handled as such (Requirement III.6.8.3-C).

In the case of precinct counting of manually-marked paper ballots, the precinct count scanner should be configured to reject ballots containing marginal marks (Dangling ref: PleaseAddReference_HFP Precinct paper tabulator, capability to reject marginal marks). For example, a hypothetical optical scanner that detected marks based only on overall darkness could be configured so that a mark that was more than (30 ± 2) % dark would count as a vote, a mark that was less than (10 ± 2) % dark would count as a non-vote, and anything in between would be rejected as marginal. (These numbers are just examples to clarify the general intent, and are not necessarily fit for use in an any given election.)

The uncertainty at both ends of the marginal zone is of no consequence. A mark that was exactly 30 % dark would either be accepted as a vote or rejected as marginal and returned to the voter for clarification. Either way, it would not be mistaken for a non-vote. Similarly, a mark that was exactly 10 % dark would either be accepted as a non-vote or rejected as marginal and returned to the voter for clarification. Either way, it would not be mistaken for a vote. (Detectable marks in the lower range are typically hesitation marks, accidental smudges, or damage to the paper.)

In the central count case, rejection of marginal marks is only helpful if someone is going to examine each affected ballot and judge the intent of the voter. If this is not

going to occur, then it is preferable to disable the detection of marginal marks so that every mark is counted either as a vote or as a non-vote. Unfortunately, it is not technically possible to do this without creating the potential for irreproducible tabulation results. For example, if a hypothetical optical scanner that detected marks based only on overall darkness were calibrated to distinguish votes from non-votes using a threshold of (25 ± 2) % darkness, the detection of marks that were between 23 % and 27 % dark would not reproduce on a different scanner of the same kind. Moreover, the detection of marks that happened to fall very close to the actual detection threshold of the scanner as calibrated would not repeat on the same scanner. As the darkness of a mark (or whatever the scanner is measuring) approaches the detection threshold, the signal-to-noise ratio approaches zero. At some point, the noise determines the result that is tabulated.

Short of banning the use of manually-marked paper ballots, which would create a crisis for absentee voting, the best that can be done for this central count case is to prohibit bias in the detection of marginal marks (Requirement III.6.8.5-H) and advise that the detection of marginal marks be made as repeatable as possible (Requirement III.6.8.5-I).

## 3.2.5 Coding conventions

### 3.2.5.1 General

Volume 1, Section 5.2 and Volume 2, Section 5.4 of [6] define coding conventions and a source code review to be conducted by test labs. That material has been substantially revised in these Guidelines.

The requirement to follow coding conventions serves two purposes. First, by requiring specific risk factors to be mitigated, coding conventions support integrity and maintainability of voting system logic. Second, by making the logic more transparent to a reviewer, coding conventions facilitate test lab evaluation of the logic's correctness to a level of assurance beyond that provided by operational testing.

[6] Volume 1, Section 5.2.6 specifies that vendors are permitted to use current best practices in lieu of the coding conventions defined in the VVSG. However, the coding conventions in [6] are not aligned with the modern state of the practice, and if followed, could do more harm than good. The misalignments are (1) that the conventions, some of which were carried over from [1], are out of date, and (2) that the conventions, being limited by the requirement to remain language-neutral, are variously incomplete and/or inappropriate in the context of different programming languages with their different idioms and practices. The vast majority of coding conventions used in practice are tailored to specific programming languages.

In these Guidelines, the few coding conventions that have significant impact on integrity and transparency and that generalize relatively well to different programming languages have been retained, expanded, and made mandatory, while the many coding conventions that are language-sensitive and stylistic in nature, and are made redundant by more recent, publicly available coding

conventions, have been removed in favor of the published conventions. Meanwhile, the evaluation of logical correctness that was underspecified in [6] has been greatly enhanced (see Volume V Section 4.7).

### 3.2.5.2 Structured programming

Note: Specific programming languages are identified to support the discussion. In no case does such identification imply recommendation or endorsement, nor does it imply that the programming languages identified are necessarily the best or only languages acceptable for voting system use.

| CONCEPT | VSS [1][2] / VVSG [6] | ADA [26][29] | C [27][31] | C++ [30][34] | C# [35][38] | JAVA [52] | VISUAL BASIC 8 [53] |
|---|---|---|---|---|---|---|---|
| Sequence | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Loop with exit condition | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| If/Then/Else conditional | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Case conditional | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Named block exit | No | Yes | No | No | No | Yes | No[1] |
| Block-structured exception handling | No | Yes | No | Yes | Yes | Yes | Yes |

Table 3-1 Presence of high-level concepts of control flow in the coding conventions of earlier Guidelines and in various programming languages

Prominent among the requirements addressing logical transparency is the requirement to use high-level control constructs and to refrain from using the low-level arbitrary branch (a.k.a. goto). As is reflected in Table 1, most high-level concepts for control flow were established by the time the first edition of the Guidelines was published and are supported by all of the programming languages that were examined as probable candidates for voting system use as of this iteration. However, two additional concepts have been slower to gain universal support.

The first additional concept, called here the "named block exit," is the ability to exit a specific block from within an arbitrary number of nested blocks, as opposed to only being able to exit the innermost block, without resorting to goto. The absence of named block exit from some languages is not cause for concern here because deeply nested blocks are themselves detrimental to the transparency of logic and most coding conventions encourage restructuring them into separate callable units.

The second additional concept, called here "block-structured exception handling," is the ability to associate exception handlers with blocks of logic, and implicitly, the presence of the exception concept in the programming language. (This simply means try/throw/catch or equivalent statements, and should not be confused with

the specific implementation known as Structured Exception Handling (SEH) [48].[2]) Unlike deeply nested blocks, exceptions cannot be eliminated by restructuring logic. "When exceptions are not used, the errors cannot be handled but their existence is not avoided." [32]

Previous Guidelines required voting systems to handle such errors by some means, preferably using programming language exceptions ([6] I.5.2.3.e), but there was no unambiguous requirement for the programming language to support exception handling. These Guidelines require programming language exceptions because without them, the programmer must check for every possible error condition in every possible location, which both obfuscates the application logic and creates a high likelihood that some or many possible errors will not be checked for. Additionally, these Guidelines require block-structured exception handling because, like all unstructured programming, unstructured exception handling obfuscates logic and makes its verification by the test lab more difficult. "One of the major difficulties of conventional defensive programming is that the fault tolerance actions are inseparably bound in with the normal processing which the design is to provide. This can significantly increase design complexity and, consequently, can compromise the reliability and maintainability of the software." [19]

Existing voting system logic implemented in programming languages that do not support block-structured exception handling can be brought into compliance either through migration to a newer programming language (most likely, a descendant of the same language that would require minimal changes) or through the use of a COTS package that retrofits block-structured exception handling onto the previous language with minimal changes. While the latter path may at first appear to be less work, it should be noted that many library functions may need to be adapted to throw exceptions when exceptional conditions arise, whereas in a programming environment that had exceptions to begin with the analogous library functions would already do this (see Requirement III.5.4.1.5-A.1).

### 3.2.6 Applicability to COTS and borderline COTS products

To clarify the treatment of components that are neither vendor-developed nor unmodified COTS and to allow different levels of scrutiny to be applied depending on the sensitivity of the components being reviewed, new terminology has been introduced: application logic, border logic, configuration data, core logic, COTS (revised definition), hardwired logic, and third-party logic. Using this terminology, requirements have been scoped more precisely than they were in previous iterations of the Guidelines.

The new terminology obviates the software vs. firmware distinction that in practice has sometimes caused confusion. The requirements applying to application logic are not relaxed in any way if that logic is realized in firmware or hardwired logic instead of software. Consequently, the use of hardwired logic in an application logic capacity is all but prohibited, as it is unlikely to meet requirements such as Requirement III.5.4.1.2-A. It is expected that hardwired logic will be limited to COTS and border logic.

By requiring "many different applications," the definition of COTS deliberately prevents any application logic from receiving a COTS designation.

Details regarding the testing implications of these revisions are provided in Volume V Section 1.4.2.

### 3.2.7 Reference models

Volume III Section 7.1 provides an informative model of the entire voting process.

Volume III Section 7.2 provides an informative state model for vote-capture devices to clarify the definitions of voting session and active period, particularly for the case of early voting.

Volume III Section 7.3 provides normative terms and constraints for use in evaluating the correctness of voting system logic. Volume V Section 4.7 describes the verification procedure.

### 3.2.8 Deletions

Requirements regarding the system's handling of unofficial data and reports have been deleted or converted to procedural requirements (Requirement III.6.9.4-B) because the distinction between unofficial and official data is often outside the scope of the voting system. It is now assumed that any vote data present on a voting system and any reports that it generates are potentially official. Requirements on the reconciliation of provisional ballots and other activities involved in the creation of official data are unaffected by this change.

As discussed in Volume III Section 1.4.5.1, prescriptive coding conventions not directly related to integrity and transparency have been deleted in favor of published, credible conventions.

Requirements on system and device availability have been deleted because they did not reflect the logistical overhead of repairing equipment on election day and because it is generally impossible to place precinct equipment back into service after it has been repaired on election day without raising concerns about possible tampering. Instead, Requirement III.5.3.1-B has been tightened to discourage equipment from failing in the first place.

A requirement to designate one set of redundant cast vote records in a DRE as the "primary" set has been deleted because it prejudices the result of an audit.

Requirements that were redundant with the definitions of device classes (e.g., [2] I.2.4.3.2.1.b, all paper-based systems shall allow the voter to punch or mark the ballot to register a vote) have been deleted.

Requirements predicated on state law, local practices, software developed by the voting jurisdiction, and other variables that are indeterminate and untestable in the federal certification process have been deleted.

Requirements that were stated in terms of vague generalities, such as "appropriate" or "intended" options or behavior, for which no precise replacement could be determined and to which no testing value could be ascribed, have been deleted.

Vacuous requirements, such as "Be of any size and shape consistent with its intended use," have been deleted.

Redundant requirements, such as "Comply with the requirements of Section Y" when Section Y is already known to be applicable, have been deleted.

Informative text that was overtaken by changes in the requirements or the structure of the guidelines has been deleted.

Definitions and requirements pertaining to punchcard technology have been deleted.

## 3.2.9 Options Not Standardized in Volume 3

### 3.2.9.1 Merged ballot approach to open primaries

In paper-based systems, open primaries have sometimes been handled by printing a single ballot style that merges the contests from all parties and instructing the voter to vote only in the contests applicable to a single party. This approach requires additional logic in the tabulator to support the rejection or discarding of votes that violate these special instructions, while the approach of assigning different ballot configurations to different parties does not.

Support for the merged ballot approach is not required for a tabulator to satisfy the requirements in these Guidelines for support of open primaries. Although the merged ballot approach does allow the selection of party to be made in private, the issues with usability and tabulation logic that it incurs raise doubt of whether the benefits of standardizing the approach would exceed the cost in added complexity. Voting systems may provide this option as an extension to the Guidelines without breaking conformance.

In systems affected by this issue, assigning different ballot configurations for different parties sacrifices the privacy of the party selection to avoid the issues with usability and tabulation logic. However, the conflict addressed in this trade-off exists only in paper-based systems where poll workers are responsible for giving voters the correct ballot style. DREs and EBPs can provide privacy for the selection of party and then activate a ballot that contains only the contests appropriate to that selection.

### 3.2.9.2 Recall candidacy linked to recall question

In some jurisdictions, a vote for a candidate to replace a recalled official is counted only if the recall question on the same ballot was voted, and sometimes only if it was voted in the affirmative. Like the merged ballot approach to open primaries, the issues with usability and tabulation logic that this approach incurs raise doubt of whether the benefits of standardizing the approach would exceed the cost in added

complexity. Voting systems may provide this option as an extension to the Guidelines without breaking conformance.

### 3.2.9.3 Logic for counting scratch votes

Although initially it seems obvious that a scratch vote in a 1-of-M race should take precedence over a straight party vote, it is less obvious after considering the generalized case of an N-of-M race in which the number of candidates endorsed by the selected party might be less than *N*. Approaches supported by commercially available technology include (1) all straight party selections are cancelled when an explicit selection exists; (2) both straight party and explicit selections are counted; (3) both straight party and explicit selections are counted unless this exceeds *N*, in which case only the explicit selections are counted; (4) both straight party and explicit selections are counted unless this exceeds *N*, in which case straight party selections from the bottom of the list are dropped until the number of selections is reduced to *N*.

These Guidelines do not specify any particular approach to resolving scratch votes, but the approach(es) supported are required to be described in the Voting Equipment User Documentation. See Requirement IV.3.4.4-B.

### 3.2.9.4 Logic for reconciling write-in double votes

Reconciliation of double votes means handling the case where, in an N-of-M contest, a voter has attempted to cast multiple votes for the same candidate using the write-in mechanism. If the voter has selected a ballot position for a given candidate but also written in that candidate's name, or if the voter has written in the same candidate twice using the same spelling or different legal spellings, some corrective action is required—possibly counting only one of the votes, possibly considering the contest to be overvoted. Which action should be specified by jurisdiction election law.

Given a sufficiently robust mechanism for reconciliation of aliases, the reconciliation of double votes can be automated. Once it is known that the name written in identifies the same candidate as the previous ballot position, the tabulator can take whatever action is specified by election law.

These Guidelines do not specify any particular approach to reconciling double votes, but the approach(es) supported are required to be described in the Voting Equipment User Documentation. See Requirement IV.3.4.4-C.

### 3.2.9.5 Logic for ranked order voting

The 1-of-M case of ranked order voting, known by various names including instant runoff voting, requires the definition of criteria for breaking ties. Whereas in plurality voting the voting system need only report the vote totals, a voting system supporting ranked order voting must implement tie-breaking logic in order to be certain of reaching a reportable result.

It is also necessary to decide whether voters may assign equal rankings to two candidates, whether voters are required to rank every candidate and how to compute a result in the case where they do not.

The N-of-M generalization, called single transferable vote, has two additional adjustable parameters: the vote quota (the number of votes required to declare a candidate elected) and the weighting or distribution of votes transferred from candidates that exceed the quota.

Finally, to the extent that a particular ranked order variant defines certain voter responses to be partly or wholly invalid, the manner in which the votes from the affected ballots are to be accounted for and reported (analogous to the reporting of overvotes in plurality contents) must be decided.

Ranked order voting has had insufficient use in the United States to establish clear precedent on how these questions are to be answered; consequently, it would be premature to standardize any particular algorithm or set of algorithms, or attempt to accommodate every possible interpretation.

## 3.3 Volume 4 Changes

### 3.3.1 Separation of Standards on Data To Be Provided from Product Standard

As part of the overall cleanup of the Guidelines, requirements to document certain things or to provide certain information have been moved into a separate volume from functional and performance requirements applying to the voting equipment itself.

### 3.3.2 Separation of requirements on Voting Equipment User Documentation from requirements on Technical Data Package

In previous Guidelines, there were many requirements saying such things as "Provide documentation," "The vendor shall document," "The vendor shall provide detailed descriptions of," or "Documentation shall include" with no indication of whether said documentation should be available to all users (in the Voting Equipment User Documentation) or merely to the test lab (in the Technical Data Package). These Guidelines have clarified which is which.

A copy of the Voting Equipment User Documentation is included in the Technical Data Package.

### 3.3.3 Changes in TDP content

Technical Data Package requirements have been modified to enable verification of voting application logic implemented in software, firmware, and hardware (see Volume V Section 1.4.3.3 and Volume V Section 4.7) and to clarify source code requirements in boundary cases. Operating systems that are customized or that implement application-level voting logic are subject to a source code review.

Numerous changes in wording have been made to clarify the requirements that were carried over from previous Guidelines.

### 3.3.4 Revisions to test lab reports

The Certification Test Plan and Test Report described in [6] required revision to deal with the evolution of certification testing to include standard test methods and an expanded scope of testing.

The chapters on the Certification Test Plan and Test Report have been changed from complete, but informative, outlines of the reports to minimal, but normative, sets of requirements on what the test reports must contain. Test labs are now encouraged to apply relevant external standards, such as [39] and [40], to determine the organization and content of test plans, provided that the information described in Volume IV Chapter 4 does appear in the result.

### 3.3.5 Public Information Package (PIP)

Public assurance that the voting system is fit for use can occur vicariously, through trust in the test lab and election officials; indirectly, through verification that the certification process was responsibly executed; directly, through election verification; or through a combination of these.

Consistent with TGDC Resolution #28-05, standards on data to be provided, called a "Public Information Package," that must be publicly available and published as evidence that the certification process was responsibly executed, now appear in Volume IV Chapter 6.

The same minimal requirements apply to the PIP as apply to the test report, and the same minimal requirements apply to the test plan contained in the PIP as apply to the test plan contained in the test report. The difference is that the test report for the certification authority may contain additional, vendor-proprietary information that would not be suitable for publication.

# 3.4 Volume 5 Changes

## 3.4.1 Reorganization of testing standard

The testing standard has been reorganized to focus on test methods and avoid repetition of requirements from the product standard.

The hardware testing vs. software testing distinction is no longer a guiding principle in the organization of the Guidelines. Although different testing specialties are likely to be subcontracted to different laboratories, the prime contractor must report to the certification authority on the conformity of the system as a whole.

## 3.4.2 Applicability to COTS and borderline COTS products

To clarify the treatment of components that are neither vendor-developed nor unmodified COTS and to allow different levels of scrutiny to be applied depending on the sensitivity of the components being reviewed, new terminology has been introduced: application logic, border logic, configuration data, core logic, COTS (revised definition), hardwired logic, and third-party logic. Table 5 describes the resulting categories.

| CATEGORIES | LEVEL OF SCRUTINY | TESTED? | SOURCE CODE/DATA REQUIRED? | CODING STANDARDS ENFORCED? | SHOWN TO BE CORRECT? |
|---|---|---|---|---|---|
| COTS | Black box | Yes | No | No | No |
| third-party logic, border logic, configuration data | Clear box | Yes | Yes | No | No |
| application logic | Coding standards | Yes | Yes | Yes | No |
| core logic | Logic verification | Yes | Yes | Yes | Yes |

Table 3-2 Levels of scrutiny

COTS may be tested as a black box (i.e., exempted from source code inspections). Whether it is exempted from specific tests depends on whether the certifications and scrutiny that it has previously received suffice for voting system certification purposes. This determination is made by the test lab and justified in the test plan as described in Requirement IV.4.1-D.

Notably, the distinction between software, firmware, and hardwired logic does not impact the level of scrutiny that a component receives; nor are the requirements

applying to application logic relaxed in any way if that logic is realized in firmware or hardwired logic instead of software.

By requiring "many different applications," the definition of COTS deliberately prevents any application logic from receiving a COTS designation.

Finally, the conformity assessment process has been modified to increase assurance that what is represented as unmodified COTS is in fact COTS (Volume V Section 2.5.2.3).

## 3.4.3 New and revised inspections

### 3.4.3.1 Source code review for workmanship

In harmony with revisions to the requirements in Volume III Section 5.4, the source code review for workmanship now focuses on coding practices with a direct impact on integrity and transparency and on adherence to published, credible coding conventions, in lieu of coding conventions embedded within the standard itself.

### 3.4.3.2 Source code review for security

This section is to be provided by STS.

### 3.4.3.3 Logic verification

This revision of the Voluntary Voting System Guidelines adds logic verification to the testing campaign to achieve a higher level of assurance that the system will count votes correctly.

Traditionally, testing methods have been divided into black-box and white-box test design. Neither method has universal applicability; they are useful in the testing of different items.

Black-box testing is usually described as focusing on testing functional requirements, these requirements being defined in an explicit specification. It treats the item being tested as a "black box," with no examination being made of the internal structure or workings of the item. Rather, the nature of black-box testing is to develop and utilize detailed scenarios, or test cases. These test cases include specific sets of input to be applied to the item being tested. The output produced by the given input is then compared to a previously defined set of expected results.

White-box testing (sometimes called clear-box or glass-box testing to suggest a more accurate metaphor) allows one to peek inside the "box," and focuses specifically on using knowledge of the internals of the item being tested to guide the testing procedure and the selection of test data. White-box testing can discover extra non-specified functions that black-box testing wouldn't know to look for and can exercise data paths that would not have been exercised by a fixed test suite. Such extras can only be discovered by inspecting the internals.

Complementary to any kind of operational testing is logic verification, in which it is shown that the logic of the system satisfies certain constraints. When it is impractical to test every case in which a failure might occur, logic verification can be used to show the correctness of the logic generally. However, verification is not a substitute for testing because there can be faults in a proof just as surely as there can be faults in a system. Used together, testing and verification can provide a high level of assurance that a system's logic is correct.

A commonly raised objection to logic verification is the observation that, in the general case, it is exceedingly difficult and often impractical to verify any nontrivial property of software. This is not the general case. While these guidelines try to avoid constraining the design, all voting system designs must preserve the ability to demonstrate that votes will be counted correctly. If a voting system is designed in such a way that it *cannot* be shown to count votes correctly, then that voting system does not satisfy Requirement III.5.1-B.

## 3.4.4 New and revised test methods

### 3.4.4.1 End-to-end testing

The testing specified in [2] and [6] is not required to be end-to-end but may bypass portions of the system that would be exercised during an actual election ([6] II.1.8.2.3).

The use of text fixtures that bypass portions of the system may lower costs and/or increase convenience, but the validity of the resulting testing is difficult to defend. If a discrepancy arose between the results reported by test labs and those found in state acceptance tests, it would likely be attributable to this practice.

Language permitting the use of simulation devices to accelerate the testing process has been tightened to prohibit bypassing portions of the voting system that would be exercised in an actual election, with few exceptions (Volume V Section 2.6.3), and a volume test analogous to the California Volume Reliability Testing Protocol [5] has been specified (Requirement V.5.2.3-D).

### 3.4.4.2 Reliability, accuracy, and probability of misfeed

Previous versions of these Guidelines specified a Probability Ratio Sequential Test [13][14][42] for assessment of reliability and accuracy. No test was specified for assessment of probability of misfeed, though it would have been analogous.

The Probability Ratio Sequential Tests for reliability and accuracy ran concurrent with the temperature and power variation test. There was no specified way to assess errors and failures observed during other portions of the test campaign.

Reliability, accuracy, and probability of misfeed are now assessed using data collected through the course of the entire test campaign. This increases the amount of data available for assessment of conformity to these performance requirements without necessarily increasing the duration of testing.

#### 3.4.4.3 Performance-based usability testing

This section is to be provided by HFP.

#### 3.4.4.4 Open-ended vulnerability testing

This section is to be provided by STS.

# 2 Draft VVSG Recommendations to the EAC

**May 2007 DRAFT**

## VOLUME 2:

## TERMINOLOGY STANDARD

COMMON DEFINITIONS

# Volume 2 Table of Contents

# Volume 2: Terminology Standard

# Chapter 1: Introduction

## 1.1 Scope and Applicability

This part of the Voluntary Voting System Guidelines, the Terminology Standard, defines terms that are used in the Product Standard, Standards on Data to be Provided, and Testing Standard.

Terminology for standardization purposes must be sufficiently precise and formal to avoid ambiguity in the interpretation and testing of the standard. Terms must be defined to mean exactly what is intended in the requirements of the standard, no more and no less. Consequently, this terminology may differ from plain English and be unsuitable for applications that are beyond the scope of the Guidelines. Readers are especially cautioned to avoid comparisons between this terminology and the terminology used in election law.

Any term that is defined neither in this terminology standard nor in any of the referenced documents has its regular (dictionary) meaning.

## 1.2 Audience

The Voluntary Voting System Guidelines are intended primarily for use by:

- Designers and manufacturers of voting systems;
- Test labs performing the analysis and testing of voting systems in support of the national certification process;
- Software repositories designated by the national certification authority or by a state; and
- Test labs and consultants performing the state certification of voting systems.

This part of the Voluntary Voting System Guidelines, the Terminology Standard, is intended primarily for use by vendors and testing labs.

The Terminology Standard may also be of use to election officials in understanding the intent of requirements in the Product Standard.

# Chapter 2: Definitions

Each term is followed by a normative definition. Some terms are further explained with informative text following the indicator "Note:."

**1-of-M voting:** N-of-M voting where N = 1.

**absentee ballot:** Ballot resulting from absentee voting.

**absentee voting:** Voting that can occur unsupervised at a location chosen by the voter.

**Acc-VS:** (Accessible Voting Station) Voting station equipped for individuals with disabilities referred to in 42 USC 15481 (a)(3)(B).

**activation device:** Voting device that creates credentials necessary to initiate a voting session using a specific ballot style. Note: This covers a range of devices such as electronic pollbooks and card activators that encode a token with the appropriate ballot style for the voter. The token is used to activate the correct ballot on a DRE or EBP.

**active period:** Span of time during which a vote-capture device either is ready to begin a voting session or is in use in a voting session. See Volume III Section 7.2.

**administrator:** Role defined in Volume III Section 7.4.

**affiliation:** Association with a political party. Note: Affiliation with a political party does not imply endorsement by that political party. See also, endorsement.

**application logic:** Software, firmware, or hardwired logic from any source that is specific to the voting system, with the exception of border logic.

**archival:** (Media) Able to preserve content for a period of time without significant loss. Note: In the context of voting, the relevant period of time is usually 22 months. See Volume III Section 5.5.3.

**archivalness:** Ability of a medium to preserve its content for a period of time without significant loss. Note: In the context of voting, the relevant period of time is usually 22 months. See Volume III Section 5.5.3.

**audit device:** Voting device that supports processes of verification and/or independent assessment of the performance of the voting system.

**ballot choice:** That with which a vote in a given ballot position is associated, other than a candidate for office; e.g., in response to a ballot question, the value Yes or the value No.

**ballot configuration:** Set of contests in which voters of a particular group (e.g., political party and/or election district) are entitled to vote.

**ballot image:** Electronically produced record of all votes cast by a single voter.

**ballot rotation:** Process of varying the order of the candidate names within a given contest.

**ballot style:** Concrete presentation of a particular ballot configuration. Note: A given ballot configuration may be realised by multiple ballot styles, which may differ in the language used, the ordering of contests and candidates, etc.

**benchmark:** Quantitative point of reference to which the measured performance of a system or device may be compared.

**border logic:** Software, firmware, or hardwired logic that is developed to connect application logic to COTS or third-party logic. Note: Although it is typically developed by the voting system vendor, border logic is constrained by the requirements of the third-party or COTS interface with which it must interact. It is not always possible for border logic to achieve its function while conforming to standard coding conventions. For this reason, border logic should be minimized relative to application logic and where possible, wrapped in a conforming interface. An example of border logic that could not be so wrapped is a customized boot manager that connects a bootable voting application to a COTS BIOS.

**callable unit:** (Of a software program or analogous logical design) Function, method, operation, subroutine, procedure, or analogous structural unit that appears within a module.

**cast ballot:** Ballot in which the voter has taken final action in the selection of candidates and choices and irrevocably confirmed his or her intent to vote as selected. See also read ballot and counted ballot.

**cast vote record:** Archival record of all votes produced by a single voter. Note: Cast vote records may be in electronic, paper, or other form. Electronic cast vote records are also called ballot images.

**CCOS:** (Central Count Optical Scanner) Optical scanner used as a central tabulator. Note: Most machines in this class are special purpose machines that use reflected light to identify marks at specific locations on the ballot. They are designed to read stacks of ballots at a time.

**central election official:** Role defined in Volume III Section 7.4.

**central tabulator:** Tabulator that counts votes from multiple precincts at a central location. Note: Voted ballots are typically placed into secure storage at the polling place and then transported or transmitted to a central tabulator. A tabulator that may be configured for use either in the precinct or in the central location may satisfy the requirements for both *Precinct tabulator* and *Central tabulator*.

**challenged ballot:** Ballot cast by a voter whose eligibility to vote is disputed by someone who is not an election official. See also provisional ballot.

**choice:** Ballot choice.

**class:** (1) Identified set of requirements. (2) Voting systems or devices to which those requirements apply. See Volume III Section 2.6.

**closed primary:** Primary election in which the voter receives a ballot containing only those partisan contests pertaining to the political party with which the voter is affiliated, along with nonpartisan contests and ballot issues presented at the same election. Note: Usually, unaffiliated voters are permitted to vote only on nonpartisan contests and ballot issues.

**combined precinct:** Two or more precincts assigned the same polling place.

**configuration data:** Non-executable input to software, firmware, or hardwired logic.

**conformity assessment:** Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled. ([37])

**contest:** (1) A single decision being put before the voters, e.g., the selection of candidates to fill a particular public office or the approval or disapproval of a constitutional amendment. Note: This term subsumes other terms such as "race" and "question" that are sometimes used to refer to specific kinds of contests. (2) Subdivision of a ballot pertaining to a single decision being put before the voters.

**core logic:** Subset of application logic that is responsible for vote recording and tabulation.

**COTS:** Software, firmware, device or component that is used in the United States by many different people or organizations for many different applications and that is incorporated into the voting system with no vendor- or application-specific modification. Note: (1) The expansion of COTS as Commercial Off-The-Shelf is no longer helpful, since much of what satisfies the requirements is non-commercial software that is not available in stores. The acronym COTS is used here only because it is familiar to the audience. (2) By requiring "many different applications," this definition deliberately prevents any application logic from receiving a COTS designation. (3) See Volume V Section 2.5.2.3 for details.

**counted ballot:** Read ballot whose votes are included in the candidate and choice vote totals. See also cast ballot and read ballot.

**crossover vote:** Scratch vote. Note: The term scratch vote is preferred because crossover vote is more likely to be misinterpreted.

**cross-party endorsement:** Endorsement of a given candidate or choice by two or more political parties.

**cumulative voting:** Voting variation in which the voter is entitled to allocate a fixed number of votes (*N*) over a list of *M* candidates or write-ins. Note: Unlike N-of-M voting, cumulative voting allows the voter to allocate more than one vote to a given candidate.

**CVR:** Cast vote record.

**device:** Functional unit that performs its assigned tasks as an integrated whole.

**DRE:** (Direct Record Electronic) Combination VEBD and tabulator that gathers votes via an electronic voter interface, records voting data and ballot images in memory components, and produces a tabulation of the voting data. Note: A typical DRE presents ballot choices to the voter on an electronic monitor, and after the voter finishes the ballot the voter's choices are stored locally on the computer.

**EBM:** (Electronically-assisted Ballot Marker) VEBD that produces an executed, human-readable paper ballot as a result, and that does not make any other lasting record of the voter's votes. Note: One kind of EBM presents ballot choices to the voter on an electronic monitor; after the voter finishes the ballot, the voter's choices are printed on a paper ballot that is the only record of the voter's choices. However, vote-by-telephone systems that are in use at the time of this writing are also EBMs. The voter uses an audio interface (remotely) and a paper ballot is produced (centrally). An EBM may mark ballot positions on a pre-printed ballot or it may print an entire ballot (the latter kind are called EBPs); however, in any event, the ballot produced is assumed to be human-readable and comparable to an MMPB.

**EBP:** (Electronic Ballot Printer) EBM that prints an entire ballot, including ballot style-dependent content.

**ECOS:** (EMPB-Capable Optical Scanner) Optical scanner used to count EMPBs.

**election district:** Administrative division in which voters are entitled to vote in contests that are specific to that division, such as those for state senators and delegates. Note: An election district may overlap multiple precincts, and a precinct may overlap multiple election districts (see split precinct).

**election judge:** Role defined in Volume III Section 7.4.

**election official:** Central election official, election judge, or poll worker.

**election verification:** Confirmation that all recorded votes were counted correctly. See also voter verification.

**electronic device:** Device that uses electricity.

**electronic voter interface:** Component of an electronic vote-capture device that communicates ballot information to the voter and accepts input from the voter.

**EMPB:** (EBM-Marked Paper Ballot) Ballot marked by an EBM.

**EMS:** (Election Management System) Tabulator used to prepare ballots and programs for use in casting and counting votes and to consolidate, report, and display election results. Note: This device receives results data from the vote-capture devices, accumulates the results, and reports the accumulated results. Typically, the Election Management System will interact with several different classes of voting devices. The EMS receives election results from electronic media devices in one or more of four connections: modem, local bus, direct serial, and/or local area ethernet.

**end-to-end:** (1) (Security) Supporting both voter verification and election verification. (2) (Generically) Covering the entire elections process, from election definition through the reporting of final results.

**endorsement:** Approval by a political party, e.g., as the candidate that the party elects to field in a particular contest and/or as the candidate that should receive straight party votes. A candidate or choice may be endorsed by more than one party. See also, affiliation.

**error rate:** Ratio of the number of errors that occur to the volume of data processed. ([2] I.3.2.1) Note: The specific error rate used in the benchmark for voting system accuracy is report total error rate.

**failure:** (Voting system reliability) 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. (Source: Expanded from [2] I.3.4.3.) Note: 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. Misfeeds of ballots into optical scanners are handled by a separate benchmark (Requirement III.6.8.4-C), so these are not included as failures for the general reliability benchmark.

**failure rate:** Ratio of the number of failures that occur to the volume of data processed. Note: Failures may be divided e.g. into user-serviceable and non-user-serviceable categories, and the measure of volume varies by device class.

**find:** Determine and deliver a finding. (Based on [47] definition #11.)

**finding:** Result of a formal evaluation by a test lab or accredited expert; verdict. (Based on [47] definition #6.)

**firmware:** Executable logic stored in nonvolatile memory.

**general election:** Election in which there are no partisan contests.

**hardwired logic:** Logic implemented through the design of an integrated circuit; the programming of a Programmable Logic Device (PLD), Field-Programmable Gate Array (FPGA), Peripheral Interface Controller (PIC), or similar; the integration of smaller hardware components; or mechanical design (e.g., as in lever machines).

**hesitation mark:** Small dot made by resting the point of a writing utensil on a ballot.

**implementation statement:** Statement by a vendor indicating the capabilities, features, and optional functions and extensions that have been implemented in a voting system.

**in-person voting:** Voting that occurs at a polling place under the supervision of poll workers.

**inspection:** Examination of a product design, product, process or installation and determination of its conformity with specific requirements or, on the basis of professional judgement, with general requirements. ([37])

**instant runoff voting:** Ranked order voting.

**logic defect:** Fault in software, firmware, or hardwired logic.

**marginal mark:** Mark within a voting target that does not conform to vendor specifications for a reliably detectable vote. Note: See Volume III Section 1.4.4. The word "marginal" refers to the limit of what is detectable by an optical scanner, not the margin of the page. Marks that are outside of voting targets are called extraneous marks.

**MCOS:** (MMPB-Capable Optical Scanner) Optical scanner used to count MMPBs.

**misfeed rate:** Ratio of the misfeed total to the total ballot volume (see Requirement V.5.3.4-B).

**MMPB:** (Manually-Marked Paper Ballot) (1) Vote-capture device consisting of a paper ballot and a writing utensil. (2) Paper ballot that was marked by a person using a writing utensil.

**module:** Structural unit of software or analogous logical design, typically containing several callable units that are tightly coupled. Note: Modular design requires that inter-module coupling be loose and occur over defined interfaces. A module should contain all elements needed to compile or interpret successfully and have limited access to data in other modules. A module should be substitutable with another module whose interfaces match the original module. In software, a module typically corresponds to a single source code file or a source code / header file pair. In object-oriented languages, this typically corresponds to a single class of object.

**N-of-M voting:** Voting variation in which the voter is entitled to allocate a fixed number of votes (*N*) over a list of *M* candidates or write-ins, with the constraint that at most 1 vote may be allocated to a given candidate. See also cumulative voting.

**non-executable:** Declarative or informative in nature; not subject to interpretation as a sequence of imperative instructions as in a functional programming language.

**nonpartisan contest:** Contest such that eligibility to vote in that contest is independent of political party affiliation or lack thereof.

**nonvolatile memory:** Memory in which information can be stored indefinitely with no power supplied. Note: Read-only memory (ROM), programmable read-only memory (PROM), erasable programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), and flash memory are examples of nonvolatile memory.

**open primary:** Primary election in which the voter may choose a political party at the time of voting and vote in partisan contests associated with that party, along

with nonpartisan contests and ballot issues presented at the same election. Note: Also known as pick-your-party primary. Some states require voters to publicly declare their choice of party at the polling place, after which the poll worker provides or activates the appropriate ballot. Other states allow the voters to make their choice of party within the privacy of the voting booth. Voters also are permitted to vote on nonpartisan contests and ballot issues that are presented at the same election.

**operational test:** Test conducted on voting equipment in an active (operational) state by a procedure in the form of a scientific experiment.

**operational testing:** Testing using operational tests.

**optical scanner:** Tabulator that counts votes that were recorded by means of marks made on the surface of a paper ballot.

**paper-based device:** Device that records votes, counts votes, and/or produces a report of the vote count from votes cast on paper cards or sheets.

**partisan contest:** Contest such that eligibility to vote in that contest is restricted based on political party affiliation or lack thereof. Note: The affiliation might be the registered affiliation of the voter or it might be an affiliation declared at the time of voting. See closed primary, open primary.

**PCOS:** (Precinct Count Optical Scanner) Optical scanner used as a precinct tabulator. Note: A PCOS is a special purpose scanner designed to enable the voter to feed his or her own paper ballot—one ballot at a time.

**poll worker:** Role defined in Volume III Section 7.4.

**precinct:** Administrative division in which voters cast ballots at the same polling place. Note: It is possible for two or more precincts to cast ballots at a given polling place. See combined precinct.

**precinct tabulator:** Tabulator that counts votes at the polling place. Note: These devices typically tabulate ballots as they are cast and print the results after the close of polls. For DREs and some paper-based systems, these devices provide electronic storage of the vote count and may transmit results to a central location over public telecommunication networks. A tabulator that may be configured for use either in the precinct or in the central location may satisfy the requirements for both *Precinct tabulator* and *Central tabulator*.

**primary election:** Election in which there are partisan contests. Note: Primary elections are held to determine which candidate will represent a political party in a subsequent general election.

**profile:** Subset of a standard for a particular constituency or purpose that defines the requirements, options, constraints, and extensions that are specific to that constituency or purpose.

**programmed device:** Electronic device that includes application logic.

**provisional ballot:** Ballot cast by a voter whose eligibility to vote is disputed by an election official. See also challenged ballot.

**ranked order voting:** Voting variation in which voters express their intent by ordering candidates from strongest to weakest preference. Note: Implementations of ranked order voting differ in whether voters are required to rank every candidate and in the algorithm used to determine a winner or winners.

**read ballot:** Cast ballot that has been processed. Note: A read ballot may or may not be counted. For example, an optical scan cast ballot that has been scanned successfully is a read ballot. See also cast ballot and counted ballot.

**record:** Preserved evidence of activities performed or results achieved (e.g., forms, reports, test results).

**relevant contest:** Contest appearing in a ballot style or ballot associated with a given reporting context. Note: If a contest is included in a ballot style associated with a given reporting context, that contest is relevant even if no ballots of that style were counted.

**report:** Self-contained, timestamped, archival record, such as a printout or analogous electronic file, that is produced at a specific time and subsequently protected from modification.

**reporting context:** Scope within which reported totals or counts are calculated; e.g., precinct or election district. Note: Reporting contexts may overlap in complex ways; e.g., in the case of split precincts, there is not a simple containment relationship between election districts and precincts.

**report total error rate:** Ratio of the report total error to the report total volume (see Requirement V.5.3.3-B).

**review-required ballot:** Ballot that is flagged or separated for some form of manual processing.

**scratch vote:** Explicit vote that conflicts with the vote(s) implied by a straight party vote. ([44]) Note: Also called crossover vote.

**split precinct:** Precinct serving voters from two or more administrative divisions, such as election districts, that require different ballot configurations.

**straight party voting:** Voting variation in which the selection of a political party in a special contest implies votes for the candidates endorsed by that party in all straight-party-votable contests on the ballot.

**tabulator:** Device that counts votes.

**testing:** Determination of one or more characteristics of an object of conformity assessment, according to a procedure. Note: "Testing" typically applies to materials, products or processes. ([37])

**third-party logic:** Software, firmware, or hardwired logic that is neither application logic nor COTS; e.g., general-purpose software developed by a third party that is

either customized (e.g., ported to a new platform, as is Windows CE) or not widely used, or code generated by a COTS package.

**thought mark:** Hesitation mark.

**VEBD:** (Voter-Editable Ballot Device) Vote-capture device that gathers votes via an electronic voter interface and allows the voter to alter previously made selections without spoiling the ballot.

**VEBD-A:** (Audio VEBD) VEBD that communicates ballot information to the voter using sound.

**VEBD-V:** (Video VEBD) VEBD that communicates ballot information to the voter using light (e.g., via a typical electronic display).

**vote-capture device:** Device that is used directly by a voter to vote a ballot.

**voter:** Role defined in Volume III Section 7.4.

**voter verification:** Confirmation that all votes were recorded as the voter intended. See also election verification. Note: It is debatable whether an ambiguous record, such as an MMPB containing marginal marks or a punchcard containing dimpled or hanging chads, satisfies the intent of voter verification. On the one hand, the paper record was produced directly by the voter and deliberately cast, so arguably it represents the intent of the voter. On the other hand, a conscientious voter would never intentionally cast an ambiguous ballot.

**voting device:** Device that is part of the voting system. Note: Components and materials that are vital to the function of the voting device within the voting system, such as smart cards and ballot printers, are considered parts of the device for the purpose of certification testing.

**voting process:** Entire array of procedures, people, resources, equipment and locations associated with the conduct of elections. See also, voting system.

**voting session:** (1) Span of time beginning when a ballot is enabled or activated and ending when that ballot is printed, cast or spoiled (depending on the technology used). See Volume III Section 7.2. (2) Interaction between the voter and vote-capture device that occurs during that span of time.

**voting station:** Vote-capture device with its privacy enclosure.

**voting system:** Equipment (including hardware, firmware, and software), materials, and documentation used to define elections and ballot styles, configure voting equipment, identify and validate voting equipment configurations, perform logic and accuracy tests, activate ballots, capture votes, count votes, reconcile ballots needing special treatment, generate reports, transmit election data, archive election data, and audit elections. See also, voting process.

**VVPAT:** (Voter-Verified Paper Audit Trail) DRE that supports voter verification using a VVPR.

**VVPR:** (Voter-Verified Paper Record) Paper CVR produced by a vote-capture device that supports voter verification (e.g., VVPAT and EBM).

**write-in:** Vote for a candidate who is explicitly named by the voter in lieu of choosing a candidate who is already listed on the ballot. Note: This does not preclude writing in the name of a candidate who is already listed on the ballot..

3

# Draft VVSG Recommendations to the EAC

**May 2007 DRAFT**

**VOLUME 3:**

**PRODUCT STANDARD**

VOTING EQUIPMENT REQUIREMENTS

# Volume 3 Table of Contents

# Volume 3: Product Standard

# Chapter 1: Introduction

## 1.1 Scope and Applicability

This part of the Voluntary Voting System Guidelines, the Product Standard, contains requirements applying to the voting system and the voting devices that it contains.

The overall goal of the Guidelines is to produce systems with the following attributes:

- Secure
- Accurate
- Reliable
- Usable
- Accessible
- Fit for their intended use

The certifying authority may consider not only whether a voting system is in conformance with the requirements, but also whether it meets these higher level goals.

## 1.2 Audience

The Voluntary Voting System Guidelines are intended primarily for use by:

- Designers and manufacturers of voting systems;
- Test labs performing the analysis and testing of voting systems in support of the national certification process;
- Software repositories designated by the national certication authority or by a state; and
- Test labs and consultants performing the state certification of voting systems.

This part of the Voluntary Voting System Guidelines, the Product Standard, is intended primarily for use by vendors and testing labs.

The Product Standard may also be of use to election officials in setting requirements for voting systems in requests for proposals.

# Chapter 2: Conformance Clause

## 2.1 Scope and Applicability

The Voluntary Voting System Guidelines are intended primarily for use by:

- Designers and manufacturers of voting systems;
- Test labs performing the analysis and testing of voting systems in support of the national certification process;
- Software repositories designated by the national certification authority or by a state; and
- Test labs and consultants performing the state certification of voting systems.

The Guidelines may also be of use to election officials in setting requirements for voting systems in requests for proposals.

The Guidelines include:

- A product standard (Volume III) defining requirements that apply to voting systems that vendors produce;
- Standards on data to be provided (Volume IV) defining requirements that apply to documentation, reports, and other information that vendors and test labs deliver;
- A testing standard (Volume V) defining test methods that test labs implement; and
- A terminology standard (Volume II) defining terms used in the foregoing.

## 2.2 Structure of Requirements

Each volume of the Guidelines is organized into hierarchically organized sections and subsections that address topics of interest. Sections typically begin with prose explaining the general purpose, etc.—this is informative background to help understand the requirements. Sections also contain requirements, which are the hard and fast rules to be followed for conformance. The Guidelines carefully distinguish normative requirements from informative context using conventions that are explained below.

Each voting system requirement is identified according to a hierarchical scheme in which higher-level, "parent" requirements (such as "provide accessibility for visually impaired voters") are supported by lower-level subrequirements (e.g., "provide an audio-tactile interface"). "Parent" requirements have identifiers consisting of a

section number suffixed by a letter (e.g., 1.2.3-A) and are indicated by straight arrows in the left margin. Subrequirements have identifiers consisting of their parent requirements' identifiers suffixed by a digit (e.g., 1.2.3-A.1) and are indicated by bent arrows in the left margin.

Each requirement is composed of a descriptive title, normative text, optional informative discussion, and two fields labelled *Applies to:* and *Test reference:*.

The applicability of a requirement is specified with the *Applies to:* field, which indicates the class(es) of voting systems or devices to which the requirement applies. Classes are defined in Volume III Section 2.6.

A requirement having *N* different classes separated by commas in its *Applies to:* field is equivalent to *N* separate requirements that repeat the same text, each repetition applying to one of the listed classes.

The scope of a parent requirement is inherited by its subrequirements unless they explicitly specify a narrower scope. The scope may be narrowed through a generic relation (e.g., *DRE* is a subclass of *Vote-capture device*) or a partitive relation (e.g., a *DRE* is part of a *Voting system*). If no narrowing is needed then the *Applies to:* field may be omitted.

The *Test reference:* field indicates the general testing approach or approaches that would be used to assess conformity with the requirement.

## 2.3 Normative Language

The following keywords are used to convey conformance requirements:

- **Shall** indicates a mandatory requirement to do something. Synonymous with "is required to."
- **Is prohibited** indicates a mandatory requirement not to do something. Synonymous with "**SHALL** not."
- **Should, Is encouraged** indicate an optional recommended action, one that is particularly suitable, without mentioning or excluding others. Synonymous with "is permitted and recommended."
- **May** indicates an optional, permissible action. Synonymous with "is permitted."

Requirements are further indicated by the presence of green text and arrows in the left margin. Requirements are directly applicable to achieving conformance to the Guidelines.

Informative parts of this document include discussion, examples, extended explanations, and other matter that is necessary for proper understanding of the Guidelines and conformance to them. Informative text may serve to clarify requirements, but it is not otherwise applicable to achieving conformance to the Guidelines.

## 2.4 Conformance Designations

A voting system conforms to the product standard if all stated requirements that apply to the voting system and its constituent devices are fulfilled. The implementation statement (see Volume III Section 2.5) declares the capabilities, features and optional functions that have been implemented and are subject to conformance and certification testing.

There is no concept of partial conformance—neither that a voting system is *x* % conforming, nor that a device that is not a complete voting system by itself is conforming. Individual devices of voting systems are not tested or certified except as parts of complete systems.[3]

## 2.5 Implementation Statement

An implementation statement documents the requirements that have been implemented by the voting system, the optional features and capabilities supported by the voting system, and any extensions (i.e., additional functionality beyond what is defined in the Guidelines) that it implements.

An implementation statement may take the form of a checklist to be completed for each voting system submitted for certification. It is used by test labs to identify the conformity assessment activities that are applicable.

→ **2.5-A** Implementation statement

An implementation statement ***SHALL*** include:

1. Full product identification of the voting system, including version number or timestamp;
2. Separate identification of each device (see below) that is part of the voting system;
3. Version of VVSG to which certification is desired;
4. Classes implemented (see Volume III Section 2.6.3);
5. Device capacities and limits (especially those appearing in Volume III Section 7.3.1);
6. List of languages supported; and
7. Signed attestation that the foregoing accurately characterizes the system submitted for testing.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

This requirement addresses many issues about the scope of certification and uncertainty whether particular features have been implemented in voting systems.

A keyboard, mouse or printer connected to a programmed voting device, as well as any optical drive, hard drive or similar component installed within it, are considered

components of the voting device, not separate devices. The voting device is "responsible" for these components—e.g., a DRE must prevent unauthorized flashing of the firmware in its optical drive or other components that could be subverted to manipulate vote outcomes.

Specified capacities and limits should include the limit (if any) on the length of a candidate name that the system can process and display without truncation and similar limits for any other text fields whose usable or practically usable sizes are bounded. If the system provides a way to access the entirety of a long name even when it does not fit the width of the display and does not use any data structures that would force truncation, such a limit might not apply.

Vendors may wish to contact their intended testing labs in advance to determine if those labs can supply them with an implementation statement *pro forma* to facilitate meeting this requirement.

*Source:* *New requirement.*

*Impact:* *Signature added per SB advice 2006-07-20.*

# 2.6 Classes

## 2.6.1 Voting device terminology

| TERM | DEFINITION |
|---|---|
| Voting device | Device that is part of the voting system. *Voting device* subsumes *Activation device*, *Vote-capture device*, *Paper-based device*, *Electronic device*, *Tabulator*, *Audit device*, and all device voting variations (*In-person voting device*, etc.). |
| Activation device | Voting device that creates credentials necessary to initiate a voting session using a specific ballot style. Note: This covers a range of devices such as electronic pollbooks and card activators that encode a token with the appropriate ballot style for the voter. The token is used to activate the correct ballot on a DRE or EBP. |
| Vote-capture device | Device that is used directly by a voter to vote a ballot. *Vote-capture device* subsumes *Acc-VS*, *VEBD*, and *MMPB*. |
| Paper-based device | Device that records votes, counts votes, and/or produces a report of the vote count from votes cast on paper cards or sheets. *Paper-based device* subsumes *MMPB*, *EBM*, and *Optical scanner*. |
| Electronic device | Device that uses electricity. *Electronic device* subsumes *Programmed device*. |
| Programmed | Electronic device that includes application logic. *Programmed* |

| TERM | DEFINITION |
|---|---|
| device | *device* subsumes *VEBD*, *Optical scanner*, and *EMS*. |
| Tabulator | Device that counts votes. *Tabulator* subsumes *DRE*, *Optical scanner*, *EMS*, *Precinct tabulator* and *Central tabulator*. |
| Precinct tabulator | Tabulator that counts votes at the polling place. Note: These devices typically tabulate ballots as they are cast and print the results after the close of polls. For DREs and some paper-based systems, these devices provide electronic storage of the vote count and may transmit results to a central location over public telecommunication networks. A tabulator that may be configured for use either in the precinct or in the central location may satisfy the requirements for both *Precinct tabulator* and *Central tabulator*. *Precinct tabulator* subsumes *PCOS*. |
| Central tabulator | Tabulator that counts votes from multiple precincts at a central location. Note: Voted ballots are typically placed into secure storage at the polling place and then transported or transmitted to a central tabulator. A tabulator that may be configured for use either in the precinct or in the central location may satisfy the requirements for both *Precinct tabulator* and *Central tabulator*. *Central tabulator* subsumes *CCOS*. |
| Audit device | Voting device that supports processes of verification and/or independent assessment of the performance of the voting system. |
| VEBD | (Voter-Editable Ballot Device) Vote-capture device that gathers votes via an electronic voter interface and allows the voter to alter previously made selections without spoiling the ballot. *VEBD* subsumes *VEBD-A*, *VEBD-V*, *DRE* and *EBM*. |
| Acc-VS | (Accessible Voting Station) Voting station equipped for individuals with disabilities referred to in 42 USC 15481 (a)(3)(B). |
| MMPB | (Manually-Marked Paper Ballot) Vote-capture device consisting of a paper ballot and a writing utensil. |
| EBM | (Electronically-assisted Ballot Marker) VEBD that produces an executed, human-readable paper ballot as a result, and that does not make any other lasting record of the voter's votes. Note: One kind of EBM presents ballot choices to the voter on an electronic monitor; after the voter finishes the ballot, the voter's choices are printed on a paper ballot that is the only record of the voter's choices. However, vote-by-telephone systems that are in use at the time of this writing are also EBMs. The voter uses an audio interface (remotely) and a paper ballot is produced (centrally). An EBM may mark ballot positions on a pre-printed ballot or it may print an entire ballot (the latter kind are called EBPs); however, in any event, the |

| TERM | DEFINITION |
|---|---|
| | ballot produced is assumed to be human-readable and comparable to an MMPB. *EBM* subsumes *EBP*. |
| EBP | (Electronic Ballot Printer) EBM that prints an entire ballot, including ballot style-dependent content. |
| VEBD-A | (Audio VEBD) VEBD that communicates ballot information to the voter using sound. |
| VEBD-V | (Video VEBD) VEBD that communicates ballot information to the voter using light (e.g., via a typical electronic display). |
| DRE | (Direct Record Electronic) Combination VEBD and tabulator that gathers votes via an electronic voter interface, records voting data and ballot images in memory components, and produces a tabulation of the voting data. Note: A typical DRE presents ballot choices to the voter on an electronic monitor, and after the voter finishes the ballot the voter's choices are stored locally on the computer. *DRE* subsumes *VVPAT*. |
| VVPAT | (Voter-Verified Paper Audit Trail) DRE that supports voter verification using a VVPR. |
| Optical scanner | Tabulator that counts votes that were recorded by means of marks made on the surface of a paper ballot. *Optical scanner* subsumes *ECOS*, *MCOS*, *PCOS* and *CCOS*. |
| ECOS | (EMPB-Capable Optical Scanner) Optical scanner used to count EMPBs. |
| MCOS | (MMPB-Capable Optical Scanner) Optical scanner used to count MMPBs. |
| PCOS | (Precinct Count Optical Scanner) Optical scanner used as a precinct tabulator. Note: A PCOS is a special purpose scanner designed to enable the voter to feed his or her own paper ballot—one ballot at a time. |
| CCOS | (Central Count Optical Scanner) Optical scanner used as a central tabulator. Note: Most machines in this class are special purpose machines that use reflected light to identify marks at specific locations on the ballot. They are designed to read stacks of ballots at a time. |
| EMS | (Election Management System) Tabulator used to prepare ballots and programs for use in casting and counting votes and to consolidate, report, and display election results. Note: This device receives results data from the vote-capture devices, accumulates the results, and reports the accumulated results. Typically, the Election Management System will interact with several different classes of voting devices. The EMS receives election results from electronic media devices in one or more of four connections: modem, local bus, direct serial, and/or |

| TERM | DEFINITION |
|---|---|
| | local area ethernet. |

Table 2-1 Voting device terminology

## 2.6.2 Classes overview

A class simultaneously identifies a set of requirements and a set of voting systems or devices to which those requirements apply. The purpose of classes is to categorize requirements into related groups of functionality that apply to different types of voting systems and devices.

Classes may subsume other classes. For example, *Paper-based device* subsumes *MMPB*, *EBM*, and *Optical scanner*. The subsuming class is called the superclass while the subsumed classes are called subclasses. A group of related classes forms a classification hierarchy or lattice.

Subclasses "inherit" the requirements of their superclasses. Additionally, a subclass may further constrain a class by adding new requirements. However, a subclass is not allowed to relax or remove requirements inherited from a superclass.

There is no assumption of disjointness for classes. Unless otherwise specified, a voting system or device may belong to several classes simultaneously, such as *Acc-VS* and *DRE* to signify an accessible DRE device.

A voting system conforms to a class if all stated requirements identified by that class are fulfilled. Since subclasses are not allowed to relax or remove requirements inherited from a superclass, it is true in all cases that a voting system or device conforming to a subclass also conforms to all of its superclasses. For example, a voting system conforming to any subclass of *Voting system* fulfills the general requirements that apply to all voting systems.

The classification mechanism is useful in many different contexts when there is a need to identify specific portions of the VVSG. Table 3 provides several examples.

| CONTEXT | USE |
|---|---|
| VVSG | Requirements applicable to a given class |
| Implementation statement | This system conforms to a specified class |
| Conformity assessment | Tests and reviews applicable to the specified class |
| Certification | Scope of certification is the specified class |
| Declaration of conformity | This product is certified to that class |
| Request for proposals | Seeking to procure a system conforming to a specified class |

Table 2-2 Use of classes in different contexts

Figure 1 and Figure 2 repeat in pictorial form the classification hierarchies that are defined in the next section to illustrate their high-level structure. A class is represented by an oval containing the name of the class. When two classes are connected by a line, this indicates that the higher class subsumes the lower one.

## 2.6 Classes

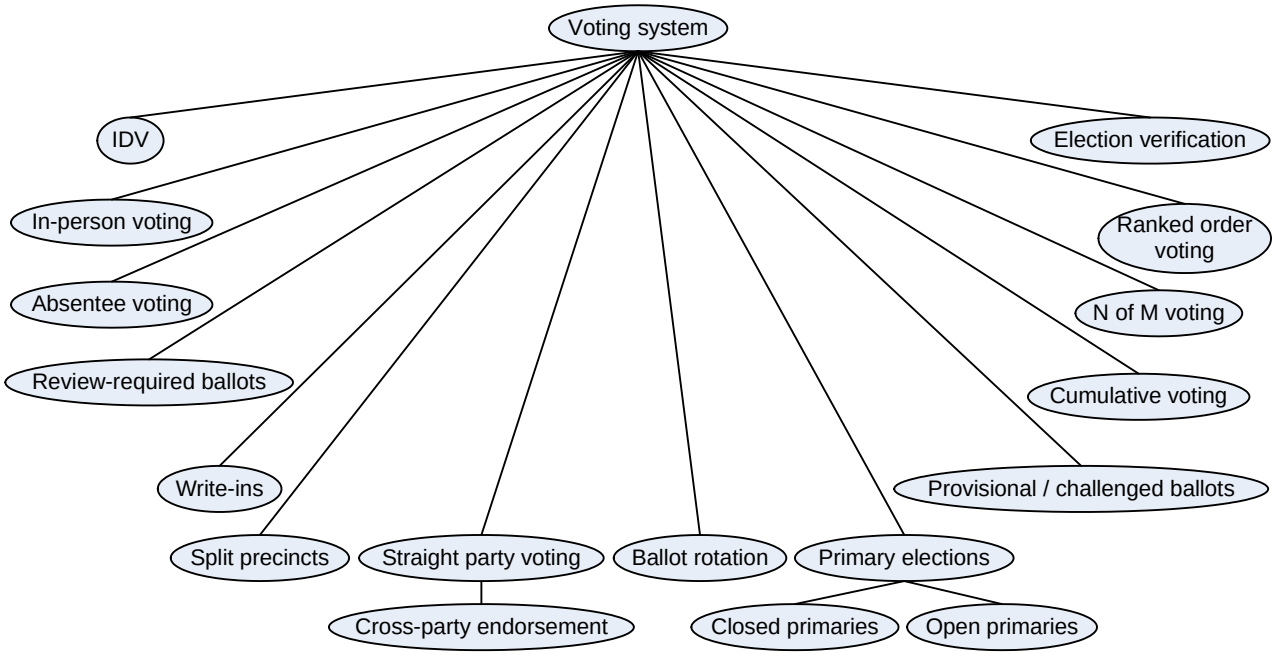



Figure 2-1 Voting system classes

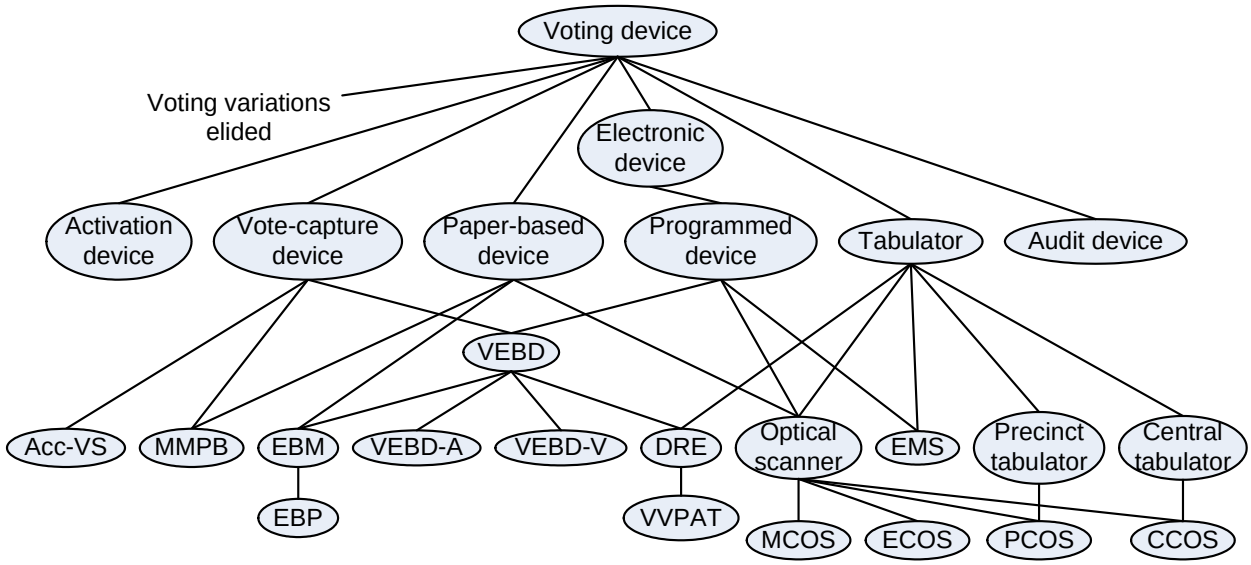



Figure 2-2 Voting device classes

## 2.6.3 Classes identified in implementation statement

**2.6.3-A** Implementation statement, system classes

An implementation statement for a voting system ***SHALL*** identify all applicable classes from Volume III Section 2.6.3.1.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1, Requirement V.4.2-C*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

**2.6.3-B** Implementation statement, device classes

For each distinct device included in the system, an implementation statement for a voting system ***SHALL*** identify:

1. All applicable classes from Volume III Section 2.6.3.2; and
2. All applicable classes from Volume III Section 2.6.3.3.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1, Requirement V.4.2-C*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

**2.6.3-C** Implementation statement, voting variations documentation references

For each of the voting variations identified per Requirement III.2.6.3-A and Requirement III.2.6.3-B, the implementation statement ***SHALL*** cite the specific section or sections of the Voting Equipment User Documentation where the use of that voting variation is documented.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Voting variations are enumerated in Volume III Section 2.6.3.1 and Volume III Section 2.6.3.2.

*Source:* *[7], modified per 2006-07-20 input.*

*Impact:* *Click here to add the Impact*

### 2.6.3.1 Supported voting variations (system-level)

The classes enumerated in this section identify voting variations supported by the voting system. Although the intent of most is apparent from the applicable requirements, the following may require additional explanation.

Conformance to the *Write-ins* class indicates that the voting system is capable of end-to-end processing of write-in votes, including reconciliation of write-ins and generation of a final, consolidated report that includes individual tallies for all write-in candidates. If the voting system requires that write-in votes be counted manually, then it does not satisfy Requirement III.5.2-D and therefore does not conform to the *Write-ins* class. However, it may conform to the Review-required ballots class (see below).

The same principle applies to the Absentee voting class and the *Provisional / challenged ballots* class. If the counting of these ballots is external to the voting system, then the system does not satisfy Requirement III.5.2-B or Requirement III.5.2-I and therefore does not conform to the *Absentee voting* or *Provisional / challenged ballots* class, respectively.

Conformance to the *Review-required ballots* class indicates that the voting system is capable of flagging or separating ballots for later processing and including the results of that processing in the reported totals. If the consolidation of counts from review-required ballots with counts from other ballots is external to the voting system, then the system does not satisfy Requirement III.6.9.3.3-I and therefore does not conform to the *Review-required ballots* class.

In some systems, write-in votes are counted as anonymous ballot positions, and these votes are assigned to candidates through manual post-processing only if the election is close enough to warrant the effort. Although this approach does not conform to the *Write-ins* class, the system's handling of write-in positions is identical to its handling of other ballot positions, so the behavior is testable.

Choose all that apply.

- In-person voting
- Absentee voting
- Provisional / challenged ballots
- Review-required ballots
- Primary elections
  - Closed primaries

    - Open primaries
- Write-ins
- Ballot rotation
- Straight party voting
    - Cross-party endorsement
- Split precincts
- N of M voting
- Cumulative voting
- Ranked order voting
- IDV (Independent Dual Verification)
- Election verification

#### 2.6.3.2 Supported voting variations (device-level)

It is necessary to specify voting variations at the device level as well as the system level because a system may support a given voting variation without having that support in every device. For example, a system may support absentee voting by having absentee ballot support in one special tabulator and in the central EMS. However, for the most part, these should agree with the variations claimed at the system level.

*IDV* (Independent Dual Verification) and *Election verification* do not appear in this list because they are strictly system-level concepts.

Choose all that apply.

- In-person voting device
- Absentee voting device
- Provisional / challenged ballots device
- Review-required ballots device
- Primary elections device
- Closed primaries device
- Open primaries device
- Write-ins device
- Ballot rotation device
- Straight party voting device
- Cross-party endorsement device
- Split precincts device
- N of M voting device
- Cumulative voting device
- Ranked order voting device

#### 2.6.3.3 Voting device classes

The classes enumerated in this section identify different types of voting devices. Choose all that apply.

- Activation device
- Vote-capture device
- Paper-based device
- Electronic device
  - Programmed device
- Tabulator
  - Precinct tabulator
  - Central tabulator
- Audit device
- Acc-VS (accessible voting station)
- MMPB (Manually-Marked Paper Ballot)
- VEBD (Voter-Editable Ballot Device)
  - EBM (Electronically-assisted Ballot Marker)
    - EBP (Electronic Ballot Printer)
  - VEBD-A (Audio VEBD)
  - VEBD-V (Video VEBD)
  - DRE (Direct Record Electronic)
    - VVPAT (Voter-Verified Paper Audit Trail)
- Optical scanner
  - MCOS (MMPB-Capable Optical Scanner)
  - ECOS (EMPB-Capable Optical Scanner)
- EMS (Election Management System)

*PCOS* is implied if *Precinct tabulator* and *Optical scanner* are identified. *CCOS* is implied if *Central tabulator* and *Optical scanner* are identified. At least one of *ECOS* and *MCOS* must be identified if *Optical scanner* is identified.

### 2.6.4 Semantics of classes

A class simultaneously identifies a set of requirements and a set of voting systems or devices to which those requirements apply.

For a class C, let S(C) represent the set of voting systems or devices identified by C and let R(C) represent the set of requirements applicable to those voting systems or devices.

A subclass identifies a superset of the requirements and a subset of the voting systems or devices identified by its superclass. A voting system that conforms to a subclass necessarily conforms to its superclass. The superclass is said to *subsume* the subclass.

If class $C_1$ subsumes $C_2$, then

$$R(C_2) \supseteq R(C_1)$$

$$S(C_2) \subseteq S(C_1)$$

A class may have multiple superclasses. Let P(C) represent the set of superclasses of C. Then

$$R(C) \supseteq \bigcup_{x \in P(C)} R(x)$$

$$S(C) \subseteq \bigcap_{x \in P(C)} S(x)$$

Given classes $C_3$ and $C_4$, one may derive a new subclass by combining $C_3$ and $C_4$. By default, this new class identifies the union of the requirements and the intersection of the voting systems or devices identified by $C_3$ and $C_4$. However, additional requirements that applied to neither superclass may apply specifically to the new subclass. The combining operation on classes is represented with a wedge ($\wedge$).

$$R(C_3 \wedge C_4) \supseteq R(C_3) \cup R(C_4)$$

$$S(C_3 \wedge C_4) = S(C_3) \cap S(C_4)$$

A class that is derived by combining classes that are disjoint is said to be incoherent and identifies no voting systems or devices. The set of requirements identified by an incoherent class is likely to be self-contradictory.

## 2.7 Extensions

Extensions are additional functions, features, and/or capabilities included in a voting system that are not defined in the Guidelines. To accommodate the needs of states that may impose additional requirements and to accommodate changes in technology, these Guidelines allow extensions. However, as extensions are essentially subclasses of one or more classes defined in these Guidelines, they are subject to the integrity constraint that applies to all subclasses: an extension is not allowed to contradict or relax requirements that would otherwise apply to the system and its constituent devices.

➜ **2.7-A** Extensions shall not break conformance

Extensions ***SHALL*** not contradict or relax requirements of these Guidelines.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

# 2.8 Innovation Class Submissions

This section contains requirements for innovation class submissions. An innovation class submission is a voting system that includes one or more distinct innovative devices. The submitter must follow the same procedures that any submitter of a voting system must follow except that the submitter must also request and justify that a new device class be created in the VVSG for each distinct innovative device in the submission. For each new device class requested, the submitter must show where in the device class structure the new class is to be created. In listing the specific requirements of the new class, the submitter is expected to follow all rules of class hierarchy and requirement inheritance from Section 2.6.

→ **2.8-A** Innovative device class submission

For each distinct innovative device class submission included In the voting system, the implementation statement for the voting system ***SHALL*** identify:

1. New device classes to be created and where they fit into the device class hierarchy;
2. Suggested requirements and test methods for new classes;
3. Justifications for items 1 and 2.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **2.8-B** Identification of applicable requirements

For each distinct innovative device class submission included in the voting system, the implementation statement for the voting system ***SHALL*** identify all requirements that apply to the new class.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Identification of applicable requirements may occur through inheritance from superclasses or it may occur through reuse of requirements from other, similar classes.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **2.8-C** Identification of innovativeness

Each distinct innovative class submission ***SHALL*** include documentation that provides an explanation as to why the voting system and its accompanying devices are innovative and how they differ from voting technology that implement other voting device classes in the VVSG.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The submission in effect requests the creation of a new device class for each distinct innovative device included in the voting system. This requirement is for the purpose of evaluating whether the creation of a new class is justified. To satisfy this requirement, the submitter may provide an overview of the device describing its functionality, boundaries, and interactions with other devices.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

# Chapter 3: Usability, Accessibility, and Privacy Requirements

***VERSION DATE: 2007-May-15***

## 3.1 Overview

[[Convention for embedded comments: they are enclosed in double brackets. These remarks and questions are directed to the TGDC and its HFP subcommittee. Comments that involve substantive issues (rather than mere re-wording) are marked as “Major”]]

[[Throughout, the marker “XREF” is used to indicate a reference to another part of the VVSG – these need to be resolved, but only after all the requirements have “settled down”.]]

The importance of usability and accessibility in the design of voting systems has become increasingly apparent. It is not sufficient that the internal operation of these systems be correct; in addition, voters and election officials must be able to use them effectively and efficiently.

There are some properties of voting systems that make good design especially difficult:

- The voting task itself can be fairly complex; the voter may have to navigate an electronic ballot, choose multiple candidates in a single contest, understand the effect of party-line voting, or decide on ballot questions written in legal language.
- Voting is performed infrequently (compared with tasks such as using an ATM), so there is relatively limited opportunity for voters and poll workers to gain familiarity with the process.
- Changes in the election process, including new voting equipment, may require voters and poll workers to use new and unfamiliar procedures.
- The set of "users" for voting equipment is exceptionally diverse. The voting public encompasses a broad range of factors, including physical and cognitive abilities, language skills, and technology experience.

### 3.1.1 Purpose

The challenge, then, is to provide a voting system that voters can use comfortably, efficiently, and with justified confidence that they have cast their votes correctly.

The requirements within this section are intended to serve that goal. Three broad principles motivate this section:

1. All eligible voters are to have access to the voting process without discrimination. The voting process must be accessible to individuals with disabilities. The voting process includes access to the polling place, instructions on how to vote, initiating the voting session, making ballot selections, review of the ballot, final submission of the ballot, and getting help when needed.
2. Each cast ballot must accurately capture the selections made by the voter. The ballot must be presented to the voter in a manner that is clear and usable. Voters should encounter no difficulty or confusion regarding the process for recording their selections.
3. The voting process must preserve the secrecy of the ballot. The voting process should preclude anyone else from determining the content of a voter's ballot, without the voter's cooperation. If such a determination is made against the wishes of the voter, then his or her privacy has been violated.

Note that these principles refer to the entire voting *process*. The VVSG applies only to voting systems; other aspects of the process (such as administrative rules and procedures) are outside the scope of the VVSG, but are nonetheless crucial for the full achievement of the principles.

Also, please see section XREF/Intro which describes the relationship between HAVA and the VVSG.

### 3.1.2 Special Terminology

Several uncommon terms are used in this section. For the convenience of the reader, they are defined below. Many other technical terms frequently used throughout the VVSG are defined in the Glossary. Note in particular the distinctions among these terms: voting process, voting system, voting device, voting session, and voting station.

- **Accessible Voting Station (Acc-VS)** - the voting station specially equipped for individuals with disabilities referred to in HAVA 301 (a)(3)(B).
- **Audio-Tactile Interface (ATI)** - a voter interface designed not to require visual reading of a ballot. Audio is used to convey information to the voter and sensitive tactile controls allow the voter to convey information to the voting system.
- **Common Industry Format (CIF)** - the format to be used for usability test reporting, described in ISO/IEC 25062:2006 "Common Industry Format (CIF) for Usability Test Reports". [[There are plans for a more specific version of the CIF targeted towards voting. If this comes about, it will be referred to here. Not available for July version.]]
- **Voter-Editable Ballot Device (VEBD)** - voting systems such as DREs and EBMs that present voters with an editable ballot (as opposed to manually-marked paper ballots), allowing them easily to

change their choices prior to final casting of the ballot. "VEBD-V" denotes the visual interface of such systems and "VEBD-A" denotes the audio interface.

- **Voting Performance Protocol (VPP)** - a carefully defined method for measuring how well subjects perform various voting tasks within a controlled experiment.

### 3.1.3 Interaction of Usability and Accessibility Requirements

All the requirements in Section 3 have the purpose of improving the quality of interaction between voters and voting systems. Please note how sub-sections 3.2 and 3.3 XREF work together:

-- The requirements for general usability in subsection 3.2 XREF apply to all voting systems, *including the Acc-VS.* Requirements for any alternative languages required by state or federal law are included under this heading.

-- The requirements of subsection 3.3 XREF to assist voters with physical, sensory, or cognitive disabilities apply to the *accessible voting station* (Acc-VS) required by HAVA Section 301 (a)(3)(B). The features of the Acc-VS may also assist those not usually described as having a disability, e.g., voters with poor eyesight or limited dexterity.

## 3.2 General Usability Requirements

The voting system should support a process that provides a high level of usability for all voters. The goal is for voters to be able to negotiate the process effectively, efficiently, and comfortably.

Many of the mandatory voting system standards in HAVA Section 301 relate to the interaction between the voter and the voting system:

---

a. Requirements.--Each voting system used in an election for federal office shall meet the following requirements:

1. In general.--

A. Except as provided in subparagraph (B), the voting system (including any lever voting system, optical scanning voting system, or direct recording electronic system) shall--

i. Permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted;

ii. Provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is

cast and counted (including the opportunity to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error); and

iii. If the voter selects votes for more than one candidate for a single office -

I. Notify the voter that the voter has selected more than one candidate for a single office on the ballot;

II. Notify the voter before the ballot is cast and counted of the effect of casting multiple votes for the office; and

III. Provide the voter with the opportunity to correct the ballot before the ballot is cast and counted.

B. A state or jurisdiction that uses a paper ballot voting system, a punch card voting system, or a central count voting system (including mail-in absentee ballots and mail-in ballots), may meet the requirements of subparagraph (A)(iii) by -

i. Establishing a voter education program specific to that voting system that notifies each voter of the effect of casting multiple votes for an office; and

ii. Providing the voter with instructions on how to correct the ballot before it is cast and counted (including instructions on how to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error).

C. The voting system shall ensure that any notification required under this paragraph preserves the privacy of the voter and the confidentiality of the ballot.

---

The requirements of section 3.2 XREF are intended to support these basic usability standards of HAVA.

## 3.2.1 Performance Requirements

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. In the context of voting, the primary user is the voter (although the equipment is used by poll workers as well), the product is the voting system, and the task is the correct recording of the voter's ballot selections. Additional requirements for task performance are independence and privacy: the voter should normally be able to complete the voting task without assistance from others, and the voter selections should be private. Lack of independence or privacy may adversely affect effectiveness (e.g., by possibly inhibiting the voter's free choice) and efficiency (e.g., by slowing down the process). Among the basic metrics for voting usability are:

- low error rate for marking the ballot (the voter selection is correctly conveyed to and represented within the voting system)
- efficient operation (time required to vote is not excessive)
- satisfaction (voter experience is safe, comfortable, free of stress, and instills confidence)

General usability is covered by both high-level performance-based requirements (in this subsection) and design requirements (in following subsections). Whereas the latter require the presence of specific features generally thought to promote usability, the former *directly* address metrics for effectiveness (e.g., correct capture of voter selections), efficiency (e.g., time taken to vote), and satisfaction. The voting system is tested by having groups of people (representing voters) attempt to perform various typical voting tasks. The requirement is met only if those tasks are accomplished with a specified degree of success.

### 3.2.1.1 Overall Performance Metrics

The requirements of this section set benchmarks for the usability of the voting session as a whole.

→ **3.2.1.1-A** Overall Effectiveness

The system ***SHALL*** achieve an overall accuracy rating of at least XXX, [[Actual benchmarks to be filled in later.]] as measured by the NIST Voting Performance Protocol (NIST VPP).

*Applies to:* *Voting System*

*Test Reference:* *Performance*

DISCUSSION

This requirement ensures that the system enables voters to accurately cast votes for the candidates and referendum positions as intended.

→ **3.2.1.1-B** Overall Efficiency

When the conventional visual/tactile interface is used, the system ***SHALL*** achieve an overall mean voting session time of at most XXX minutes as measured by the NIST VPP.

*Applies to:* *Voting System*

*Test Reference:* *Performance*

DISCUSSION

This requirement ensures that the system enables voters to vote with reasonable speed. Note that this requirement does not apply to the audio interface of a system, nor to the use of special input devices for voters with dexterity disabilities.

→ **3.2.1.1-C** Overall Satisfaction

The system ***SHALL*** achieve an overall satisfaction rating of at least XXX, as measured by the NIST VPP.

*Applies to:* *Voting System*

*Test Reference:* *Performance*

DISCUSSION

This requirement ensures that the system is reasonably comfortable and pleasant to use.

### 3.2.1.2 Vendor Testing

[[Major – note new wording for usability testing by vendor – HFP section requires what testing is to be done. Vol IV contains blanket reporting requirement - suggested wording: "The vendor shall document all the usability testing performed as required in section 3 (? XREF) and report the test results using the Common Industry Format."]]

→ **3.2.1.2-A** Usability Testing by Vendor for General Population

The vendor ***SHALL*** conduct summative usability tests on the voting system using individuals who are representative of the general population. See requirement IV.2.6.2-A XREF for associated reporting requirement.

*Applies to:* *Voting System*

*Test Reference:* *Inspection*

DISCUSSION

Voting system developers are required to conduct realistic usability tests on the final product before submitting the system to conformance testing. This is to encourage early detection and resolution of usability problems.

## 3.2.2 Functional Capabilities

The usability of the voting process is enhanced by the presence of certain functional capabilities. These capabilities differ somewhat depending on whether or not the system presents an editable interface within which voters can easily change their selections (typically an electronic screen) or an interface in which voters must obtain a new ballot to make changes (typically a manually marked paper ballot).

→ **3.2.2-A** Notification of Effect of Overvoting

If the voter makes more than the allowable number of selections for a contest, the voting system ***SHALL*** notify the voter of the effect of this action before the ballot is cast and counted.

*Applies to:* *Voting system*

*Test Reference:* *Functional*

D I S C U S S I O N

In the case of manual systems, this may be achieved through appropriately placed instructions. This requirement has no force for VEBD systems, since they prevent overvoting in the first place.

→ **3.2.2-B** Undervoting to be Permitted

The voting system ***SHALL*** allow the voter, at his or her choice, to submit an undervoted ballot without correction.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

→ **3.2.2-C** Correction of Ballot

The voting system ***SHALL*** provide the voter the opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

In the case of manual systems, this may be achieved through appropriately placed written instructions. Some corrections may require the voter to obtain a new paper ballot from a poll worker. Also, note the requirements on precinct-count optical scanners in section 3.2.2.2 XREF below.

→ **3.2.2-D** Notification of Successful Ballot Casting

If (and only if) the ballot is cast successfully, the system ***SHALL*** so notify the voter.

*Applies to:* *DRE, PCOS*

*Test Reference:* *Functional*

D I S C U S S I O N

The purpose of this requirement is to provide feedback to the voter to assure him or her that the voting session has been completed. A precipitous confirmation of successful casting that is contradicted by an error that occurs around the same time would be misleading and non-compliant behavior.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **3.2.2-E** Notification of Ballot Casting Failure (DRE)

If the ballot is not cast successfully, including storage of the ballot image, a DRE ***SHALL*** so notify the voter and provide clear instruction as to the steps the voter should take to cast his or her ballot.

*Applies to:* *DRE*

*Test Reference:* *Functional*

D I S C U S S I O N

If a DRE fails at the point of casting a ballot, it must clearly indicate to the voter and to election officials responding to the failure whether or not the ballot was cast. Otherwise, election officials may be unable to provide substantial confirmation that the vote was or was not counted, possibly resulting in disenfranchisement or the casting of two ballots by a single voter.

A device that is observed to "freeze" when the voter attempts to cast the ballot, providing no evidence one way or the other whether the ballot was cast, is assessed a disenfranchisement failure (see Xref: Manageable failures per election), the most serious type of failure.

*Source:* *2002 VSS I.2.4.3.3.k / VVSG'05 I.2.3.3.3.m*

*Impact:* *Click here to add the Impact*

→ **3.2.2-F** Notification of Ballot Casting Failure (PCOS)

If the ballot is not cast successfully, including reading of the ballot and transport of the ballot into the ballot box, a PCOS ***SHALL*** so notify the voter.

*Applies to:* *PCOS*

*Test Reference:* *Functional*

D I S C U S S I O N

See also Xref: Paper-based tabulator, indicate status of misfed ballot.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

### 3.2.2.1 Editable Interfaces

Voting systems such as DREs and EBMs present voters with an editable interface, allowing them easily to change their choices prior to final casting of the ballot.

→ **3.2.2.1-A** Prevention of Overvotes

The voting system ***SHALL*** prevent voters from making more than the allowable number of choices for each contest.

*Applies to:* *VEBD*

*Test Reference:* *Functional*

D I S C U S S I O N

This requirement does not specify exactly how the system must respond when a voter attempts to select an "extra" candidate. For instance, the system may prevent the selection and issue a warning, or, in the case of a single-choice contest, simply change the selection.

→ **3.2.2.1-B** Warning of Undervotes

The voting system ***SHALL*** provide feedback to the voter, before final casting of the ballot, that identifies specific contests or ballot issues for which he or she has made fewer than the allowable number of selections (i.e., undervotes).

*Applies to:* *VEBD*

*Test Reference:* *Functional*

DISCUSSION

For VEBD systems, no allowance is made for disabling this feature. Also, see requirement below on "Clarity of Warnings".

→ **3.2.2.1-C** Independent Correction of Ballot

The voting system ***SHALL*** provide the voter the opportunity to correct the ballot before it is cast and counted. This correction process ***SHALL*** not require external assistance. The corrections to be supported include modifying an undervote or overvote, and changing a vote from one candidate to another.

*Applies to:* *VEBD*

*Test Reference:* *Functional*

DISCUSSION

Click here and type the discussion about this requirement

→ **3.2.2.1-D** Ballot Editing per Contest

The voting system ***SHALL*** allow the voter to change a vote within a contest before advancing to the next contest.

*Applies to:* *VEBD*

*Test Reference:* *Functional*

DISCUSSION

The point here is that voters using an editable interface should not have to wait for a final ballot review screen in order to change a vote.

→ **3.2.2.1-E** Contest Navigation

The voting system ***SHALL*** provide navigation controls that allow the voter to advance to the next contest or go back to the previous contest before completing a vote on the contest(s) currently being presented (whether visually or aurally).

*Applies to:* *VEBD*

*Test Reference:* *Functional*

DISCUSSION

For example, voters should not be forced to proceed sequentially through all the contests before going back to check their selections for a previous contest.

### 3.2.2.2 Non-Editable Interfaces

Non-Editable interfaces, such as manually marked paper ballots (MMPB) do not have the same flexibility as do editable interfaces. Nonetheless, certain features are required, especially in the case of precinct-based optical scanners. Note that the technical definition of "marginal mark" may be found in the glossary. Basically, a marginal mark is one that, according the vendor specifications, is neither clearly countable as a vote nor clearly countable as a non-vote.

➞ **3.2.2.2-A** Notification of Overvoting

The voting system ***SHALL*** be capable of providing feedback to the voter that identifies specific contests or ballot issues for which he or she has made more than the allowable number of selections (i.e. overvotes).

*Applies to:* *PCOS*

*Test Reference:* *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

➞ **3.2.2.2-B** Notification of Undervoting

The voting system ***SHALL*** be capable of providing feedback to the voter that identifies specific contests or ballot issues for which he or she has made fewer than the allowable number of selections (i.e. undervotes). The system ***SHALL*** provide a means for an authorized election official to deactivate this capability entirely and by contest.

*Applies to:* *PCOS*

*Test Reference:* *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

➞ **3.2.2.2-C** Notification of Blank Ballots

The voting system ***SHALL*** be capable of notifying the voter that he or she has submitted a paper ballot that is blank on one or both sides. The system ***SHALL*** provide a means for an authorized election official to deactivate this capability.

*Applies to:* *PCOS*

*Test Reference:* *Functional*

DISCUSSION

One purpose of this feature is to detect situations in which the voter might be unaware that the ballot is two-sided. This feature is distinct from the ability to detect and warn about undervoting.

→ **3.2.2.2-D** Ballot Correction or Submission Following Notification

After the voting system has notified the voter that a potential error condition (such as an overvote, undervote, or blank ballot) exists, the system ***SHALL*** allow the voter to correct the ballot or to submit it as is.

*Applies to:* *PCOS*

*Test Reference:* *Functional*

DISCUSSION

This requirement mandates that the equipment be capable of allowing either correction or immediate submission. For instance, a questionable paper ballot might be physically ejected for possible correction. This requirement does not constrain the *procedures* that jurisdictions might adopt for handling such situations (e.g. whether poll worker intervention is required).

→ **3.2.2.2-E** Handling of Marginal Marks

Paper-based precinct tabulators should be able to identify a ballot containing marginal marks. When such a ballot is detected, the tabulator ***SHALL***:

- Return the ballot to the voter;
- Provide feedback to the voter that identifies the specific contests or ballot issues for which a marginal mark was detected;
- Allow the voter either to correct the ballot or to submit the ballot "as is" without correction.

*Applies to:* *Precinct tabulator*

*Test Reference:* *Functional*

DISCUSSION

The purpose of this requirement is to provide more certainty about the handling of poorly-marked ballots. If a given candidate or option is clearly marked as chosen, or left completely unmarked, then there is no ambiguity to resolve. But each vendor should define a "gray zone" (with respect to location, darkness, etc.) in which marks will be actively flagged as ambiguous.

## 3.2.3 Privacy

[[Major - Privacy section moved up.]] The voting process must preclude anyone else from determining the content of a voter's ballot without the voter's cooperation.

Privacy ensures that the voter can make selections based solely on his or her own preferences without intimidation or inhibition.

### 3.2.3.1 Privacy at the Polls

➞ **3.2.3.1-A** System Support of Privacy

When deployed according to the installation instructions provided by the vendor, the voting system ***SHALL*** prevent others from determining the contents of a voter's ballot.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

↳ **3.2.3.1-A.1** Visual Privacy

The ballot, [[added:]] any other visible record containing ballot information, and any input controls ***SHALL*** be visible only to the voter during the voting session and ballot submission.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

[[Added discussion as per WQ suggestions.]] This requirement may involve different approaches for electronic and paper interfaces. In both cases, appropriate shielding of the voting station is important. When a paper record with ballot information needs to be transported by the voter, devices such as privacy sleeves may be necessary. This requirement applies to all records with information on ballot choices (such as a vote verification record) even if that record is not itself a ballot.

↳ **3.2.3.1-A.2** Auditory Privacy

The audio interface of the voting system ***SHALL*** be audible only to the voter.

*Applies to:* *VEBD-A*

*Test Reference:* *Functional*

D I S C U S S I O N

Voters who are hard of hearing but need to use an audio interface may also need to increase the volume of the audio. Such situations require headphones with low sound leakage.

↳ **3.2.3.1-A.3** Privacy of Warnings

The voting system ***SHALL*** issue all warnings in a way that preserves the privacy of the voter and the confidentiality of the ballot.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

HAVA 301 (a)(1)(C) mandates that the voting system shall notify the voter of an attempted overvote in a way that preserves the privacy of the voter and the confidentiality of the ballot. This requirement generalizes that mandate.

↳ **3.2.3.1-A.4** No Receipts

The voting system ***SHALL*** not issue a receipt to the voter that would provide proof to another of how he or she voted.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

### 3.2.3.2 No Recording of Alternative Format Usage

When voters use non-typical ballot interfaces, such as large print or alternative languages, their anonymity may be vulnerable. To the extent possible, only the logical contents of their ballots should be recorded, not the special formats in which they were rendered. In the case of paper ballots, where the interface *is* the record, some format information is unavoidably preserved.

→ **3.2.3.2-A** No Recording of Alternate Languages

No information ***SHALL*** be kept within an electronic cast vote record that identifies any alternative language feature(s) used by a voter.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

DISCUSSION

Click here and type the discussion about this requirement

→ **3.2.3.2-B** No Recording of Accessibility Features

No information ***SHALL*** be kept within an electronic cast vote record that identifies any accessibility feature(s) used by a voter.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

DISCUSSION

Click here and type the discussion about this requirement

## 3.2.4 Cognitive Issues

The features specified in this section are intended to minimize cognitive difficulties for voters. They should always be able to operate the voting system and understand the effect of their actions.

→ **3.2.4-A** Completeness of Instructions

The voting station ***SHALL*** provide instructions for all its valid operations.

*Applies to:* *Voting System*

*Test Reference:* *Inspection*

DISCUSSION

If an operation is available to the voter, it must be documented. Examples include how to change a vote, how to navigate among contests, how to cast a straight party vote, how to cast a write-in vote, and how to adjust display and audio characteristics.

→ **3.2.4-B** Availability of Assistance from the System

The voting system ***SHALL*** provide a means for the voter to get help directly from the system at any time during the voting session.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

DISCUSSION

The voter should always be able to get help from the system if needed. The purpose is to minimize the need for poll worker assistance. VEBD voting systems may provide this with a distinctive "help" button. Any type of voting system may provide written instructions that are separate from the ballot.

### → **3.2.4-C** Plain Language

All instructional material for the voter ***SHALL*** conform to norms and best practices for plain language.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

DISCUSSION

Although part of general usability, the use of plain language is also expected to assist voters with cognitive disabilities. The plain language requirements apply to instructions that are inherent to the voting system or that get generated by default. To the extent that instructions are determined by election officials designing the ballot, they are beyond of the scope of this requirement.

### ↳ **3.2.4-C.1** Clarity of Warnings

Warnings and alerts issued by the voting system should clearly state:

- the nature of the problem
- whether the voter has performed or attempted an invalid operation or whether the voting equipment itself has malfunctioned in some way
- the set of responses available to the voter

*Applies to:* *Voting System*

*Test Reference:* *Functional*

DISCUSSION

For instance, “You have not interacted with the system for the past three minutes. Please press the ‘Need more time’ button right away to tell the system that you’re still here – Thank you.” rather than “System detects imminent timeout condition”. In case of an equipment failure, the only action available to the voter might be to get assistance from a poll worker.

### ↳ **3.2.4-C.2** Context before Action

When an instruction is based on a condition, the condition should be stated first, and then the action to be performed.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

For instance, use "In order to change your vote, do X", rather than "Do X, in order to change your vote".

↳ **3.2.4-C.3** Simple Vocabulary

The system should use familiar, common words and avoid technical or specialized words that voters are not likely to understand.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

For instance, "... there are more contests on the other side ..." rather than "...additional contests are presented on the reverse ..."

↳ **3.2.4-C.4** Start Each Instruction on a New Line

The system should start the visual presentation of each new instruction on a new line.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

This implies not "burying" several unrelated instructions in a single long paragraph.

↳ **3.2.4-C.5** Use of Positive

The system should issue instructions on the correct way to perform actions, rather than telling voters what not to do.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

For example, “Fill in the oval for your write-in vote to count” rather than “If the oval is not marked, your write-in vote cannot be counted”.

↳ **3.2.4-C.6** Use of Imperative Voice

The system's instructions should address the voter directly rather than use passive voice constructions.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

DISCUSSION

For example, "remove and retain this ballot stub" rather than "this ballot stub must be removed and retained by the voter."

↳ **3.2.4-C.7** Gender-based Pronouns

The system should avoid the use of gender-based pronouns.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

DISCUSSION

For example, "...write in your choice directly on the ballot..." rather than "... write in his name directly on the ballot..."

→ **3.2.4-D** No Bias among Choices

Consistent with election law, the voting system should support a process that does not introduce any bias for or against any of the selections to be made by the voter. In both visual and aural formats, contest choices ***SHALL*** be presented in an equivalent manner.

*Applies to:* *Voting System*

*Test Reference:* *Inspection*

DISCUSSION

Certain differences in presentation are mandated by state law, such as the order in which candidates are listed and provisions for voting for write-in candidates. But comparable characteristics such as font size or voice volume and speed must be the same for all choices.

→ **3.2.4-E** Ballot Design

The voting system ***SHALL*** provide the capability to design a ballot with a high level of clarity and comprehensibility.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

DISCUSSION

Click here and type the discussion about this requirement

↳ **3.2.4-E.1** Contests Split among Pages or Columns

The voting system should not visually present a single contest spread over two pages or two columns.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

DISCUSSION

Such a visual separation poses the risk that the voter may perceive one contest as two, or fail to see additional choices. If a contest has a large number of candidates, it may be infeasible to observe this guideline.

↳ **3.2.4-E.2** Indicate Maximum Number of Candidates

The ballot ***SHALL*** clearly indicate the maximum number of candidates for which one can vote within a single contest.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

DISCUSSION

Click here and type the discussion about this requirement

↳ **3.2.4-E.3** Consistent Representation of Candidate Selection

The relationship between the name of a candidate and the mechanism used to vote for that candidate ***SHALL*** be consistent throughout the ballot.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

DISCUSSION

For example, the response field where voters indicate their selections must not be located to the left of some candidates' names, and to the right of others'.

↳ **3.2.4-E.4** Placement of Instructions

The system should display instructions near to where they are needed.

*Applies to:* *Voting system*

*Test Reference:* *Functional*

D I S C U S S I O N

For instance, only general instructions should be grouped at the beginning of the ballot; those pertaining to specific situations should be presented where and when needed.

➞ **3.2.4-F** Conventional Use of Color

The use of color by the voting system should agree with common conventions: (a) green, blue or white is used for general information or as a normal status indicator; (b) amber or yellow is used to indicate warnings or a marginal status; (c) red is used to indicate error conditions or a problem requiring immediate attention.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

➞ **3.2.4-G** Icons and Language

When an icon is used to convey information, indicate an action, or prompt a response, it ***SHALL*** be accompanied by a corresponding linguistic label.

*Applies to:* *Voting device*

*Test Reference:* *Functional*

D I S C U S S I O N

While icons can be used for emphasis when communicating with the voter, they must not be the sole means by which information is conveyed, since there is no widely accepted "iconic" language and therefore not all voters may understand a given icon.

## 3.2.5 Perceptual Issues

The requirements of this section are designed to minimize perceptual difficulties for the voter.

→ **3.2.5-A** Screen Flicker

No voting system display screen ***SHALL*** flicker with a frequency between 2 Hz and 55 Hz.

*Applies to:* *VEBD-V*

*Test Reference:* *Inspection*

D I S C U S S I O N

Aside from usability concerns, this requirement protects voters with epilepsy.

→ **3.2.5-B** Resetting of Adjustable Aspects at End of Session

Any aspect of the voting station that is adjustable by the voter or poll worker, including font size, color, contrast, audio volume, or rate of speech, ***SHALL*** automatically reset to a standard default value upon completion of that voter's session. For the Acc-VS, the aspects include synchronized audio/video mode and non-manual input mode.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

This ensures that the voting station presents the same initial appearance to every voter.

→ **3.2.5-C** Ability to Reset to Default Values

If any aspect of a voting system is adjustable by the voter or poll worker, there ***SHALL*** be a mechanism to reset all such aspects to their default values.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

The purpose is to allow a voter or poll worker who has adjusted the system into an undesirable state to reset all the aspects and begin again.

→ **3.2.5-D** Minimum Font Size

All voting systems ***SHALL*** provide a minimum font size of 3.0mm (measured as the height of a capital letter) for all text intended for voters [[added poll workers to scope]] or poll workers.

*Applies to:* *Voting device*

*Test Reference:* *Functional*

D I S C U S S I O N

All millimeters will be calculated using Hard Metric Conversion. (See Glossary for definition.)

→ **3.2.5-E** Available Font Sizes

A voting station that uses an electronic image display ***SHALL*** be capable of showing all information in at least two font sizes, (a) 3.0-4.0 mm and (b) 6.3-9.0 mm, under control of the voter. The system ***SHALL*** allow the voter to adjust font size throughout the voting session while preserving the current ballot choices.

*Applies to:* *VEBD-V*

*Test Reference:* *Functional*

D I S C U S S I O N

All millimeters will be calculated using Hard Metric Conversion. (See Glossary for definition.) While larger font sizes may assist most voters with poor vision, certain disabilities such as tunnel vision are best addressed by smaller font sizes. Larger font sizes may also assist voters with cognitive disabilities. This requirement mandates the availability of at least two font sizes, but additional choices (including continuous variability) are allowed.

→ **3.2.5-F** Use of Sans Serif Font

All text intended for the voter should be presented in a sans serif font.

*Applies to:* *Voting device*

*Test Reference:* *Functional*

D I S C U S S I O N

Research has shown that users prefer such fonts.

→ **3.2.5-G** Legibility of Paper Ballots and Verification Records

All voting systems using paper ballots [[added:]] or paper verification records should make provisions for voters with poor reading vision.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

Possible solutions include: (a) providing paper ballots in at least two font sizes, 3.0 - 4.0mm and 6.3 - 9.0mm and (b) providing [[added:]] electronic or optical devices for magnification.

→ **3.2.5-H** Contrast Ratio

The minimum figure-to-ground ambient contrast ratio for all text and informational graphics (including icons) intended for voters [[Added poll workers to scope.]] or poll workers ***SHALL*** be 3:1.

*Applies to:* *Voting device*

*Test Reference:* *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

→ **3.2.5-I** High Contrast for Electronic Displays

The voting station ***SHALL*** be capable of showing all information in high contrast either by default or under the control of the voter. The system ***SHALL*** allow the voter to adjust contrast throughout the voting session while preserving the current ballot choices. High contrast is a figure-to-ground ambient contrast ratio for text and informational graphics of at least 6:1.

*Applies to:* *VEBD-V*

*Test Reference:* *Inspection*

D I S C U S S I O N

→ **3.2.5-J** Accommodation for Color Blindness

The default color coding ***SHALL*** support correct perception by voters with color blindness.

*Applies to:* *Voting System*

*Test Reference:* *Inspection*

DISCUSSION

There are many types of color blindness and no color coding can, by itself, guarantee correct perception for everyone. However, designers should take into account such factors as: red-green color blindness is the most common form; high luminosity contrast will help colorblind voters to recognize visual features; and color-coded graphics can also use shape to improve the ability to distinguish certain features.

→ **3.2.5-K** No Reliance Solely on Color

Color coding ***SHALL*** not be used as the sole means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

DISCUSSION

While color can be used for emphasis, some other non-color mode must also be used to convey the information, such as a shape or text style. For example, red can be enclosed in an octagon shape.

## 3.2.6 Interaction Issues

The requirements of this section are designed to minimize interaction difficulties for the voter.

→ **3.2.6-A** No Page Scrolling

Voting systems ***SHALL*** not require page scrolling by the voter.

*Applies to:* *VEBD*

*Test Reference:* *Functional*

DISCUSSION

That is, the page of displayed information must fit completely within the physical screen presenting it. Scrolling is not an intuitive operation for those unfamiliar with the use of computers. Even those experienced with computers often do not notice a scroll bar and miss information at the bottom of the "page." Voting systems may require voters to move to the next or previous "page."

→ **3.2.6-B** Unambiguous Feedback for Voter's Selection

The voting system ***SHALL*** provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

→ **3.2.6-C** Accidental Activation

Input mechanisms ***SHALL*** be designed to minimize accidental activation.

*Applies to:* *Voting device*

*Test Reference:* *Functional*

D I S C U S S I O N

There are at least two kinds of accidental activation. One is when a control is activated as it is being "explored" by the voter because the control is overly sensitive to the touch. A second issue is the problem of having a control in a location where it can easily be activated unintentionally. An example would be a button in the very bottom left corner of the screen where a voter might hold the unit for support.

↳ **3.2.6-C.1** Size and Separation of Touch Areas

On touch screens, the sensitive touch areas ***SHALL*** have a minimum height of 0.5 inches and minimum width of 0.7 inches. The vertical distance between the centers of adjacent areas ***SHALL*** be at least 0.6 inches, and the horizontal distance at least 0.8 inches.

*Applies to:* *VEBD*

*Test Reference:* *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

↳ **3.2.6-C.2** No Repeating Keys

No key or control on a voting system ***SHALL*** have a repetitive effect as a result of being held in its active position.

*Applies to:* *Voting device*

*Test Reference:* *Functional*

D I S C U S S I O N

This is to preclude accidental activation. For instance, if a voter is typing in the name of a write-in candidate, depressing and holding the "e" key results in only a single "e" added to the name.

### 3.2.6.1 Timing Issues

These requirements address how long the system and voter wait for each other to interact. For the purposes of this section we define the following terms:

- **Initial system response time:** the time taken from when the voter performs some detectible action (such as pressing a button) to when the voting system *begins* responding in some obvious way (such as an audible response or any change on the screen)
- **Completed system response time:** the time taken from when the voter performs some detectible action to when the voting system completes its response and settles into a stable state (e.g. finishes "painting" the screen with a new page)
- **Voter inactivity time:** the amount of time the equipment will wait for detectible voter activity before issuing an alert to the voter
- **Alert time:** the amount of time the equipment will wait for detectible voter activity after issuing an alert and then going into an inactive state requiring poll worker intervention

→ **3.2.6.1-A** Maximum Initial System Response Time

The initial system response time of the voting system ***SHALL*** be no greater than 0.5 seconds.

*Applies to:* *VEBD*

*Test Reference:* *Functional*

D I S C U S S I O N

This is so the voter can very quickly perceive that his/her action has been detected and is being processed. The voter never gets the sense of dealing with an unresponsive or "dead" system. Note that this requirement applies to VEBD-A (audio) as well as to VEBD-V (visual) systems.

→ **3.2.6.1-B** Maximum Completed System Response Time for Vote Confirmation

When the voter performs an action to record a single vote, the completed system response time of the voting system ***SHALL*** be no greater than one second in the case of a visual response, and no greater than five seconds in the case of an audio response.

*Applies to:* *VEBD*

*Test Reference:* *Functional*

D I S C U S S I O N

For example, if the voter touches a button to indicate a vote for a candidate, a visual system might display an "X" next to the candidate's name, and an audio system might announce "You have voted for Smith for Governor".

→ **3.2.6.1-C** Maximum Completed System Response Time for All Operations

The completed system response time of the voting system for visual operations ***SHALL*** be no greater than 10 seconds.

*Applies to:* *VEBD-V*

*Test Reference:* *Functional*

D I S C U S S I O N

Even for "large" operations such as initializing the ballot or painting a new screen, the system must never take more than 10 seconds. In the case of audio systems, no upper limit is specified, since certain operations may take longer, depending on the length of the text being read (e.g. reading out a long list of candidates running in a contest).

→ **3.2.6.1-D** System Response Indicator

If the system has not completed its visual response within one second, it ***SHALL*** present to the voter, within 0.5 seconds of the voter's action, some indication that it is preparing its response.

*Applies to:* *VEBD*

*Test Reference:* *Functional*

D I S C U S S I O N

For instance, the system might present an hourglass icon indicating that it is "busy" processing the voter's request. This requirement is intended to preclude the "frozen screen" effect, in which no detectible activity is taking place for several seconds.

There need not be a specific "activity" icon, as long as some visual change is apparent (such as progressively "painting" a new screen).

→ **3.2.6.1-E** Voter Inactivity Time

The voting system ***SHALL*** detect and warn about lengthy voter inactivity during a voting session. Each system ***SHALL*** have a defined and documented inactivity time, and that time ***SHALL*** be between two and five minutes.

*Applies to:* *VEBD*

*Test Reference:* *Functional*

DISCUSSION

Each type of system must have a given inactivity time that is consistent among and within all voting sessions. This ensures that all voters are treated equitably.

→ **3.2.6.1-F** Alert Time

Upon expiration of the voter inactivity time, the voting system ***SHALL*** issue an alert and provide a means by which the voter may receive additional time. The alert time ***SHALL*** be between 20 and 45 seconds.

*Applies to:* *VEBD*

*Test Reference:* *Functional*

DISCUSSION

Click here and type the discussion about this requirement

## 3.2.7 Alternative Languages

HAVA Section 301 (a)(4) states that the voting system shall provide alternative language accessibility pursuant to the requirements of section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a). Ideally every voter would be able to vote independently and privately, regardless of language. As a practical matter, alternative language access is mandated under the Voting Rights Act of 1975, subject to certain thresholds (e.g., if the language group exceeds 5% of the voting age population). Thus, election officials must ensure that the voting system they deploy is capable of handling the languages meeting the legal threshold within their districts.

While the following requirements support this process, it should be noted that they are requirements only for voting systems to be *certified*. It is anticipated that jurisdictions will apply additional requirements appropriate for their particular circumstances for procurement and deployment.

→ **3.2.7-A** General Support for Alternative Languages

The voting system ***SHALL*** be capable of presenting the ballot, ballot selections, review screens, [[added:]] vote verification records, and voting instructions in any language declared by the vendor to be supported by the system.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

For example, if the vendor claims that a given system is capable of supporting Spanish and Chinese, then it must do so.

↳ **3.2.7-A.1** Voter Control of Language

The system ***SHALL*** allow the voter to select among the available languages throughout the voting session while preserving the current ballot choices.

*Applies to:* *VEBD*

*Test Reference:* *Functional*

D I S C U S S I O N

For instance, a voter may initially choose an English version of the ballot, but then wish to switch to another language in order to read a referendum question.

↳ **3.2.7-A.2** Complete Information in Alternative Language

All the information presented to the voter in the typical case of English-literate voters (including instructions, warnings, messages, ballot choices, and vote verification information) ***SHALL*** also be presented when an alternative language is being used, whether the language is written or spoken.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

Therefore, it may not be sufficient simply to present the ballot *per se* in the alternative language, especially in the case of VEBD systems. All the supporting information must also be available in the alternative language.

↳ **3.2.7-A.3** Usability Testing by Vendor for Alternative Languages

The vendor ***SHALL*** conduct summative usability tests for each of the system's supported languages, using subjects who are fluent in those languages but not fluent in English. See requirement IV.2.6.2-A XREF for associated reporting requirement.

*Applies to:* *Voting System*

*Test Reference:* *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

## 3.2.8 Usability for Poll Workers

Voting systems are used not only by voters to record their choices, but also by poll workers who are responsible for set-up, operation while polls are open, light maintenance, and poll closing. Because of the wide variety of implementations, it is impossible to specify detailed design requirements for these functions. The requirements below describe general capabilities that all systems must support.

→ **3.2.8-A** Clarity of System Messages for Poll Workers

All messages generated by the system for poll workers in support of the operation, maintenance, or safety of the system ***SHALL*** adhere to the requirements for clarity in section 12.2.3 XREF.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

### 3.2.8.1 Operation

Poll workers are responsible for opening polls, keeping the polls open and running smoothly during voting hours, and closing the polls afterwards. Operations may be categorized in three phases:

**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
- 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.

→ **3.2.8.1-A** Ease of Normal Operation

The procedures for system setup, polling, and shutdown, [[clarified:]] as documented by the vendor, ***SHALL*** be reasonably easy for the typical poll worker to learn, understand, and perform.

*Applies to:* *Voting system*

*Test Reference:* *Functional*

D I S C U S S I O N

This requirement covers procedures and operations for those aspects of system operation normally performed by poll workers and other "non-expert" operators. It does not address inherently complex operations such as ballot definition or system repair. While a certain amount of complexity is unavoidable, these "normal" procedures should not require any special expertise. The procedures may require a reasonable amount of training. Also, see requirements for usability of system documentation in Volume IV, Chapter 3 XREF.

→ **3.2.8.1-B** Usability Testing by Vendor for Poll Workers

The vendor ***SHALL*** conduct summative usability tests on the voting system using individuals who are representative of the general population. The tasks to be covered in the test ***SHALL*** include setup, operation, and shutdown. See requirement IV.2.6.2-A XREF for associated reporting requirement.

*Applies to:* *Voting System*

*Test Reference:* *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

### 3.2.8.2 Maintenance

Maintainability represents the ease with which maintenance actions can be performed based on the design characteristics of equipment and software and on the processes that the vendor and election officials have in place for preventing failures and for reacting to failures. Maintainability includes the ability of equipment and software to self-diagnose problems and make non-technical election workers aware of a problem. Maintainability addresses all scheduled and unscheduled events, which are performed to:

- Determine the operational status of the system or a component
- Adjust, align, tune or service components
- Repair or replace a component having a specified operating life or replacement interval
- Repair or replace a component that exhibits an undesirable predetermined physical condition or performance degradation
- Repair or replace a component that has failed
- Verify the restoration of a component or the system to operational status

Maintainability will be determined based on the presence of specific physical attributes that aid system maintenance activities, and the ease with which system maintenance tasks can be performed by the test lab. Although a more quantitative basis for assessing maintainability, such as the Mean Time to Repair the system is desirable, the certification of a system is conducted before it is approved for sale and thus before a broader base of maintenance experience can be obtained.

→ **3.2.8.2-A** Physical Attributes for Maintenance

The following physical attributes ***SHALL*** be sufficiently available so as to support good maintainability:

- Presence of labels and the identification of test points
- Provision of built-in test and diagnostic circuitry or physical indicators of condition
- Presence of labels and alarms related to failures
- Presence of features that allow non-technicians to perform routine maintenance tasks (such as update of the system database)

*Applies to:* *Voting device*

*Test Reference:* *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

➞ **3.2.8.2-B** Additional Attributes for Maintenance

The following additional attributes ***SHALL*** be sufficiently available so as to support good maintainability:

- Ease of detection by a non-technician that equipment has failed
- Low false alarm rates (i.e. indications of problems that do not exist)
- Ease of access to components for replacement
- Ease with which adjustment and alignment can be performed
- Ease with which database updates can be performed by a non-technician
- Ease with which a poll worker can adjust, align, tune or service components

*Applies to:* *Voting System*

*Test Reference:* *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

## 3.2.8.3 Safety

All voting systems and their components must be designed so as to eliminate hazards to personnel or to the equipment itself. Hazards include, but are not limited to:

- fire hazards
- electrical hazards
- potential for equipment tip-over (stability)
- potential for cuts and scrapes (e.g. sharp edges)
- potential for pinching (e.g. tight, spring-loaded closures)
- potential for hair or clothing entanglement

➞ **3.2.8.3-A** Safety Certification

All equipment associated with the voting system ***SHALL*** be certified in accordance with the requirements of UL 60950, Safety of Information Technology Equipment by a certification organization accredited by the Department of Labor, Occupational Safety and Health Administration's Nationally Recognized Testing Laboratory program. The certification organization's scope of accreditation ***SHALL*** include UL 60950.

*Applies to:* *Voting System*

*Test Reference:* *Inspection*

D I S C U S S I O N

UL 60950 is a comprehensive standard for IT equipment and addresses all the hazards discussed above under Safety.

## 3.3 Accessibility Requirements

HAVA Section 301 (a) (3) reads, in part:

---

ACCESSIBILITY FOR INDIVIDUALS WITH DISABILITIES.--The voting system shall--

(A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters;

(B) satisfy the requirement of subparagraph (A) through the use of at least one direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place;

---

The voting process is to be accessible to voters with disabilities through the use of a specially equipped voting station. A machine so equipped is referred to herein as an accessible voting station (Acc-VS).

The requirements in this subsection are intended to address this HAVA mandate. Ideally, every voter would be able to vote independently and privately. As a practical matter, there may be some number of voters who, because of the nature of their disabilities, will need personal assistance with any system. Nonetheless, these requirements are meant to make the voting system independently accessible to as many voters as possible.

[[A re-write to explain the relation between sections 3.2 and 3.3]] This subsection 3.3 (XREF) - Accessibility Requirements covers *only those features that are unique to the Acc-VS.* For instance, an audio interface would be of interest mainly to those with vision or other reading disabilities, but not to those who can use a visual interface. The preceding subsection 3.2 (XREF) – General Usability Requirements covers the features that are applicable *both* to the general population and to voters with disabilities. Those requirements apply to all voting systems, including the Acc-VS. Therefore, to determine what features are required of the Acc-VS, one must examine both subsections 3.2 and 3.3 XREF.

This subsection is organized according to the type of disability being addressed. For each type, certain appropriate design features are specified. Note, however, that a feature intended primarily to address one kind of disability may very well assist voters with other kinds.

## 3.3.1 General

The requirements of this sub-section are relevant to a wide variety of disabilities.

[[Next two are new requirements to support end-to-end testing. Added "vendor's complete voting system" to clarify intent.]]

→ **3.3.1-A** Accessibility throughout the Voting Session

The Acc-VS ***SHALL*** be integrated into the vendor's complete voting system so as to support accessibility for disabled voters throughout the voting session.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

This requirement ensures accessibility to the voter throughout the entire session. Not only must individual system components (such as ballot markers, paper records, and optical scanners) be accessible, but they must work together to support this result.

↳ **3.3.1-A.1** Documentation of Accessibility Procedures

The vendor ***SHALL*** supply documentation describing 1) recommended procedures that fully implement accessibility for voters with disabilities and 2) how the Acc-VS supports those procedures.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection, Functional*

DISCUSSION

The purpose of this requirement is for the vendor not simply to deliver system components, but also to describe the accessibility scenarios they are intended to support.

→ **3.3.1-B** Complete Information in Alternative Formats

When the provision of accessibility involves an alternative format for ballot presentation, then all information presented to non-disabled voters, including instructions, warnings, error and other messages, and ballot choices, ***SHALL*** be presented in that alternative format.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

Click here and type the discussion about this requirement

→ **3.3.1-C** No Dependence on Personal Assistive Technology

The support provided to voters with disabilities ***SHALL*** be intrinsic to the accessible voting station. It ***SHALL*** not be necessary for the accessible voting station to be connected to any personal assistive device of the voter in order for the voter to operate it correctly.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

This requirement does not preclude the accessible voting station from providing interfaces to assistive technology. (See definition of "personal assistive devices" in the Glossary.) Its purpose is to assure that disabled voters are not required to bring special devices with them in order to vote successfully. The requirement does not assert that the accessible voting station will eliminate the need for a voter's ordinary non-interfacing devices, such as eyeglasses or canes.

→ **3.3.1-D** Secondary Means of Voter Identification

If a voting system provides for voter identification or authentication by using biometric measures that require a voter to possess particular biological characteristics, then the system ***SHALL*** provide a secondary means that does not depend on those characteristics.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

For example, if fingerprints are used for voter identification, another mechanism must be provided for voters without usable fingerprints.

[[Major – re-worded/generalized somewhat from earlier version.]]

→ **3.3.1-E** Accessibility of Paper-based Vote Verification

If the Acc-VS generates a paper record (or some other durable, human-readable record) for the purpose of allowing voters to verify their ballot

choices, then the system ***SHALL*** provide a means to ensure that the verification record is accessible to all voters with disabilities, as identified in section 3.3 XREF.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

D I S C U S S I O N

[[New:]] 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. The purpose of this requirement is to ensure that all voters have a similar opportunity for vote verification. Note that this requirement addresses the special difficulties that may arise with the use of paper. Verification is part of the voting process, and all the other general requirements apply to verification, in particular those dealing with dexterity (e.g. 3.3.4-C "Ballot Submission and Vote Verification"), blindness (e.g. 3.3.3-E "Ballot Submission and Vote Verification"), and partial vision issues (e.g. 3.2.4-G "Legibility of Paper Ballots and Verification Records").

↳ **3.3.1-E.1** Audio Readback for Paper-based Vote Verification.

If the Acc-VS generates a paper record (or some other durable, human-readable record) for the purpose of allowing voters to verify their ballot choices, then the system ***SHALL*** provide a mechanism that can read that record and generate an audio representation of its contents.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

D I S C U S S I O N

Sighted voters can directly verify the contents of a paper record. The purpose of this requirement is to allow voters with visual disabilities to verify, even if indirectly, the contents of the record. It is recognized that the verification depends on the integrity of the mechanism that reads the record to the voter. The audio must be generated via the paper record and therefore not depend on any electronic or other "internal" record of the ballot. Note that the paper record and its audio representation may be rendered in an alternative language.

## 3.3.2 Partial Vision

These requirements specify the features of the accessible voting station designed to assist voters with partial vision.

Partial (or low) vision includes dimness of vision, haziness, film over the eye, foggy vision, extreme near-sightedness or far-sightedness, distortion of vision, color

distortion or blindness, visual field defects, spots before the eyes, tunnel vision, lack of peripheral vision, abnormal sensitivity to light or glare and night blindness. For the purposes of this discussion low vision is defined as having a visual acuity worse than 20/70.

People with tunnel vision can see only a small part of the ballot at one time. For these users it is helpful to have letters at the lower end of the font size range in order to allow them to see more letters at the same time. Thus, there is a need to provide font sizes at both ends of the range.

People with low vision or color blindness benefit from high contrast and from a selection of color combinations appropriate for their needs. Between 7% and 10% of all men have color vision deficiencies. Certain color combinations in particular cause problems. Therefore, use of color combinations with good contrast is required. Note also the general requirement "Accommodation for Color Blindness" in section 3.2.4 XREF.

However, some users are very sensitive to very bright displays and cannot use them for long. An overly bright background causes a visual white-out which makes these users unable to distinguish individual letters. Thus, use of non-saturated color options is an advantage for some people.

→ **3.3.2-A** Usability Testing by Vendor for Partially Sighted Voters

The vendor ***SHALL*** conduct summative usability tests on the voting system using partially sighted individuals. See requirement IV.2.6.2-A XREF for associated reporting requirement.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

→ **3.3.2-B** Adjustable Saturation for Color Displays

An accessible voting station with a color electronic image display ***SHALL*** allow the voter to adjust the color saturation throughout the voting session while preserving the current ballot choices. At least two options ***SHALL*** be available: a high and a low saturation presentation.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

It is not required that the station offer a continuous range of color saturation. "High saturation" refers to bright, vibrant colors. "Low saturation" refers to muted (or grayish) colors.

→ **3.3.2-C** Distinctive Buttons and Controls

Buttons and controls on accessible voting stations ***SHALL*** be distinguishable by both shape and color. This applies to buttons and controls implemented either "on-screen" or in hardware. This requirement does not apply to sizeable groups of keys, such as a conventional 4x3 telephone keypad or a full alphabetic keyboard.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

DISCUSSION

The redundant cues assist those with low vision. They also help individuals who may have difficulty reading the text on the screen.

→ **3.3.2-D** Synchronized Audio and Video

The voting station ***SHALL*** provide synchronized audio output to convey the same information as that which is displayed on the screen. There ***SHALL*** be a means by which the voter can disable either the audio or video output, resulting in a video-only or audio-only presentation, respectively. The system ***SHALL*** allow the voter to switch among the three modes (synchronized audio/video, video-only, or audio-only) throughout the voting session while preserving the current ballot choices.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

This feature may also assist voters with cognitive disabilities.

## 3.3.3 Blindness

These requirements specify the features of the accessible voting station designed to assist voters who are blind.

**3.3.3-A** Usability Testing by Vendor for Blind Voters

The vendor ***SHALL*** conduct summative usability tests on the voting system using individuals who are blind. See requirement IV.2.6.2-A XREF for associated reporting requirement.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

DISCUSSION

Click here and type the discussion about this requirement

**3.3.3-B** Audio-Tactile Interface

The accessible voting station ***SHALL*** provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface, as specified in Subsection 6.6 XREF.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

Note the necessity of both audio output and tactilely discernible controls for voter input. Full functionality includes at least:

- Instructions and feedback on initial activation of the ballot (such as insertion of a smart card), if applicable
- Instructions and feedback to the voter on how to operate the accessible voting station, including settings and options (e.g., volume control, repetition)
- Instructions and feedback for navigation of the ballot
- Instructions and feedback for contest choices, including write-in candidates
- Instructions and feedback on confirming and changing selections
- Instructions and feedback on final submission of ballot

**3.3.3-B.1** Equivalent Functionality of ATI

The ATI of the accessible voting station ***SHALL*** provide the same capabilities to vote and cast a ballot as are provided by its visual interface.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

For example, if a visual ballot supports voting a straight party ticket and then changing the choice in a single contest, so must the ATI.

↳ **3.3.3-B.2** ATI Supports Repetition

The ATI ***SHALL*** allow the voter to have any information provided by the voting system repeated.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

This feature may also be useful to voters with cognitive disabilities.

↳ **3.3.3-B.3** ATI Supports Pause and Resume

The ATI ***SHALL*** allow the voter to pause and resume the audio presentation.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

This feature may also be useful to voters with cognitive disabilities.

↳ **3.3.3-B.4** ATI Supports Transition to Next or Previous Contest

The ATI ***SHALL*** allow the voter to skip to the next contest or return to previous contests.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

This is analogous to the ability of sighted voters to move on to the next contest once they have made a selection or to abstain from voting on a contest altogether.

↳ **3.3.3-B.5** ATI Can Skip Referendum Wording

The ATI ***SHALL*** allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

This is analogous to the ability of sighted voters to skip over the wording of a referendum on which they have already made a decision prior to the voting session (e.g., "Vote yes on proposition #123").

→ **3.3.3-C** Audio Features and Characteristics

All voting stations that provide audio presentation of the ballot ***SHALL*** do so in a usable way, as detailed in the following sub-requirements.

*Applies to:* *VEBD-A*

*Test Reference:* *Functional*

DISCUSSION

These requirements apply to all voting system audio output, not just to the ATI of an accessible voting station.

↳ **3.3.3-C.1** Standard Connector

The ATI ***SHALL*** provide its audio signal through an industry standard connector for private listening using a 3.5mm stereo headphone jack to allow voters to use their own audio assistive devices.

*Applies to:* *VEBD-A*

*Test Reference:* *Functional*

DISCUSSION

Click here and type the discussion about this requirement

↳ **3.3.3-C.2** T-Coil Coupling

When a voting system utilizes a telephone style handset or headphone to provide audio information, it ***SHALL*** provide a wireless T-Coil coupling for assistive hearing devices so as to provide access to that information for voters with partial hearing. That coupling ***SHALL*** achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.

*Applies to:* *VEBD-A*

*Test Reference:* *Functional*

DISCUSSION

Note that requirement XREF 1.3.6-C forbids EM interference with hearing devices.

↳ **3.3.3-C.3** Sanitized Headphone or Handset

A sanitized headphone or handset ***SHALL*** be made available to each voter.

*Applies to:* *VEBD-A*

*Test Reference:* *Inspection*

DISCUSSION

This requirement can be achieved in various ways, including the use of "throwaway" headphones, or of sanitary coverings.

↳ **3.3.3-C.4** Initial Volume

The voting system ***SHALL*** set the initial volume for each voting session between 40 and 50 dB SPL.

*Applies to:* *VEBD-A*

*Test Reference:* *Functional*

DISCUSSION

A voter does not "inherit" the volume as set by the previous user of the voting station. See 3.2.4-B XREF "Resetting of Adjustable Aspects at End of Session".

↳ **3.3.3-C.5** Range of Volume

The audio system ***SHALL*** allow the voter to control the volume throughout the voting session while preserving the current ballot choices. The volume ***SHALL*** be adjustable from a minimum of 20dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.

*Applies to:* *VEBD-A*

*Test Reference:* *Functional*

DISCUSSION

Click here and type the discussion about this requirement

↳ **3.3.3-C.6** Range of Frequency

The audio system ***SHALL*** be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.

*Applies to:* *VEBD-A*

*Test Reference:* *Functional*

D I S C U S S I O N

The required frequencies include the range of normal human speech. This allows the reproduced speech to sound natural.

↳ **3.3.3-C.7** Intelligible Audio

The audio presentation of verbal information should be readily comprehensible by voters who have normal hearing and are proficient in the language. This includes such characteristics as proper enunciation, normal intonation, appropriate rate of speech, and low background noise. Candidate names should be pronounced as the candidate intends.

*Applies to:* *VEBD-A*

*Test Reference:* *Functional*

D I S C U S S I O N

This requirement covers both recorded and synthetic speech. It applies to those aspects of the audio content that are inherent to the voting system or that get generated by default. To the extent that the audio presentation is determined by election officials designing the ballot, it is beyond of the scope of this requirement.

↳ **3.3.3-C.8** Control of Speed

The audio system ***SHALL*** allow the voter to control the rate of speech throughout the voting session while preserving the current ballot choices. The range of speeds supported ***SHALL*** include 75% to 200% of the nominal rate.

*Applies to:* *VEBD-A*

*Test Reference:* *Functional*

D I S C U S S I O N

Many blind voters are accustomed to interacting with accelerated speech. This feature may also be useful to voters with cognitive disabilities.

→ **3.3.3-D** Ballot Activation

If the voting station supports ballot activation for non-blind voters, then it ***SHALL*** also provide features that enable voters who are blind to perform this activation.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

D I S C U S S I O N

For example, smart cards might provide tactile cues so as to allow correct insertion.

→ **3.3.3-E** Ballot Submission and Vote Verification

If the voting station supports ballot submission [[added:]] or vote verification for non-blind voters, then it ***SHALL*** also provide features that enable voters who are blind to perform these actions.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

D I S C U S S I O N

For example, if voters using this station normally perform paper-based verification, or if they feed their own optical scan ballots into a reader, blind voters should also be able to do so.

→ **3.3.3-F** Tactile Discernability of Controls

All mechanically operated controls or keys on an accessible voting station ***SHALL*** be tactilely discernible without activating those controls or keys.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

D I S C U S S I O N

Note also the more general requirement (1.2.5-C XREF) against accidental activation of controls.

→ **3.3.3-G** Discernability of Key Status

The status of all locking or toggle controls or keys (such as the "shift" key) ***SHALL*** be visually discernible, and also discernible either through touch or sound.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

Click here and type the discussion about this requirement

## 3.3.4 Dexterity

These requirements specify the features of the accessible voting station designed to assist voters who lack fine motor control or use of their hands.

→ **3.3.4-A** Usability Testing by Vendor for Voters with Dexterity Disabilities

The vendor ***SHALL*** conduct summative usability tests on the voting system using individuals lacking fine motor control. See requirement IV.2.6.2-A XREF for associated reporting requirement.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

DISCUSSION

Click here and type the discussion about this requirement

→ **3.3.4-B** Support for Non-Manual Input

The accessible voting station ***SHALL*** provide a mechanism to enable non-manual input that is functionally equivalent to tactile input. All the functionality of the accessible voting station (e.g., straight party voting, write-in candidates) that is available through the conventional forms of input, such as tactile, ***SHALL*** also be available through the non-manual input mechanism.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

This requirement ensures that the accessible voting station is operable by individuals who do not have the use of their hands. Examples of non-manual controls include mouth sticks and "sip and puff" switches. While it is desirable that the voter be able to independently initiate use of the non-manual input mechanism, this requirement guarantees only that the voter can vote independently once the mechanism is enabled.

→ **3.3.4-C** Ballot Submission and Vote Verification

If the voting station supports ballot submission [[added:]] or vote verification for non-disabled voters, then it ***SHALL*** also provide features that enable voters who lack fine motor control or the use of their hands to perform these actions.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

For example, if voters using this station normally perform paper-based verification, or if they feed their own optical scan ballots into a reader, voters with dexterity disabilities should also be able to do so. Note that the general requirement for privacy when voting (3.2.7.1-A XREF) still applies

**3.3.4-D** Manipulability of Controls

All keys and controls on the accessible voting station ***SHALL*** be operable with one hand and ***SHALL*** not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys ***SHALL*** be no greater 5 lbs. (22.2 N).

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

Controls are to be operable without excessive force.

→ **3.3.4-E** No Dependence on Direct Bodily Contact

The accessible voting station controls ***SHALL*** not require direct bodily contact or for the body to be part of any electrical circuit.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

This requirement ensures that controls are operable by individuals using prosthetic devices.

## 3.3.5 Mobility

These requirements specify the features of the accessible voting station designed to assist voters who use mobility aids, including wheelchairs. Many of the requirements of this section are based on the ADA Accessibility Guidelines for Buildings and Facilities (ADAAG).

→ **3.3.5-A** Clear Floor Space

The accessible voting station ***SHALL*** provide a clear floor space of 30 inches (760 mm) minimum by 48 inches (1220 mm) minimum for a stationary mobility aid. The clear floor space ***SHALL*** be level with no slope exceeding 1:48 and positioned for a forward approach or a parallel approach.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

DISCUSSION

Click here and type the discussion about this requirement

→ **3.3.5-B** Allowance for Assistant

When deployed according to the installation instructions provided by the vendor, the voting station ***SHALL*** allow adequate room for an assistant to the voter. This includes clearance for entry to and exit from the area of the voting station.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

Disabled voters sometimes prefer to have an assistant help them vote. The setup of the voting station should not preclude this.

→ **3.3.5-C** Visibility of Displays and Controls

All labels, displays, controls, keys, audio jacks, and any other part of the accessible voting station necessary for the voter to operate the voting system ***SHALL*** be easily legible and visible to a voter in a wheelchair with normal eyesight (no worse than 20/40, corrected) who is in an appropriate position and orientation with respect to the accessible voting station.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

DISCUSSION

There are a number of factors that could make relevant parts of the accessible voting station difficult to see such as; small lettering, controls and labels tilted at an awkward angle from the voter's viewpoint, and glare from overhead lighting.

### 3.3.5.1 Controls within Reach

The requirements of this sub-section ensure that the controls, keys, audio jacks and any other part of the accessible voting station necessary for its operation are within easy reach. Note that these requirements have meaningful application mainly to controls in a fixed location. A hand-held tethered control panel is another acceptable way of providing reachable controls.

→ **3.3.5.1-A** Forward Approach, No Obstruction

If the accessible voting station has a forward approach with no forward reach obstruction then the high reach ***SHALL*** be 48 inches maximum and the low reach ***SHALL*** be 15 inches minimum. See Figure 1.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

DISCUSSION

Click here and type the discussion about this requirement

→ **3.3.5.1-B** Forward Approach, with Obstruction

If the accessible voting station has a forward approach with a forward reach obstruction, the following sub-requirements apply (See Figure 2).

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

DISCUSSION

Click here and type the discussion about this requirement

↳ **3.3.5.1-B.1** Maximum Size of Obstruction

The forward obstruction ***SHALL*** be no greater than 25 inches in depth, its top no higher than 34 inches and its bottom surface no lower than 27 inches.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

↳ **3.3.5.1-B.2** Maximum High Reach over Obstruction

If the obstruction is no more than 20 inches in depth, then the maximum high reach ***SHALL*** be 48 inches, otherwise it ***SHALL*** be 44 inches.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

↳ **3.3.5.1-B.3** Toe Clearance under Obstruction

Space under the obstruction between the finish floor or ground and 9 inches (230 mm) above the finish floor or ground ***SHALL*** be considered toe clearance and ***SHALL*** comply with the following provisions:

- Toe clearance depth ***SHALL*** extend 25 inches (635 mm) maximum under the obstruction
- The minimum toe clearance depth under the obstruction ***SHALL*** be either 17 inches (430 mm) or the depth required to reach over the obstruction to operate the accessible voting station, whichever is greater
- Toe clearance width ***SHALL*** be 30 inches (760 mm) minimum

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

↳ **3.3.5.1-B.4** Knee Clearance under Obstruction

Space under the obstruction between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground ***SHALL*** be considered knee clearance and ***SHALL*** comply with the following provisions:

- Knee clearance depth ***SHALL*** extend 25 inches (635 mm) maximum under the obstruction at 9 inches (230 mm) above the finish floor or ground

- The minimum knee clearance depth at 9 inches (230 mm) above the finish floor or ground ***SHALL*** be either 11 inches (280 mm) or 6 inches less than the toe clearance, whichever is greater
- Between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground, the knee clearance depth ***SHALL*** be permitted to reduce at a rate of 1 inch (25 mm) in depth for each 6 inches (150 mm) in height. (It follows that the minimum knee clearance at 27 inches above the finish floor or ground ***SHALL*** be 3 inches less than the minimum knee clearance at 9 inches above the floor.)
- Knee clearance width ***SHALL*** be 30 inches (760 mm) minimum

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

→ **3.3.5.1-C** Parallel Approach, No Obstruction

If the accessible voting station has a parallel approach with no side reach obstruction then the maximum high reach ***SHALL*** be 48 inches and the minimum low reach ***SHALL*** be 15 inches. See Figure 3.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

→ **3.3.5.1-D** Parallel Approach, with Obstruction

If the accessible voting station has a parallel approach with a side reach obstruction, the following sub-requirements apply. See Figure 4.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

D I S C U S S I O N

Since this is a parallel approach, no clearance under the obstruction is required.

↳ **3.3.5.1-D.1** Maximum Size of Obstruction

The side obstruction ***SHALL*** be no greater than 24 inches in depth and its top no higher than 34 inches.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

↳ **3.3.5.1-D.2** Maximum High Reach over Obstruction

If the obstruction is no more than 10 inches in depth, then the maximum high reach ***SHALL*** be 48 inches, otherwise it ***SHALL*** be 46 inches.

*Applies to:* *Acc-VS*

*Test Reference:* *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

[[Mobility figures go here.]]

## 3.3.6 Hearing

These requirements specify the features of the accessible voting station designed to assist voters with hearing disabilities.

→ **3.3.6-A** Reference to Audio Requirements

The accessible voting station ***SHALL*** incorporate the features listed under requirement 3.3.3-C XREF "Audio Features and Characteristics" for voting equipment that provides audio presentation of the ballot.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

D I S C U S S I O N

Note especially the requirements for volume initialization and control.

→ **3.3.6-B** Visual Redundancy for Sound Cues

If the voting system provides sound cues as a method to alert the voter, the tone ***SHALL*** be accompanied by a visual cue, unless the station is in audio-only mode.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

For instance, the voting equipment might beep if the voter attempts to overvote. If so, there would have to be an equivalent visual cue, such as the appearance of an icon, or a blinking element. If the voting system has been set to audio-only mode, there would be no visual cue.

→ **3.3.6-C** No Electromagnetic Interference with Hearing Devices

No voting equipment ***SHALL*** cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices. The voting equipment, considered as a wireless device, ***SHALL*** achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.

*Applies to:* *Voting device*

*Test Reference:* *Functional*

DISCUSSION

"Hearing devices" include hearing aids and cochlear implants.

## 3.3.7 Cognition

These requirements specify the features of the accessible voting station designed to assist voters with cognitive disabilities.

→ **3.3.7-A** General Support for Cognitive Disabilities

The accessible voting station should provide support to voters with cognitive disabilities.

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

DISCUSSION

Because of the highly varied nature of disabilities falling within the "cognitive" category, there are no design features uniquely aimed at helping those with such disabilities. However, many of the features designed primarily for other disabilities and for general usability are also highly relevant to these voters:

- the synchronization of audio with the displayed screen information (3.3.2-F XREF)

- the general cognitive usability requirements (3.2.3 XREF) and, in particular, the use of plain language (3.2.3-C XREF)
- large font sizes (3.3.2-B XREF)
- the ability to control various aspects of the audio presentation (3.3.3-B and 3.3.3-C XREF) such as pausing, repetition, and speed

## 3.3.8 English Proficiency

These requirements specify the features of the accessible voting station designed to assist voters who lack proficiency in reading English.

→ **3.3.8-A** Use of ATI

For voters who lack proficiency in reading English, the voting equipment ***SHALL*** provide an audio interface for instructions and ballots as described in section 3.3.3-B XREF "Audio-Tactile Interface".

*Applies to:* *Acc-VS*

*Test Reference:* *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

## 3.3.9 Speech

→ **3.3.9-A** Speech not to be Required by Equipment

No voting equipment ***SHALL*** require voter speech for its operation.

*Applies to:* *Voting System*

*Test Reference:* *Functional*

D I S C U S S I O N

This does not preclude voting equipment from offering speech input as an option, but speech must not be the only means of input.

# Chapter 4: Security and Audit Architecture Requirements

## 4.1 Introduction/Scope Voting equipment which complies with the VVSG2007 must support the necessary set of procedures to achieve software dependence.

Software independence means that incorrect behavior of a voting system leading to a change in the results of the election can, in principle, be detected. This kind of incorrect behavior can be detected through the use of good auditing steps; without such steps, the voting system's bad behavior would not reliably be caught. In this chapter, the minimal set of procedures needed to achieve software independence is specified, and requirements imposed by the need to support these procedures are specified for each voting system architecture.

There are broadly two kinds of auditing steps:

- Steps to ensure that all the available records from the voting system agree. These include:
  - Pollbook audit -- verifying that the number of voters for each precinct or election district, and using each ballot style, agrees with the totals reported by the voting equipment. This guards against a voting machine reporting more votes than it had voters, or reassigning some voters to the wrong precinct or ballot style.
  - Hand audit of paper and electronic records -- verifying that the voter-verifiable paper records agree with the reported totals from the voting machine. This guards against a voting machine silently misrecording the voter's votes.
  - Checking machine records against final tally -- verifiying that the electronic records from the voting machine agree with the final reported totals. This guards against a compromised tally server misreporting the final results.
- Steps to ensure that the voting machine is interacting with the voter properly and recording the votes fairly. These include:
  - Parallel Testing -- isolating some voting machines on election day, and testing them in a way intended to be impossible for the machines to distinguish from normal voting. This guards against the voting machine introducing errors to favor some candidate, omitting choices, skipping races, or simply recording the wrong choice in both

electronic and paper records, in hopes that the voter will not notice the contents of the paper record.

- Spot Parallel Testing -- testing ballot marking devices during the election, by entering choices based on a testing script, and then verifying that the printed ballot correctly represents those choices.
- Observational Testing -- sending testers who are authorized to vote in an election to cast their own votes, but to do so using assistive technology such as audio ballots. This guards against the voting machine selectively recording the wrong choice on both paper and electronic records when a voter appears not to be able to verify the paper record.In order to be software independent, each voting system shall support all the steps to ensure that the records agree. VVPAT systems shall support parallel and observational testing; ballot markers shall support spot parallel and observational testing.

The first three auditing steps, intended to ensure the agreement of all available sets of records, are normal parts of current election procedure in many places. Support for these is required of all voting systems; requirements in this chapter provide additional support for these common procedural defenses, and ensure that they can be done in a secure way. The second three auditing steps, intended to ensure the correctness of the voting system's interaction with the voter, are not common election practice, and apply specifically to VVPAT systems and ballot marking devices. Support for these procedural defenses ensures that they can be used effectively.

Support for the full set of auditing procedures described in this chapter imposes a number of different requirements. In order to support the audit steps to ensure that pollbooks, paper records, electronic records, and the final tally from the election are in agreement, extensive requirements on the contents of the electronic records from each voting machine or PCOS scanner, the paper records or ballots used, and the final election tally appear below and in the Electronic Records and VVPR chapters. In order to support the audit steps to ensure that the voting system is presenting choices and recording votes correctly, requirements on the design and behavior of the voting system appear below. Parallel testing imposes the largest requirements of this kind; observational testing and spot parallel testing are much less difficult to accommodate.

### 4.1.1 Auditing Procedures Affect Equipment Requirements

The auditing procedures impose requirements for the equipment in three ways:

- Some procedures need specific information or behavior from voting systems in order to be possible or practical. For example, hand-auditing paper and electronic records is only possible if all voting systems produce paper and electronic records that count the same thing.
- Some procedures require certain assurances about the operation of the voting equipment, in order 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.

- Some requirements of these procedures raise other potential security problems, which must be addressed by other requirements. For example, electronic records summarizing the votes cast on a given voting machine must be produced in a way that does not violate ballot secrecy.

## 4.2 Requirements for Supporting Auditing Procedures

This subsection outlines the testable requirements on voting system equipment and documentation for supporting the required auditing procedures.

### 4.2.1 Pollbook Audit

The purpose of the pollbook audit is to verify that:

- The total number of ballots recorded by the voting system in some location is the same as the total number of voters authorized to cast votes.
- The total number of ballots for each precinct or election district, and for each ballot style, is the same as the total number of voters authorized to vote in that precinct, election district, and ballot style.

This addresses the threat that a tampered voting machine or scanner might have inserted or deleted votes, and also the threat that it may have assigned some voters the wrong precinct, election district, or ballot style to prevent them voting in certain elections or to dilute the effect of their votes.[[Note: This decreases the threat but does not eliminate it.]]

At a high level, the procedure is performed as follows:

- The total number of ballots, and the total number of each distinct type (ballot style, election district, precinct, etc.) is retrieved from the pollbook.
- The total number of ballots, and the number for each ballot style, precinct, or election district, are retrieved from the final tally report or the summary reports produced by the voting equipment. The totals from different machines within one polling place may have to be added together to get counts.
- The numbers are compared, and any discrepancies explained and/or reported.

→ **4.2.1-A** Support for Pollbook Audit

The voting equipment ***SHALL*** support the pollbook audit.

*Applies to:* *Voting System*

*Test Reference:*

D I S C U S S I O N

The pollbook audit is critical for blocking some known attacks on voting systems. All voting systems must support the pollbook audit.

*Source:* *NIST Threats Workshop, Brennan Center Report*

*Impact:*

→ **4.2.1-B** Requirements on Voting System Records and Reports

The voting equipment ***SHALL*** produce records and reports which support the pollbook audit.

- Summary records produced by each voting machine ***SHALL*** include total number of ballots recorded, and total number of each ballot style and election district or precinct. The voting equipment ***SHALL*** support printing this report. See the Electronic Records section.
- The final election tally report ***SHALL*** include total number of ballots recorded and total number of each ballot style and election district, broken down by polling place. The voting equipment ***SHALL*** support printing this report. See the Electronic Records section.
- Each paper record or ballot ***SHALL*** include enough information for an auditor to unambiguously determine the ballot style, election district, and precinct without relying on additional equipment. See the VVPR section.

*Applies to:* *VVPAT, PCOS*

*Test Reference:*

D I S C U S S I O N

The pollbook audit is only practical when the number of ballots, and of each distinct type of ballot, is available from both the pollbooks and the voting equipment. In order to ensure that the number of ballots of each type in the summary report from the equipment is accurate, the same information must appear for each paper record; this permits the hand-audit (see below) to catch discrepancies. Finally, including the number of ballots of each type, broken down by polling place, in the final reported tally from the election allows an auditor to verify agreement between the number of ballots of each type included in final tally, and the number authorized and recorded in the pollbook.

*Source:*

*Impact:*

→ **4.2.1-C** Documentation Requirement

The voting system's user documentation ***SHALL*** fully specify a workable and accurate process for producing all records necessary from the equipment and carrying out the pollbook audit.

*Applies to:* *Voting systems*

*Test Reference:*

D I S C U S S I O N

In order to fully support the pollbook audit, the voting system documentation must provide enough information for election officials to carry out the auditing step. This includes explaining how to generate all needed reports, how to check the reports against one another for agreement, and how to deal with errors and other unusual problems that come up during the audit step.

*Source:*

*Impact:*

→ **4.2.1-D** OEVT Testing

The voting system's documented procedure for pollbook audit ***SHALL*** achieve the critical security requirements of pollbook auditing, even in the face of attack.

- The pollbook audit ***SHALL*** not indicate agreement of number of ballots of each type authorized and recorded, unless these numbers are actually in agreement.

*Applies to:* *Voting systems*

*Test Reference:* *OEVT*

D I S C U S S I O N

The process documented by the vendor needs to be checked by the VSTL, both to make sure it works, and to verify that it accomplishes the security goals of pollbook auditing.

*Source:*

*Impact:*

## 4.2.2 Hand Audit of Paper Record

The hand audit of paper record applies to VVPAT and PCOS voting systems.

All approved voting systems in VVSG2007 produce a voter-verifiable paper record, as well as electronic records from the voting process. The hand audit of paper record procedure verifies that these records are in substantial agreement. This procedure addresses the threats that the voting machine or scanner might record results electronically that disagree with the choices indicated by the voter.

The procedure is done as follows:

- Several polling places or voting machines are randomly selected for auditing.
- The set of races or ballot questions to be recounted is selected.
- For each polling place or voting machine to be audited:
  - The paper records from each polling place or machine to be audited are brought in for counting.
  - The electronic summary record from each scanner or voting machine is printed out.
  - The auditing team hand counts the paper records for the races to be recounted. It also hand counts the total number of paper ballots/records, and the total number for each ballot style.
- The auditing team verifies that its counting results agree with those from the summary report.

→ **4.2.2-A** Support for hand audit of paper records

The voting system ***SHALL*** support the hand audit of paper records.

*Applies to:* *Voting System*

*Test Reference:*

D I S C U S S I O N

Hand-auditing paper records to verify agreement with reported electronic records is necessary to detect misbehavior by voting equipment; voter-verifiable paper records offer the voter an opportunity to discover attempts to misrecord his vote on the paper record, and the hand-audit ensures that equipment that misrecords votes on the electronic record but not the paper record is very likely to be caught.

*Source:*

*Impact:*

→ **4.2.2-B** Electronic Records Requirements to Support Hand Auditing

The following requirements apply to all voting systems that must support the hand audit procedure:

- The electronic summary record from the voting machine or scanner ***SHALL*** provide all information necessary to hand-audit the paper

records, and the equipment ***SHALL*** provide a means to print out the summary records needed to support hand audit. See the Electronic Records chapter for more details.

- The final election tally ***SHALL*** contain all information necessary to hand-audit at the precinct level, and equipment ***SHALL*** support the production of information necessary to support the hand audit at the individual VVPAT level. The equipment ***SHALL*** support printing out the summary records needed to support hand audit. See the Electronic Records chapter for more details.
- The paper record of each cast ballot ***SHALL*** include all information necessary to carry out the hand-audit, including:
- The precinct, election district, and ballot style of this ballot.
- Inclusion of the paper record of a given ballot or ballot summary ***SHALL*** be strong evidence that the ballot was available for review by the voter, and was accepted by the voter.

*Applies to:* *Voting System*

*Test Reference:*

D I S C U S S I O N

The electronic summary information from the voting machine or scanner, and the paper records, must contain sufficient information to carry out the hand audit. This means that summaries of the totals from either the voting machines or the final tally must be easy to produce, and that these must be directly usable in carrying out a hand-audit. The hand audit is meaningful only if inclusion of the paper record on the paper roll as an accepted vote summary, or in a ballot box as a cast vote, is strong evidence that the voter had the chance to review the ballot or ballot summary, and approved it.

*Source:*

*Impact:*

→ **4.2.2-C** Requirements on VVPAT paper-roll equipment

The following requirements apply specifically to VVPAT systems using a paper roll. For more complete requirements, see the VVPR chapter.

- Each paper roll ***SHALL*** identify the voting machine which produced it, the election, and the set of available precincts, election districts, and ballot styles.
- Each ballot record on the roll ***SHALL*** begin with an unambiguous indication of the precinct, election district, and ballot style used. If the ballot is provisional or otherwise needs special processing during auditing or recounts, it ***SHALL*** indicate this in an unambigous human-readable way.
- If multiple rolls are used in a single election, the rolls ***SHALL*** indicate the total number of rolls so far, e.g., “Election 11, District 214, Machine 7991, Roll 2”
- Each ballot record on the roll ***SHALL*** include a clear indication of the voter’s vote on each race on the ballot, including an unambiguous indication of undervotes.

- Each accepted ballot record ***SHALL*** end with a printed indication that the ballot was accepted. This ***SHALL*** be printed when the voter indicates acceptance of the vote.
- Each rejected ballot record ***SHALL*** end with a printed indication that the ballot was rejected. This ***SHALL*** be printed when the voter indicates rejection of the vote.
- Expended paper rolls ***SHALL*** be closed in a container which permits tamper-evident sealing, to protect voter privacy.
- The voting system ***SHALL*** include equipment to support efficient and accurate hand-counting of paper rolls.

*Applies to:* *VVPAT with paper rolls*

*Test Reference:*

D I S C U S S I O N

Paper rolls provide some security and usability benefits in auditing, because a set of ballot summaries are bound together on a single roll of paper. Information identifying the voting machine which produced the records must be placed on each paper roll, to ensure that the hand-audit can determine which machine's electronic records must agree with the paper records.

Paper rolls also raise many issues. They are very difficult to use in hand-auditing and recounts without special equipment to make this use easier. They store the ballot summaries in order, which places ballot secrecy at risk. The movement of the paper roll into the VVPAT device is under the control of the DRE, raising the possibility of the DRE accepting or rejecting some ballot summaries without the voter's approval. The above requirements address these concerns.

*Source:* *NIST Threats Workshop, Brennan Center Report*

*Impact:*

→ **4.2.2-D** Requirements on VVPAT-cut sheet equipment

The following specific requirements apply to VVPAT voting systems with cut-sheet paper records. For further requirements, see the chapter on VVPR requirements.

- Each ballot summary ***SHALL*** contain an unambiguous indication of the machine, voting location, and ballot precinct, election district, and ballot style. If the ballot is provisional or otherwise needs special processing during auditing or recounts, it ***SHALL*** indicate this in an unambigous human-readable way.
- A ballot summary ***SHALL*** not be spread across multiple sheets. [[Discuss? This prevents off the shelf printers, which is bad, but not following it would make hand audits potentially difficult.]]
- Each sheet ***SHALL*** contain an unambiguous indication of the voter's vote on each race in the ballot, including an unambiguous indication of undervotes.

- Each accepted ballot record ***SHALL*** include an indication that it was accepted. This ***SHALL*** be printed on the sheet when the voter indicates acceptance of the vote.
- Each rejected ballot record ***SHALL*** include an indication that it was rejected. This ***SHALL*** be printed on the sheet when the voter indicates rejection of the vote.

*Applies to:* *VVPAT cut sheet*

*Test Reference:*

D I S C U S S I O N

Each ballot summary must include all information needed to identify which machine produced it, which type of ballot it is (ballot style, precinct, election district, etc.). All this information is necessary to support the hand-audit. Unambiguous rejection and acceptance markings address the threat that the DRE might attempt to reject or accept ballot summaries without the voter's approval.

*Source:*

*Impact:*

→ **4.2.2-E** Requirements on PCOS systems

The following specific requirements apply to PCOS voting systems. For further requirements, see the chapter on VVPR requirements:

- Each printed ballot ***SHALL*** indicate, in human-readable form, all information needed to process it. This includes precinct, election districti, ballot style, provisional status, etc.

*Applies to:* *PCOS*

*Test Reference:*

D I S C U S S I O N

PCOS systems are already designed to support recounts.

*Source:*

*Impact:*

→ **4.2.2-F** Documentation

The user documentation ***SHALL*** provide directions for a workable and effective hand audit procedure

*Applies to:* *Voting systems*

*Test Reference:* *OEVT*

DISCUSSION

The user documentation must explain how to produce all necessary reports and reconcile the paper and electronic records by hand-auditing.

*Source:*

*Impact:*

→ **4.2.2-G** OEVT Testing

The voting system's documented procedure for hand audit ***SHALL*** achieve the critical security requirements of hand auditing, even in the face of attack.

- The hand audit ***SHALL*** not indicate agreement of paper and electronic records, unless these numbers are actually in agreement.

*Applies to:* *Voting systems*

*Test Reference:* *OEVT*

DISCUSSION

The process documented by the vendor needs to be checked by the VSTL, both to make sure it works, and to verify that it accomplishes the security goals of hand auditing.

*Source:*

*Impact:*

## 4.2.3 Reconciling Machine/Precinct and Final Totals

The purpose of this procedure is to verify that the final reported election tally reflects the totals from each individual scanner and voting machine, plus any additions from absentee ballots, provisional ballots, and other special cases. This guards against the threat that the computer used to produce the final tally might be compromised.

At a high level, the procedure is done as follows:

- The final tally is produced according to the requirements in the Electronic Records chapter. This provides totals broken down at the level of individual polling places and individual voting machines. [[These may need to be obscured in some cases to protect voter privacy—this is an open issue.]]
- For each machine in the total which produced an electronic summary record according to the Electronic Records chapter:
  - The auditor verifies that the included from the final tally agree with the totals from the machine.

- The auditor verifies that the included set of ballot styles, precincts, election districts, etc., from each summary agrees with that from the final report.
- The auditor verifies the digitial signatures.

- For each machine whcih did not produce an electronic summary record according to the Electronic Records chapter:
  - The auditor verifies the agreement of final tally and machine or precinct records using whatever information is available.
- The auditor verifies that the total number of ballots in the adjustments for writeins and provisional ballots either does not change any election outcomes, or is consistent with the number of such ballots indicated in the summary reports.

→ **4.2.3-A** Support for Reconciling Machine Totals and Final Tally

The voting equipment ***SHALL*** support the reconciliation of the machine totals and the final election tally.

*Applies to:* *Voting System*

*Test Reference:*

D I S C U S S I O N

This auditing step simply supports the existing canvassing procedure. Every voting system must support this procedure, as it is the only defense against misbehavior by the machine computing the final election tally and producing the report. The Electronic Records chapter includes requirements to make this procedure easier to carry out, and to add cryptographic protection to the records produced by the voting machines. One complication in making a full voting system support this procedure is the likely mixing of old and new voting equipment in a full voting system.

*Source:*

*Impact:*

→ **4.2.3-B** Requirements on Voting System Records and Reports

The voting equipment ***SHALL*** produce records and reports which support the reconciliation.

- Electronic records produced by each voting machine or scanner ***SHALL*** include totals for each distinct type of ballot.
- The final election tally report ***SHALL*** include totals broken down by voting machine or scanner, and for each machine/scanner, broken down for each distinct type of ballot. This may leave provisional and write-in votes uncounted (specified only as provisional ballots, counted only as generic write-ins) to preserve privacy.

- The final election tally report ***SHALL*** include total number of ballots, and total number of ballots of each type, for each voting machine or scanner.
- The final election tally report ***SHALL*** be capable of including digitial signature information from the electronic summary records of individual voting machines and scanners.
- The final election tally report may include adjustments for provisional ballots and write-ins. These need not be linked to specific machines or polling places.

See the Electronic Records chapter for more details on these and related requirements.

*Applies to:* *VVPAT, PCOS, Pollbook Software*

*Test Reference:*

D I S C U S S I O N

This auditing step requires that electronic summary records from voting machines and scanners can be reconciled with the final election tally report. The final election tally report must thus be capable of breaking down totals by voting machine as well as by precinct.

*Source:* *NIST Threats Workshop, Brennan Center Report*

*Impact:*

→ **4.2.3-C** Documentation Requirement

The voting system's user documentation ***SHALL*** fully specify a workable and accurate process for reconciling the voting machine/scanner summary records and the final election tally.

*Applies to:* *Voting systems*

*Test Reference:*

D I S C U S S I O N

In order to fully support the audit, the voting system documentation must provide enough information for election officials to carry out the auditing step. This includes explaining how to generate all needed reports, how to check the reports against one another for agreement, and how to deal with errors and other unusual problems that come up during the audit step.

*Source:*

*Impact:*

→ **4.2.3-D** OEVT Testing

The voting system's documented procedure for reconciling voting machine summary records and the final election tally ***SHALL*** achieve the critical security requirements of the audit, even in the face of attack.

- The audit ***SHALL*** not indicate agreement of voting system summary records and the final election tally, unless these numbers are actually in agreement.

*Applies to:* *Voting systems*

*Test Reference:* *OEVT*

DISCUSSION

The process documented by the vendor needs to be checked by the VSTL, both to make sure it works, and to verify that it accomplishes the security goals.

*Source:*

*Impact:*

## 4.2.4 Spot Parallel Testing

Spot parallel testing can be done only on ballot-marking devices. The purpose of spot parallel testing is to ensure that a ballot marking device is presenting the ballot correctly to the voters, and is recording the voters' choices correctly. This addresses the threat that the ballot marker could introduce errors in one candidate's favor, skip races, omit choices, or misprint the voter's choices on the ballot.

The procedure is done as follows:

- A set of polling places and machines are selected at random.
- For each machine being tested:
  - The auditor carries out his test during the normal voting time.
  - The auditor makes selections based on a testing script, and has a picture of the full set of ballot choices he should have.
  - The auditor notes any unusual behavior noticed immediately.
  - The auditor brings his note, testing script, and the marked ballot back for analysis as needed.

→ **4.2.4-A** Support for Spot Parallel Testing

Ballot marking devices ***SHALL*** support spot parallel testing.

*Applies to:* *Ballot markers*

*Test Reference:*

DISCUSSION

Spot parallel testing provides a lightweight alternative to full parallel testing for ballot marking devices.

*Source:* *NIST Threats Workshop, Brennan Center Report*

*Impact:*

→ **4.2.4-B** Requirements on Authentication of Voter to Ballot Marker

The mechanism for authenticating the voter to the ballot marking device ***SHALL*** not allow the ballot marker to distinguish testers from normal voters, even with the pollworker's help.

*Applies to:* *Ballot markers, Pollbook Software*

*Test Reference:*

DISCUSSION

Spot parallel testing would not detect attacks if the ballot marker were somehow alerted that the tester was carrying out the test. Thus, the authentication mechanism must not permit the machine to discover this fact.

*Source:* *NIST Threats Workshop, Brennan Center Report*

*Impact:*

→ **4.2.4-C** No Networking of Ballot Marker During Voting

Ballot markers ***SHALL*** not permit communications with other devices during the vote collecting process.

*Applies to:* *Voting systems*

*Test Reference:*

DISCUSSION

Network connections from other devices to the ballot marker could be used to signal the ballot marker when a spot parallel test was taking place.

*Source:*

*Impact:*

→ **4.2.4-D** Documentation Requirement

The voting system's user documentation ***SHALL*** fully specify a workable and accurate process for spot parallel testing.

*Applies to:* *Voting systems*

*Test Reference:*

DISCUSSION

*Source:*

*Impact:*

➜ **4.2.4-E** OEVT Testing

The voting system's documented procedure for spot parallel testing ***SHALL*** achieve the critical security requirements, even in the face of attack.

- The ballot marking device ***SHALL*** not be able to distinguish testers from normal voters, even when the person giving the tester authorization to vote attempts to signal this fact to the ballot marker.

*Applies to:* *Voting systems*

*Test Reference:* *OEVT*

DISCUSSION

The process documented by the vendor needs to be checked by the VSTL, both to make sure it works, and to verify that it accomplishes the security goals.

*Source:*

*Impact:*

## 4.2.5 Observational Testing

The purpose of observational testing is to ensure that voting machine is printing a correct representation of the voter's choices on the paper record, even when the voter is using assistive technology. This addresses the threat that the voting machine will misrecord votes on both paper and electronic records when the voter appears unable to verify the paper record.

At a high level, the procedure is done as follows:

- Several election officials and volunteers agree to take part in the testing.
- Each tester is given a full description of the ballot as it is supposed to be presented to him.
- Each tester votes at his normal location, using assistive technology such as audio ballot or screen reader. The tester verifies that the printed version of his ballot is correct.
- The tester reports any problems noted, as well as using the normal process of complaining about malfunctioning machines.

→ **4.2.5-A** Support for Observational Testing

Voting machines which interact with the voter to collect votes and support assistive technology ***SHALL*** support observational testing.

*Applies to:* *VVPAT, ballot markers*

*Test Reference:*

D I S C U S S I O N

Blind, low-sight, and some alternative language voters cannot directly verify the paper record produced by the voting system, but must indicate their inability to verify the paper record to the voting machine by requesting an audio ballot, magnified screen images, or other assistive technology. This raises the possibility that a malicious voting machine could steal these voters' votes, by simply recording the wrong votes on both electronic and paper records. Observational testing provides a defense; a few hundred voters using the assistive technology are also looking carefully at the paper record, and will notice any problem. When observational testing is in use, a malicious voting machine cannot safely assume that a voter using an audio ballot will be unable to check the paper record.

*Source:*

*Impact:*

→ **4.2.5-B** Equipment Requirements for Supporting Observational Testing

The following equipment requirements support observational testing:

- The mechanism for authenticating the voter to the ballot marking device ***SHALL*** support observational testing.
- Authentication codes or tokens given to the voter ***SHALL*** not allow the ballot marker to distinguish between testers and normal voters, even when the pollworker is trying to signal the machine of this fact.

*Applies to:* *VVPAT, ballot markers, Pollbook Software*

*Test Reference:*

D I S C U S S I O N

Observational testing would not detect attacks if the voting machine were somehow alerted that the tester was carrying out the test. Thus, the authentication mechanism must not permit the machine to discover this fact.

The requirements on the equipment for supporting observational testing are extremely limited.

*Source:*

*Impact:*

→ **4.2.5-C** Documentation Requirement

The voting system's user documentation ***SHALL*** fully specify a workable and accurate process for observational testing.

*Applies to:* *Voting systems*

*Test Reference:*

D I S C U S S I O N

*Source:*

*Impact:*

→ **4.2.5-D** OEVT Testing

The voting system's documented procedure for observational testing ***SHALL*** achieve the critical security requirements, even in the face of attack.

- The voting machine ***SHALL*** not be able to distinguish testers from normal voters, even when the person giving the tester authorization to vote attempts to signal this fact to the ballot marker.

*Applies to:* *Voting systems*

*Test Reference:* *OEVT*

D I S C U S S I O N

The process documented by the vendor needs to be checked by the VSTL, both to make sure it works, and to verify that it accomplishes the security goals.

*Source:*

*Impact:*

## 4.2.6 Full Parallel Testing

The purpose of parallel testing is to verify the correct operation of a voting machine. Parallel testing addresses the threat that a voting machine is introducing occasional errors in favor of one candidate, or is presenting the choices in an incorrect way to some or all voters.

The procedure is carried out as follows:

- A few voting machines are randomly selected for parallel testing.
- The selected machines are isolated from all other machines at the polling place.
- The selected machines are subjected to a test election, according to a testing script. The whole test is videotaped, and the voter is

- The results are reviewed and compared with the scripts to detect misbehavior.

→ **4.2.6-A** Support for Parallel Testing

VVPAT voting machines ***SHALL*** support parallel testing.

*Applies to:* *VVPAT*

*Test Reference:*

D I S C U S S I O N

Parallel testing requires the ability to isolate the voting machine being tested, so that:

- Votes entered into the machine being tested are stored in a separate way from real votes.
- The voting machine is isolated, so that it cannot receive signals from anyone except the testing team.
- The voting machine cannot detect this isolation or separation.
- The voting machine commits to its electronic totals before it is allowed any outside interaction.

*Source:*

*Impact:*

→ **4.2.6-B** No Networking While Polls Open

The unit of voting equipment to be parallel tested ***SHALL*** not be capable of sending or receiving signals to any machine not either being tested or part of the testing team's equipment during voting.

The unit being tested may include more than one voting machine. However, the whole unit is tested together, with nobody not on the testing team interacting with any machine in that unit, and may have no external communications. Thus:

- If the unit being tested is a single machine, the machine ***SHALL*** not be networked to any other machine.
- If the unit being tested is a judges' station connected to a voting machine, the pair ***SHALL*** not be networked to any other machine.
- If the unit being tested is a small network of voting machines connected together, then that small network ***SHALL*** not be connected to any other machines.

*Applies to:* *VVPAT*

*Test Reference:*

DISCUSSION

If the machine or small group of machines being tested were connected to outside machines under the control of someone other than the testing team, that connection could be used to signal the voting machines that they were being tested, and thus that they should not trigger any malevolent behavior.

*Source:*

*Impact:*

→ **4.2.6-C** No Sharing of Resources

Voting machines and sets of equipment that must support parallel testing ***SHALL*** not share resources such as storage devices or printers, in which any signal or information can flow back from the shared resource to the voting machine.

*Applies to:* *VVPAT*

*Test Reference:*

DISCUSSION

Any shared resources of this kind can allow a covert channel, which would violate the isolation of the voting machine. This has the potential of either allowing the voting machine to learn that it is being isolated (if it is removed from access to the shared resource) or allowing it to receive a signal warning it not to trigger its attack behavior (if it remains connected to the shared resource).

*Source:*

*Impact:*

→ **4.2.6-D** Requirements on Voter Authorization Mechanisms to Support Parallel Testing

The mechanism by which the voter is authorized to vote, and a specific ballot style chosen for him, ***SHALL*** not permit anyone not part of the testing team to alter or control the issuance of authorizations to vote for the machine or machines being tested.

There are two broad requirements on the authorization mechanism:

- The authorization mechanism ***SHALL*** not permit communications of any kind from any person outside the testing team, or machine not being tested, to the machine(s) being tested.
- The authorization mechanism as used by the testing team (as directed in the user documentation for parallel testing support) ***SHALL***

not be possible for the equipment being tested to distinguish from the normal authorization mechanism used in voting.

This leads to the following requirements on specific mechanisms for authorizing votes:

- If authorization is done by physical key, switch, or related mechanism, the testing team ***SHALL*** have access to a copy of the physical key, the switch, etc. The poll workers ***SHALL*** not be part of the authorization process.
- If authorization is done by alphanumeric access code, the testing team ***SHALL*** be capable of generating numerical access codes for the voting machine. Procedural or technical barriers ***SHALL*** prevent testing team members from using this capability to cast unauthorized votes on other machines in the polling place.
- If authorization is done by rewriteable token, the following requirements apply:
  - The testing team ***SHALL*** be capable of generating a sufficiently large set of rewriteable tokens that the voting machine cannot distinguish this set from the set used in the normal voting process.
  - Normal election procedures ***SHALL*** completely erase the memory of the tokens between uses. The voting machines ***SHALL*** enforce this by failing if they find unexpected information on the token.
  - The testing team may need to bring replacement tokens, and use the set provided for the polling place originally, to avoid alerting the voting machine.
  - Rewriteable tokens used for this purpose should not be reused during a single election, if they contain serial numbers or other identifying information which is available to the voting machines.

*Applies to:* *VVPAT*

*Test Reference:*

D I S C U S S I O N

The mechanism for authorizing voters to vote must be available for the testing team, in order to carry out parallel testing. However, this must not become a mechanism by which the voting equipment is warned that it is being tested.

*Source:*

*Impact:*

→ **4.2.6-E** Commitment to Results Before External Communications Allowed

The voting equipment being tested ***SHALL*** commit to its results before it is permitted to connect to any outside device to transmit its results.

The voting machine ***SHALL*** commit to its totals immediately after it is closed down and before it is allowed to connect to any server (even one operated by

the testing team) or to have any communication outside the isolated testing environment. This may be done in the following ways:

- A voting machine with a printer may print the summary totals.
- A voting machine with a display screen or a printer may print a cryptographic hash of the machine's summary report. This ***SHALL*** be the same hash value used in the digital signature on the report.

*Applies to:* *Voting systems*

*Test Reference:*

D I S C U S S I O N

*Source:*

*Impact:*

→ **4.2.6-F** Documentation Requirement

The voting system's user documentation ***SHALL*** fully specify a workable and accurate process for parallel testing.

The user documentation for parallel testing ***SHALL*** include:

- Best practices for parallel testing as specified by TBD
- Guidance for testing script generation and an acceptable sample test script.
- Precise steps to be taken to isolate the voting machine without alerting it to its isolation.
- How the commitment to the results is produced before the machine is connected to any outside device or machine.
- How the commitment is to be verified against the electronic records from the voting machine.

*Applies to:* *VVPAT*

*Test Reference:*

D I S C U S S I O N

Parallel testing is a very complicated procedural defense, with many ways it can go wrong. The user documentation for the voting system **SHALL** describe in detail how the parallel testing process must be carried out. The VSTL will use this description in evaluating whether the voting system supports parallel testing.

*Source:*

*Impact:*

→ **4.2.6-G** OEVT Testing

The voting system's documented procedure for parallel testing ***SHALL*** achieve the critical security requirements, even in the face of attack.

- Once the voting equipment to be parallel tested is isolated according to the procedures given in the user documentation, it ***SHALL*** not be capable of sending or receiving signals or interacting in any way with any machine or person not part of the testing team.
- The isolated voting equipment being parallel tested ***SHALL*** not be capable of discovering, based on what it can observe, whether it is being isolated and parallel tested or is being used in a normal voting process.
- The voting equipment ***SHALL*** not be capable of transmitting different results than those to which it committed before being connected to an outside device, without being detected with overwhelming probability.

*Applies to:* *Voting systems*

*Test Reference:* *OEVT*

D I S C U S S I O N

The process documented by the vendor needs to be checked by the VSTL, both to make sure it works, and to verify that it accomplishes the security goals. For parallel testing, this is especially important, as many possible failures of the requirements for parallel testing can only be detected by good open-ended testing.

*Source:*

*Impact:*

# Chapter 5: Electronic Records Requirements

## 5.1 Introduction/Scope

In order to support auditing, a voting system must be able to produce electronic and paper records that contain the needed information in a secure and usable manner. Section XX defines the general requirements on voting systems to support auditing. This chapter addresses the requirements that specifically relate to electronic records and Section XX address the requirements that specifically relate to paper records.

Electronic records include records produced by any type of voting machine such as DREs, Optical Scan tabulators, or electronic management systems. They typically include records such as:

- Vote counts;
- Counts of ballots recorded;
- Information that identify the electronic record;
- Event logs and other records of important events or details of how the election was run on this machine; or
- Election archive information.

By ensuring that certain reports are produced, secured, and exported, many attacks can be guarded against such as:

- Tampering with electronic records in transit from the polling place to the tabulation center.
- Tampering with the operation of the tabulation center; or
- Altering election records after the totals are determined.

There are two primary types of requirements related to electronic records. The first type addresses what data must be included in the electronic records and the second type addresses securing that data to prevent or detect changes. These requirements include those for cryptographically signing electronic records and ensuring that the records are in a publicly-specified format.

This chapter specifies requirements on electronic records used to move information about election results between machines within the full voting system, to support required auditing steps, and to report votes to the public.

# 5.2 Requirements on Electronic Records and Report

## 5.2.1 Requirements on All Records Produced by Voting Equipment

The following requirements apply to records produced by the voting system for any exchange of information between machines, support of auditing procedures, or reporting of final results.

➞ **5.2.1-A** Records required to be in open format

All electronic records in this chapter ***SHALL*** be produced in a fully specified, public format.

*Applies to:* *Voting Device*

*Test Reference:*

D I S C U S S I O N

Requiring all electronic records to appear in a public format ensures that election officials can read and review the contents of the records with software not provided by the voting system vendor. This permits auditors to get review the data in the records without the need to trust software provided by the vendor.

*Source:*

*Impact:*

➞ **5.2.1-B** Records to be capable of being printed

The voting system software ***SHALL*** provide the ability to produce printed forms of all records in this chapter. The printed forms ***SHALL*** retain all required information as specified for each record type.

*Applies to:* *Voting Device*

*Test Reference:*

D I S C U S S I O N

Printed versions of all records in this chapter are either necessary or extremely helpful to support required auditing steps, as specified in the Auditing chapter.

*Source:*

*Impact:*

## 5.2.2 Requirements on Records Produced by Voting Machines and Scanners

The following requirements apply to records produced by voting machines and scanners for exchange of information between machines, transmission of results to a central tabulation center, support of auditing procedures, or reporting of intermediate election results.

→ **5.2.2-A** Cryptographic Protection of Records from Voting Machines

All electronic records from voting machines in this chapter ***SHALL*** be digitally signed with the Election Signature Key, and ***SHALL*** include a certificate linking the records to the source machine's long-term signing key and ID.

*Applies to:* *Voting Device*

*Test Reference:*

D I S C U S S I O N

The Cryptography chapter specifies the production of the Election Signature Key (ESK), a per-election signing key; these keys are used to sign records from a single election. The Election Public Key Certificate links the per-election signing keys to a permanent per-machine signing key, and a unique identification of the machine which generated the key and the record. The digital signatures address the threat that the records might be tampered with in transit or in storage. The certificate linking each record to a machine addresses the threat that a legitimate electronic record might be misinterpreted as coming from the wrong voting machine or scanner. The use of per-election keys to sign these records addresses the threat that a compromise of a voting machine before or after election day might permit production of a false set of records for the election, which could then be reported to the tabulation center.

*Source:*

*Impact:*

→ **5.2.2-B** Requirement to Verify Signed Records

The tabulation center ***SHALL*** verify the correct receipt of electronic records from voting machines and scanners.

For each voting machine which produces electronic records according to this standard, the tabulation center ***SHALL*** verify that the election ID, timestamp, and digital signature are correct before accepting the record.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

The digital signature applied to the electronic records from the voting machines is only useful if it is verified before the tabulation center accepts electronic records.

*Source:*

*Impact:*

→ **5.2.2-C** Electronic records poll opening certificate requirement

Upon opening the polls, the voting machine ***SHALL*** produce an Election Public Key Certificate to include the following information:

- Date and time at which the polls opened initially for the election.
- Serial number and other identifying information of the voting system and cryptographic module.
- Precinct and list of ballot styles supported, including hashes of each ballot definition.
- Hardware-enforced counter, which is immediately incremented upon being used.
- Current version of software on the voting system.
- Election Signature Key key.
- Digital signature with Device Signature Key of the cryptographic module.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

This record exists to strongly bind together the ESK, a per-election key, an initial poll opening time and date, a precinct and set of ballots, and a voting system. The record can be used along with associated records to make sure that each voting system that is supposed to send in some votes get to send in exactly one set of ballots, and that no additional sets of ballots are supported. The record also makes it possible to determine that all the electronic records originated from this voting system. The record can be used to verify that the voting system had the correct set of ballot definitions and styles loaded at the time of the election, and the correct version of software. The inclusion of the counter in this certificate makes it possible to detect any spurious generations of per-election keys, such as might have occurred in the past to attempt to alter another election total. This record is used in combination with others to resist a number of attacks, including attempts to insert additional or altered electronic records into the total. See the Cryptography chapter for more details on the requirements for generating and destroying per-election keys.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **5.2.2-C.1** Electronic records poll opening certificate handling requirement

The voting machine ***SHALL*** handle the Election

Signature Certificate according to the following:

- The certificate is transmitted to the tabulation center with the other electronic records.
- It is stored in the election archive, if available.
- It is written to the voting systems event log.
- If a printer is available, it should be printed in a format that allows it to be scanned back into a valid certificate.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **5.2.2-D** Electronic records poll closing records requirement

Upon closing the polls, the voting machine ***SHALL*** produce a report including the following records:

- Election Signature Key and certificate.
- Time and date when the report was generated.
- Sufficient information to allow counting of the votes. This may be vote counts or ballot images, depending on the system.
- A digital signature from the Election Signature Key.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

This record exists to carry the results from the voting system back to the tabulation center, where it can be combined with the results from other voting systems to determine a winner in each race. The tabulation center can verify the signatures in both the per-election key and certificate and in this record before accepting the data into the total. This record is sufficient to support random recount audits of paper records. It can be used to verify a correct result from a system under parallel testing. This record can be used to randomly check electronic totals, when the final result is given broken out by voting system or scanner. By requiring inclusion of the per-election key and certificate, and by signing the whole record, this electronic record format entirely eliminates attacks that rely on tampering with electronic records in transit. Because the per-election key is destroyed soon after writing this

record, there is no way for an attacker to backdate electronic records when an audit or recount is called for. See the Cryptography chapter for more details on the requirements for generating and destroying Election Signature Keys.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **5.2.2-D.1** Electronic records poll closing records handling requirement

The voting machine ***SHALL*** handle the poll closing records according to the following:

- The records are transmitted to the tabulation center with the other electronic records.
- It is stored in the election archive, if available.
- Its signature is stored in the voting systems event log.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **5.2.2-E** Electronic records summary count record requirement

The voting machine ***SHALL*** produce a summary count report including the following:

- Election Signature Key and certificate
- Time and date at poll closing
- List of ballot styles voted and for each style, how many ballots are stored.
- Number of spoiled ballots, if any.
- Ballots not yet properly counted (i.e. provisional ballots)
- For each ballot question:
  - Number of ballots voted that included the question
  - Number of votes for each candidate for this question
  - Number of votes for some write-in for this question
- Digital signature

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

The summary count record gives a summary of the results of voting on this voting system of scanner, the result of the election that would result if only this voting system's votes were counted. This summary is preliminary because provisional ballots and write-in votes may be included in the records stored by the voting system, but may not yet be able to be counted. This record can be printed (with digital signatures encoded into printable characters) and can also be stored electronically. This record exists to allow checking of the final totals, based on their agreement with local totals from the voting systems, without the need to entirely trust the computers and workers at the tabulation center. For voting systems that send a set of ballot images to the tabulation centers, this summary should in general be safe to publish, whereas the set of ballot images is not safe to publish. This record is not complete because provisional and write-in ballots require human intervention to count. However, the set of all such records will yield an approximate election result. This record does not provide much security benefit when used with instant runoff voting (IRV).

This record is sufficient to support random recount audits of paper records. It can be used to verify a correct result from a system under parallel testing. This record can be used to randomly check electronic totals, when the final results are given broken out by voting system or scanner. It can be published for each voting system, along with corrected final totals for each precinct and for absentee ballots, to show how the final election outcomes were computed.

When published for each voting system and included in a summary of final election outcomes, this record blocks the class of attacks that involves tampering with the tabulation center computer. It provides an auditing process in which the records can be used by election official and observers to catch any misbehavior in the tabulation center with high probability.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **5.2.2-E.1** Electronic records summary count record handling requirement

The voting machine ***SHALL*** handle the summary count record according to the following:

- The record is transmitted to the tabulation center with the other electronic records.
- It is stored in the election archive, if available.
- It is stored in the voting systems event log.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **5.2.2-F** Collection of cast vote records requirement

The voting machine ***SHALL*** produce a collection of cast votes recorded, including the following election:

- Election Signature Key and certificate
- Time and date at poll closing
- The set of cast vote records recorded from this election by this voting machine, in randomized order. For each vote, this includes:
  - Precinct, election district, and ballot style
  - The vote as recorded on each ballot question
  - Undervotes as recorded on each ballot question
  - Write-in information as recorded on each ballot question
  - Information specifying whether the ballot is provisional, and providing identifying information if so.
- Digital signature

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The collection of cast vote records contains the full set of votes that were recorded by the machine. This is required to support instant runoff voting, and is extremely useful in investigating possible problems in an election.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **5.2.2-F.1** Collection of cast votes handling requirement

The voting machine ***SHALL*** handle the collection of cast votes record according to the following:

- The record is transmitted to the tabulation center with the other electronic records.
- It is stored in the election archive, if available.
- It is stored in the voting systems event log.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **5.2.2-G** Electronic records event log report requirement

The voting machine ***SHALL*** produce an event log report with the following information:

- Election Signature Key and certificate
- Event log data from poll opening until poll close
- Signature

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Event log formats and requirements are specified in the System Integrity Management and System Event Logging chapters. The event log contains a listing of security-relevant events (such as installation of new software) and procedure-relevant events (such as the opening of the polls). The purpose of event logs is to leave a permanent trail of anomalies and misbehavior, so that these may be discovered later. Event logs must not include sufficient information to reconstruct the order of votes or to determine how any voter voted. The event logs support detection of problems by both manual and automated scanning. They also support investigation of any problems discovered. Event logs cannot rule out software tampering and related attacks, but make them more difficult to carry out without detection. Event logs can detect failure to follow procedures and even some low-tech attacks by pollworkers.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **5.2.2-G.1** Electronic records event log record handling requirement

The voting machine ***SHALL*** handle the event log record according to the following:

- The record is transmitted to the tabulation center with the other electronic records.
- It is retained on the voting system.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The tabulation center can verify that the event log record is received and that the digital signature and per election key and certificate are valid.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

## 5.2.3 Requirements on Records Produced by Tabulation Center Computers

The following requirements apply to the final election tally produced by the tabulation center computers and released to the public.

→ **5.2.3-A** Final election tally report requirement

The tabulation center voting machine ***SHALL*** produce a final election tally report.

The report ***SHALL*** contain the following information:

- The election totals
- The total number of ballots, and ballots of each style, precinct, and election distriict
- For each polling place:
  - The serial numbers and public keys for each voting system used in the precinct. In the case of older equipment that doesn't support the use of per-election public keys, the serial number ***SHALL*** be included.
  - The Summary Count Record for each voting system used in the precinct. In the case of older equipment that doesn't support the Summary Count Record, the same summary information is included, but without the digital signature, timestamp, and per-election key and certificate.
  - Any adjustments done to the precinct or polling place counts due to provisional ballots, write-ins, and other special cases.
- A digital signature

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The tabulation center record exists to allow checking of the final totals, based on their agreement with local totals from the voting systems, without the need to entirely trust the computers and workers at the tabulation center. The goal is to provide cryptographic support for a process that is currently done in a manual, procedural way, which may be subject to undetected error or tampering. This is the best record to use to support random recount audits of paper ballots and VVPAT records, since it includes resolutions for the special cases at the polling place level to preserve ballot secrecy for provisional ballots. This record can be published for each voting system, along with corrected final totals for each precinct and for absentee ballots, to show how the final election outcomes were computed. Challenges to handling of special cases per precinct can be made and checked base on this record. This report blocks most misbehavior at the tabulation center.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **5.2.3-B** Election tally audit report requirement

The tabulation center voting machine ***SHALL*** be capable of producing a report from the election tally which supports auditing requirements.

The report ***SHALL*** contain the following information:

- The election totals
- The total number of ballots, and ballots of each style, precinct, and election distriict
- For each polling place:
  - The serial numbers and public keys for each voting machine or scanner used in the polling place. In the case of older equipment that doesn't support the use of per-election public keys, the serial number ***SHALL*** be included.
  - The final summary of votes from that voting machine or scanner, including resolved write-in votes, and indications of provisional ballots that should and should not be included in the totals.
- A digital signature

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

This report supports hand-auditing of paper records against the final totals, and includes the resolution of provisional and write-in votes. This report could leak information about how some provisional ballots voted, but also provides more complete information for auditors to check against voter-verifiable paper records.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

# Chapter 6: Voter Verified Paper Records Requirements

[[

NOTES:

I know the formatting isn't quite right. We have some contractors who can help with this, so it will be more polished before the end of the voting.

We still don't have very many new PCOS and BMD requirements; these are almost all covered by the general VVPR requirements.

Comments I make inside double-square brackets will be removed before we ship the final version; this is a way for me to ask questions or make comments that are distinct from the text.

A fair bit of the machine-readable stuff and readback/accessibility stuff is still in flux; I did my best to reflect the consensus as best I could work it out, and to fill in blanks with my own best understanding of the issues. But there may be some disagreement about this stuff.

Known terminology issue: I often say "CVR" where I mean "summary of CVR." I am not sure if this is important to fix or not.

]]

## 6.1 Introduction/Scope

This section contains informative profiles and requirements for voting systems that produce and use Voter Verified Paper Records (VVPR). These include two broad categories:

- DRE+VVPAT voting systems couple an electronic voting machine with a printer. The voter makes selections on the voting machine, but is given the opportunity to review and verify choices on a paper record. The paper record may be a continuous roll or cut sheets.
- PCOS voting systems use paper ballots which are human-readable, and may be marked by either hand or machine, along with an electronic scanner which checks the ballot for problems such as under- and overvotes, and also records the votes.

In both categories of system, the paper records are available to the voter to review and verify, and these records are retained for later auditing or recounts as needed.

Voter verified paper records exist to provide a separate record of the voter's choices, which can be used to verify the correctness of the electronic record produced by the voting equipment. VVPR must support:

- Voter verification – voters must be able to review the records, and their presence in the final set of paper records must indicate that the voters had the chance to review and accept or reject them.
- Auditing – election officials must be able to use the paper records to statistically verify the correctness of reported electronic totals.
- Recounting – election officials must be able to use the paper records to reconstruct the full set of totals from the election.

In addition, VVPR must support other requirements of the voting system, such as usability and reliability. This chapter covers only security requirements of VVPR, requirements on usability of VVPR appear in [[reference]], while requirements on reliability appear in [[reference]].

### 6.1.1 Voter Verification and Auditing

The normal process of voting offers the voter an opportunity to *verify* a paper representation of his vote. This paper record is then stored and may be used to audit the results of an election.

The combination of verification and auditing provides a powerful defense against software attacks on the voting machine; so long as the paper records are not altered, a compromised VVPAT or ballot marking device voting machine attempting to change a voter's ballot must either:

- Print the changed ballot contents on the paper record, thus risking the voter noticing the change during verification.
- Print the ballot contents on the paper record as the voter intends, but store different ballot contents electronically, thus risking an audit detecting the change.

Similarly, a compromised PCOS scanner may change the reported totals only by altering the electronic totals it reports, thus risking detection during the audit.

Security requirements on VVPR are driven mainly by the need to support voter verification and auditing.

## 6.2 General Requirements on Voter Verified Paper Records

The following requirements apply to all VVPR used by any voting system, including VVPAT and PCOS systems.

→ **6.2-A** Human readable information sufficient for unambiguous interpretation of cast vote

All VVPR ***SHALL*** contain a human-readable summary of the cast vote. In addition, all VVPR ***SHALL*** contain enough information to completely interpret the summary of the cast vote. This includes:

- Polling place
- Precinct and/or election district
- Ballot style
- Date of election
- Complete summary of voter's choices

*Applies to:* *VVPAT, Ballot Marker, PCOS*

*Test Reference:*

D I S C U S S I O N

All VVPR contain some human-readable content. In addition, some VVPR may use machine-readable content to make counting or recounting more efficient. For example, PCOS systems place a human-readable representation of the votes beside a machine-readable set of ovals to be marked by a human or a machine.

The human-readable content of the VVPR must contain all information needed to interpret the cast vote. This is necessary to ensure that hand-audits and recounts can be done using only the human-readable parts of the paper records.

*Source:* *Auditing Chapter, NIST Threats Workshop*

*Impact:*

→ **6.2-B** Machine readability of paper record

The paper record should be created in a manner that is machine readable. The following sub-requirements apply to machine-readable representations on VVPR.

*Applies to:* *VVPAT, Ballot Marker, PCOS*

*Test Reference:*

D I S C U S S I O N

Machine-readable content on the VVPR can make counting paper records more efficient, and this should be done. Machine-readable content also introduces some security issues, however, which are addressed in the sub-requirements below.

*Source:* *Auditing Chapter, NIST Threats Workshop*

*Impact:*

↳ **6.2-B.1** Auditability of Machine Representations

The voting system ***SHALL*** include supporting software, hardware, and documentation of procedures to verify the agreement of human-readable and machine representations when they are used in recounts.

*Applies to:* *VVPAT, Ballot Marker, PCOS*

*Test Reference:*

D I S C U S S I O N

Machine readable encodings of the CVR cannot be used to recount the election without auditing. This requirement says that the auditing steps must be supported and documented. [[I need to write the auditing requirements up for the auditing chapter.]]

*Source:* *Auditing Chapter, STS Discussions*

*Impact:*

↳ **6.2-B.2** Machine readable part contains same information as human readable part

The machine-readable part of the paper record ***SHALL*** contain the entirety of the human-readable information on the paper record.

*Applies to:* *VVPAT, Ballot Marker, PCOS*

*Test Reference:*

D I S C U S S I O N

The machine-readable part of the paper record must permit the reconstruction of the human-readable part of the record.

*Source:* *STS Discussions*

*Impact:*

↳ **6.2-B.3** Machine-readable contents may include error correction/detection information

The machine-readable part of the paper ballot may also contain information intended to ensure the correct decoding of the information stored within, including:

- Checksums
- Error correcting codes
- Digital signatures

- Message Authentication Codes

*Applies to:* *VVPAT, Ballot Marker, PCOS*

*Test Reference:*

D I S C U S S I O N

Error correction/detection information is used to protect digital data from error or tampering. This information would not be meaningful to a human, so there is no reason to demand that it also appear in the human-readable part of the paper record.

*Source:* *STS Discussions*

*Impact:*

↳ **6.2-B.4** Machine-readable ballot identifiers

- The machine-readable part of the paper ballot may also contain a unique identifier
- If this feature is provided, the equipment ***SHALL*** allow it to be turned off.

*Applies to:* *VVPAT, Ballot Marker, PCOS*

*Test Reference:*

D I S C U S S I O N

Some states require the ability to link each paper record to a corresponding electronic record, which requires putting some kind of unique record identifier on the paper record. Certain vote-buying attacks are made much easier if this record identifier is visible to the voter, so it is valuable to permit it to be hidden in machine-readable content. Other states forbid the use of unique record identifiers on paper records, so it must be possible to turn this feature off.

[[Is there a better way to structure this requirement, so I'm not doing the may->**SHALL** thing?]]

*Source:* *STS Discussion, VVSG2005*

↳ **6.2-B.5** Public format

Any non-human readable information on the ballot ***SHALL*** be printed in a fully-disclosed, industry-standard public format.

*Applies to:* *VVPAT, Ballot Marker, PCOS*

*Test Reference:*

DISCUSSION

Meaningful auditing of the contents of the machine-readable parts of the paper requires the ability to use independent software and hardware to read those parts of the paper. This requires a fully-public format for the machine-readable data.

*Source:* *STS Discussion, VVSG2005, NIST Threat Analysis Workshop, Brennan Center Report*

*Impact:*

# 6.3 VVPAT Systems

## 6.3.1 Introduction and Definitions

This section contains requirements for the basic components and operation of voting devices of the profile VVPAT (Voter Verified Paper Audit Trail). Voting devices of this profile typically consist of a DRE with an attached printer and a capability for displaying printed paper records to the voter and for storing the paper records. In this configuration, prior to casting the ballot on the DRE, the voter must have the ability to verify his or her selection on the paper record in a private and independent manner. After a paper ballot is produced, but before the voter's ballot is recorded, the voter must have the opportunity to accept or reject the contents of the ballot. If a voter does not accept the contents of the paper ballot, the voter must be permitted to recast the ballot. There must be the ability to distinguish a voter's non-accepted ballot from his/her accepted ballot. The paper ballot must be useful in audits of the electronic records and in recounts and capable of being used as the official ballot in tabulations.

**Protocol of Operation**

The basic protocol of use for a VVPAT system involves making ballot choices on a DRE first, and then, before making the ballot choices final, comparing those choices to those printed on a paper record. The basic protocol consists of the following steps:

1. The voter causes the display of a summary of her ballot choices.
2. If the voter is satisfied with the summary, the voter causes the printing of a paper record that contains this same summary.
3. The voter, if she desires, compares the two summaries and is able to do one of the following:
   A. Return to making ballot choices, thereby voiding the paper record.
   B. Make her ballot choices final, thereby accepting the paper record.
   C. If the voter notes a discrepancy between the summaries, i.e., one of the summaries is in error or is not printed properly, the voter is then able to pause the operation of the voting system and, according to local election procedures, request assistance.

This protocol will vary somewhat or may involve additional steps depending upon particular implementations.

## 6.3.2 VVPAT Components and Definitions

→ **6.3.2-A** VVPAT Definition and Components

A VVPAT voting system consists minimally of the following fundamental components:

- A voting machine, on which a voter make selections and prepare to cast a ballot.
- A printer which prints a summary of the voter's ballot selections, and which allows the voter to compare it with the electronic ballot selections.
- A mechanism by which the voter may indicate acceptance or rejection of the printed summary of the CVR.
- Ballot box/cartridge to contain accepted and voided paper cast vote records.
- A paper cast vote record for each electronic cast vote record. The summary record may be printed on a separate sheet for each CVR ("cut-sheet VVPAT") or on a continuous paper roll ("paper-roll VVPAT")

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

A VVPAT profile is essentially a DRE with a capability to print a paper record summary and a capacity for the voter to accept or reject the paper record, with acceptance required for the vote to be cast electronically.

*Source: VVSG2005*

Impact:

## 6.3.3 Requirements on VVPAT Printer/Voting Machine Interactions

→ **6.3.3-A** Minimum Supply Requirement

Printing devices ***SHALL*** contain sufficient supplies of paper and ink to print a minimum of 300 paper records (this may include voided records) of at most NNN lines without reloading or opening equipment covers or enclosures.

*Applies to:* *VVPAT*

*Test Reference:*

D I S C U S S I O N

[[I think we should either:

a. Delete this requirement entirely, or

b. Turn it into a documentation requirement—"the number of lines that can be printed from a full roll **SHALL** be specified in the product documentation" or some such thing.

My reasoning: This is visible to anyone who buys the voting system. I can't see why we know what the right parameters are here better than either the vendor or the election official buying it, who will presumably notice that it requires three changes of paper per election or something.

]]

*Source:*

*Impact:*

→ **6.3.3-B** Printer connection to voting system

The printer ***SHALL*** be physically connected to the voting system via a standard, publicly documented printer port using a standard communication protocol; voters or unauthorized election officials ***SHALL*** not be able to access this connection.

*Applies to:* *VVPAT*

*Test Reference:*

D I S C U S S I O N

Examples would be parallel printer ports and USB ports.

See the Physical security chapter for guidance on how this connection **SHALL** be secured.

*Source:* *Physical Security Chapter*

*Impact:*

→ **6.3.3-C** Printer able to detect errors

The voting machine ***SHALL*** detect printer errors that may prevent paper records from being correctly displayed, printed or stored. These errors ***SHALL*** be communicated to the voting machine:

- Lack of consumables such as paper, ink, and toner
- Paper jams/misfeeds
- Other errors

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

*The requirement to detect errors is expanded on in the sub-requirements, which specify requirements on what to do when the errors are detected.*

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **6.3.3-C.1** VVPAT error handling specific requirements

If a printer error or malfunction is detected, the voting machine ***SHALL***:

- Present a clear indication to the voter and election officials of the malfunction. This must indicate clearly whether the current voter's vote has been cast, discarded, or is waiting to be completed.
- Suspend voting operations till the problem is resolved.
- Allow cancelling of the current voter's CVR by election officials in the case of an unrecoverable error.
- Protect the privacy of the voter to the greatest extent possible while the error is being resolved.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

A printer error can really only happen when the VVPAT is being printed out, which is at the end of the voting process. The main thing that must not happen is for the voting machine to end up in an ambiguous state, where the election officials can't determine whether to issue the voter another ballot or not.

↳ **6.3.3-C.2** VVPAT printer error recovery guidelines in documentation

Vendor documentation ***SHALL*** include procedures to recover from common printer errors and faults, and also how to cancel the vote suspended during handling of an error from which they cannot recover.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

If the printer just irrecoverably locks up, jams, catches fire, whatever, the vote needs to be able to be canceled, so the voter can cast his vote again on another machine. Alternatively, it would be okay to store the vote as is, if the vote is complete.

↳ **6.3.3-C.3** VVPAT general recovery from misuse or voter error

Voter error or misbehavior ***SHALL*** not be capable of causing a discrepancy between the paper and electronic CVRs.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

This prevents an error or malicious act by a voter from creating the incorrect appearance that election fraud has been attempted.

## 6.3.4 Protocol of Operation Requirements

➞ **6.3.4-A** VVPAT prints and displays a paper record

The voting system ***SHALL*** provide capabilities for the voter to print a paper record that minimally contains a summary of all ballot selections and races and for the voter to view and compare with a summary of the voter's electronic ballot selections prior to the voter making her ballot selections final.

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

➞ **6.3.4-B** Ease of record comparison

The format and presentation of the paper and electronic summaries of ballot selections ***SHALL*** be designed to facilitate the voter's rapid and accurate comparison.

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

This requirement may already be covered by HFP.

→ **6.3.4-C** VVPAT Vote Acceptance Process Requirements

When a voter indicates that the vote is to be accepted, the voting machine ***SHALL***:

- Immediately print an unambiguous indication that the vote has been accepted, in view of the voter.
- Electronically store the CVR as a cast vote.
- After a short delay, deposit the paper record of the voter's CVR into the ballot box or other receptacle.

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Immediately upon acceptance by the voter, the voting machine commits to accepting the paper record, in the voter's sight, and stores the electronic record. This defends against the threat that the voting machine might indicate a rejected vote on the paper record when the voter cannot observe it. The paper summary must be placed into the receptacle before the next voter arrives, to ensure the previous voter's privacy.

→ **6.3.4-D** VVPAT Vote Rejection Process Requirements

When a voter indicates that the vote is to be rejected, the voting machine ***SHALL***:

- Immediately print an unambiguous indication that the vote has been rejected, in view of the voter.
- Electronically store the CVR as a rejected paper record.
- After a short delay, deposit the paper record of the voter's CVR into the ballot box or other receptacle
- Recover from the rejected paper record as described in the sub-requirements.

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Immediately upon rejection by the voter, the voting machine commits to rejecting the paper record, in the voter's sight, and stores the electronic record. This defends against the threat that the voting machine might indicate an accepted vote on the paper record when the voter cannot observe it.

↳ **6.3.4-D.1** VVPAT Recovery from Rejected Vote Without Election Official Intervention

The voting machine ***SHALL*** have the capacity to be configured to allow the voter to simply vote again, when the paper summary is rejected, up to some configurable maximum number of rejected paper records.

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

[[We need to make sure the voting machine can support limits on how many times the voter can reject a paper record, and also on how many rejected votes a single DRE gets before some kind of human intervention is required. I think this may need an extra requirement.]]

↳ **6.3.4-D.2** VVPAT Recovery from Rejected Vote With Election Official Intervention

The voting machine ***SHALL*** have the capacity to be configured to require election official intervention to permit voting after a rejected paper record summary. In this case, upon rejection of a paper record, the voting machine ***SHALL***:

- Clearly display that a paper summary has been rejected.
- Suspend normal operations until unlocked by some authorization of an election official.

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

[[Is this a "**SHALL** have the capacity to" or a "may"?

I think this behavior is specified by state law.]]

## 6.3.5 Paper Human-Readable CVR Contents

*The following requirements apply to the human-readable cast vote records (CVRs) on paper ballots.*

→ **6.3.5-A** Paper-Roll VVPAT Required Human-Readable Content Per Roll

In paper-roll VVPAT systems, the voting machine ***SHALL*** mark the paper roll with the following information:

- Voting machine which produced the record.
- Election in which record was produced.
- Precinct or polling place in which record was produced.
- If multiple paper rolls were produced during this election on this machine, the number of the paper roll (e.g., Roll #2).
- A final summary line specifying how many total CVRs appear on the roll, and how many accepted CVRs appear on the roll.

*Applies to:* *Paper-roll VVPAT*

*Test Reference:*

D I S C U S S I O N

In order for recounts and audits to work, the auditor must be able to determine which electronic record corresponds to the paper roll or rolls. The above information ensures that the auditor will be able to find the right electronic record, and also supports finding all necessary paper rolls.

This requirement requires the voting machine to either detect the amount of paper remaining on the roll, or to compute how much paper is left.

*Source:* *Auditing Chapter, Electronic Records Chapter, VVSG2005, Brennan Center Report, NIST Voting Threats Workshop, STS Discussions, ESI Report*

*Impact:*

→ **6.3.5-B** Paper Roll VVPAT Requirements Per CVR

In paper-roll VVPAT systems, each Cast Vote Record (CVR) ***SHALL*** include the following information:

- Identification of the ballot being voted, including precinct or election district, party (for primaries), etc.
- Type of voting (e.g., provisional, early, etc.)
- For each ballot question:
- Name of the ballot question (e.g., “Governor”)
- Any notes needed for interpretation, such as “select 2”
- If the question was undervoted, a clear indication of this fact.
- If this is a write-in vote, a clear indication of this fact.
- The vote as it will be cast.
- An unambiguous indication of whether the ballot has been accepted or rejected by the voter.

*Applies to:* *Paper-roll VVPAT*

*Test Reference:*

D I S C U S S I O N

The paper roll and the cast vote record, together, must give an auditor all information needed to do a meaningful hand-audit or recount. The contents in this

requirement ensure that the human-readable parts of the paper rolls are sufficient to recount the election, and to audit the machine totals.

*Source:* *Auditing Chapter, Electronic Records Chapter, VVSG2005, Brennan Center Report, NIST Voting Threats Workshop, STS Discussions, ESI Report*

*Impact:*

→ **6.3.5-C** Paper Roll VVPAT CVRs on a single roll

In paper-roll VVPAT systems, a single CVR ***SHALL*** always be contained on a single roll. A CVR ***SHALL*** not be split across rolls.

*Applies to:* *Paper-roll VVPAT*

*Test Reference:*

D I S C U S S I O N

Allowing a single CVR to split across rolls would make auditing much harder, and would also make it very difficult for the voter to fully verify the printed vote summary.

This requires that the printer either detect the end of the paper roll in time to avoid splitting CVRs, or calculate the remaining paper roll length.

*Source:* *Auditing Chapter, Electronic Records Chapter, VVSG2005, Brennan Center Report, NIST Voting Threats Workshop, STS Discussions, ESI Report*

*Impact:*

→ **6.3.5-D** Cut Sheet VVPAT Content Requirements Per CVR

In paper-roll VVPAT systems, each Cast Vote Record (CVR) ***SHALL*** include the following information:

- Voting machine which produced the record.
- Election in which record was produced.
- Precinct or polling place in which record was produced.
- Identification of the ballot being voted, including precinct or election district, party (for primaries), etc.
- Type of voting (e.g., provisional, early, etc.)
- For each ballot question:
  - Name of the ballot question (e.g., “Governor”)
  - Any notes needed for interpretation, such as “select 2”
  - If the question was undervoted, a clear indication of this fact.
  - If this is a write-in vote, a clear indication of this fact.
  - The vote as it will be cast.
- An unambiguous indication of whether the ballot has been accepted or rejected by the voter.

*Applies to:* *Cut-sheet VVPAT*

*Test Reference:*

DISCUSSION

The set of detached paper records must give an auditor all information needed to do a meaningful hand-audit or recount.

Each ballot summary must include all information needed to identify which machine produced it, which type of ballot it is (ballot style, precinct, election district, etc.). All this information is necessary to support the hand-audit. Unambiguous rejection and acceptance markings address the threat that the DRE might attempt to reject or accept ballot summaries without the voter's approval.

*Source:* *Auditing Chapter, Electronic Records Chapter, VVSG2005, Brennan Center Report, NIST Voting Threats Workshop, STS Discussions, ESI Report*

*Impact:*

→ **6.3.5-E** Cut-Sheet VVPAT CVRs on a single sheet

In cut-sheet VVPAT systems, a single CVR ***SHALL*** always be contained on a single piece of paper. A CVR ***SHALL*** not be split across pieces of paper.

*Applies to:* *VVPAT*

*Test Reference:*

DISCUSSION

Allowing a single CVR to split across rolls would make auditing much harder, and would also make it very difficult for the voter to fully verify the printed vote summary.

[[

I need comments on this. Is this okay, even though it rules out using normal, off the shelf printers to make VVPAT systems? An alternative is to require that the cut sheets for each CVR are marked to indicate how many pages are in the summary, for example, "Page 1 of 4".

This prevents the use of fixed-size sheets of paper; if this requirement exists, the cut-sheet VVPAT system must be able to cut off paper from a roll.

Eliminating this requirement allows normal printers/paper, but makes it impossible to review the CVR all at once. However, it might make sense to eliminate this requirement, to allow more engineering freedom for vendors.]]

*Source:* *Auditing Chapter, Electronic Records Chapter, VVSG2005, Brennan Center Report, NIST Voting Threats Workshop, STS Discussions, ESI Report*

*Impact:*

## 6.3.6 Requirements on Supporting Linking Electronic and Paper CVRs

VVPAT systems are required to support the linking of electronic and paper records, but must also be able to disable this linkage.

→ **6.3.6-A** Identification of CVR correspondence

The voting system ***SHALL*** provide a capability for auditors to identify from an electronic CVR its corresponding paper CVR and from a paper CVR its corresponding electronic CVR. This correspondence ***SHALL*** exist for every electronic/paper CVR pair produced by the voting system for the election, regardless of the balloting style.

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

All VVPAT systems are required to support the ability to do this as an option.

[[This is here because some states require this ability. Nobody seems to have really good procedures for doing the auditing implied by this mechanism in a software-independent way, and while it's possible to do such auditing in a strong way, it's not easy.]]

*Source:*

*Impact:*

→ **6.3.6-B** Ability to disable CVR correspondence

This capability ***SHALL*** be able to be disabled as necessary to comply with election law.

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

This requirement is needed to satisfy the law in some states, which explicitly forbids such linkage information.

→ **6.3.6-C** CVR correspondence identification hidden from voter

Any information on the paper ballot which identifies the corresponding electronic record should not be viewable by the voter.

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Ideally, the correspondence information would be hidden from the voter; this makes certain kinds of vote-buying attacks more difficult. However, those attacks can also be addressed with procedures, and non-human-readable correspondence information makes it very difficult to do the audit of correspondence of records in a software-independent way. Further, some states do not allow any non-human-readable information on the paper records.

→ **6.3.6-D** CVR correspondence identification viewable to auditors

The voting system vendor ***SHALL*** include a capability for auditors to verify the correspondence between the electronic and paper CVR pairs.

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

[[And it needs to be open, not proprietary, but that's covered in the requirements on machine-readability.]]

→ **6.3.6-E** CVR correspondence identification included in digital signatures

If the voting system calculates a digital signature on the contents of its electronic CVRs, and includes CVR correspondence information in the CVR, the CVR correspondence identification ***SHALL*** be included in the digital signature.

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

This requirement assumes that electronic CVRs will have the capability of being digitally signed.

## 6.3.7 Paper-Roll VVPAT Privacy and Audit-Support Requirements

VVPAT voting systems using paper rolls introduce a voter privacy issue, because anyone who observes the sequence of voters who use a given voting machine can then use the paper roll to determine the vote of each voter.

The following requirements address this threat.

→ **6.3.7-A** VVPAT paper roll CVRs secured immediately after vote cast.

Paper-roll VVPAT systems ***SHALL*** store the part of the paper roll containing CVRs in a secure, opaque container, immediately after they are verified.

*Applies to:* *VVPAT*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

The part of the paper roll which contains the CVRs for previous voters represents a privacy risk. Voting systems that comply with this requirement decrease this risk.

*Source:*

*Impact:*

→ **6.3.7-B** VVPAT paper roll privacy during printer errors

Procedures for recovery from printer errors on paper-roll VVPAT systems ***SHALL*** not expose the contents of previously-cast CVRs.

*Applies to:* *VVPAT*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

Printer errors are too common to permit them to allow the loss of someone's privacy. This is related to the requirement for immediately storing the CVRs inside a secure, opaque container.

*Source:*

*Impact:*

→ **6.3.7-C** VVPAT paper rolls with cast vote records support tamper-seals and locks

Paper-roll VVPAT systems ***SHALL*** be designed so that when the rolls are removed from the voting machine:

- All paper containing CVRs are contained inside the secure, opaque container.
- The container may be tamper-sealed and locked.
- The container may be labeled with the machine serial number, precinct, and other identifying information to support audits and recounts.

*Applies to:* *VVPAT*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

DISCUSSION

Paper-roll VVPAT equipment must support good procedures to protect the voters' privacy. The supported procedure in this case is immediately locking and tamper-sealing each VVPAT container upon removing it from the voting machine. This is consistent with the goal of having the paper rolls with CVRs on them treated like paper ballots, stored in a locked and sealed box.

[[Somewhere (physical security, VSS2002?) there must be a good list of the requirements here. The goal is that once the paper rolls have CVRs on them, they're never handled by election officials except inside this sealed box.]]

*Source:* *NIST Voting Threats Workshop, STS Discussion*

*Impact:*

→ **6.3.7-D** Paper roll VVPAT voting systems document privacy-ensuring procedures.

Paper-roll VVPAT systems ***SHALL*** provide documentation describing necessary procedures for handling the paper rolls in a way that preserves voter privacy.

*Applies to:* *VVPAT*

*Test Reference:*

DISCUSSION

Along with a secure, opaque container designed to accomodate tamper-seals and a lock, the voting system needs to document what must be done to protect voter privacy with the paper rolls. The goal of this requirement is to ensure that the election officials are given guidance on exactly what must be done to protect the privacy of voters. This documentation will be reviewed by the labs.

*Source:*

*Impact:*

➞ **6.3.7-E** Mechanism to view spooled records

If a continuous paper spool is used to store paper CVRs, the vendor ***SHALL*** provide a mechanism for an auditor to unspool the paper, view each CVR in its entirety, and then respool the paper, without modifying the paper in any way or causing the paper to become electrically charged.

*Applies to:* *VVPAT*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

This requirement comes directly from the issues raised in the ESI report.

# 6.4 PCOS Systems

[[This section is very thin, because we don't have a lot of new requirements for PCOS—it's old technology, and people already know how to build and use these systems. The VVPR requirements here are pretty straightforward. Comments much appreciated, and much needed!

I expect there to be a lot of overlap with CRT material.

]]

## 6.4.1 Introduction and Scope

A PCOS voting system involves paper ballots which are marked in a way that is both human- and machine-readable. The marks may be put on the ballots by hand, or by a machine called a ballot marking device (BMD).

The following sections specify VVPR requirements applying to optical scan ballots, as required for supporting audit and recount.

## 6.4.2 Scanner Requirements

➞ **6.4.2-A** Scanner Optional Batching Support

The PCOS scanner should support breaking the set of paper ballots into batches.

*Applies to:* *PCOS*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

This makes auditing much easier. Subrequirements fill in the details.

*Source:*

*Impact:*

↳ **6.4.2-A.1** Batches get separate electronic records

If the scanner breaks the set of paper records into batches, it ***SHALL*** generate a separate electronic summary report (as described in the Electronic Records chapter) for each batch. The final election report ***SHALL*** support breakdowns by batch for each PCOS scanner.

*Applies to:* *PCOS*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

*Source:*

*Impact:* *Auditing, Electronic Records*

↳ **6.4.2-A.2** Batches separated for auditor convenience

If the scanner breaks the set of paper records into batches, the paper records ***SHALL*** be separated in one of three ways:

- The scanner may physically sort the records into different batches based on some preprinted marking on the ballot.
- The scanner may physically sort the records into different batches based on a count of paper records, so that every N records, a new batch is started.
- The scanner may print something on each record indicating its batch.

*Applies to:* *PCOS*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

*Source:*

*Impact:* *Auditing, Electronic Records*

↳ **6.4.2-A.3** Minimum size of batches

If the scanner breaks the set of paper records into batches, it ***SHALL*** ensure that no batch summarized in an electronic summary record contains fewer

than 50 paper records. This may require combining batches broken out by the PCOS scanner.

*Applies to:* *PCOS*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

*The specific number of 50 is arbitrary, but the size of the batch needs to be small enough that auditing by hand is easy, but large enough that voter privacy is not compromised by the publication of totals of a batch.*

*Source:*

*Impact:* *Auditing, Electronic Records*

→ **6.4.2-B** Scanner Optional Marking

The PCOS scanner may add markings to each paper ballot, including:

- Unique record identifiers to allow individual matching of paper and electronic CVRs.
- Digital signatures
- Batch information

*Applies to:* *PCOS*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

[[This was from John's original text. Not sure if it's worth putting a MAY requirement in the standard, or even if we're doing this. ]]

*Source:*

*Impact:*

# Chapter 7: Cryptography Requirements

## 7.1 Introduction/Scope

This section establishes general cryptography requirements for voting systems, specifies that signatures for protecting electronic voting records used in audits be generated in an embedded hardware signature module, and specifies the requirements for that module. These requirements include a key management scheme for the signature keys used by the signature cryptographic module, and requirements to help ensure that the signatures are reliable even if the voting device software has bugs or is tampered with.

Cryptography typically serves several purposes in voting systems. They include:

- Confidentiality: where necessary the confidentiality of voting records can be provided by encryption;
- Authentication: data and programs can be authenticated by digital signatures or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the voting systems, while voting systems apply digital signatures to authenticate the critical audit data that they output.
- Random number generation: random numbers are used for a variety of purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.

This section establishes general technical requirements for the cryptographic functionality of voting systems, and some more specific requirements that certain cryptographic functions (primarily digital signatures and key management for digital signatures) be performed in a protected cryptographic module that is isolated from the voting system software, so that it is unlikely that the keys will be revealed or the cryptographic functionality compromised, even in the presence of a bug or malicious code in the other parts of the voting system and even if an adversary (possibly a corrupt insider) gains physical access to or control of the voting system for a period of time. The purpose of the signatures is to authenticate electronic election audit records.

## 7.1.1 General Cryptographic Implementation

→ **7.1.1-A** Cryptographic Module Validation

All cryptographic functionality in voting systems subject to this guideline ***SHALL*** be implemented in a FIPS 140-x validated cryptographic module operating in FIPS mode.

*Applies to:* *All voting system devices that perform cryptographic operations*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

The current version of FIPS 140 and information about the NIST Cryptographic Module Verification Program are available at: http://csrc.nist.gov/cryptval/. Note that a voting device may use more than one crypto module, and quite commonly will use a "software" module for some functions, and a "hardware" module for other functions.

*Source:* *Click here to add the Source*

*Impact:* *Use of validated cryptographic modules ensures that the cryptographic algorithms used are secure and their correct implementation has been validated. Moreover the security module security requirements have been validated to a specified security level.*

→ **7.1.1-B** Cryptographic Strength

Voting devices ***SHALL*** employ NIST approved algorithms with a security strength of at least 112-bits to protect sensitive voting information and audit records. Message Authentication Codes of 96-bits are conventional in standardized secure communications protocols, and acceptable to protect voting records and systems, however the key used with such MACs ***SHALL*** also a security strength of at least 112 bits.

*Applies to:* *Cryptographic operations used to protect (encrypt or authenticate) voting records. This is not intended to forbid all incidental use of non-approved algorithms by OS software or standardized network security protocols.*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

As of February 2006 NIST specifies the security strength of algorithms in SP 800-57, Part 1 <http://csrc.nist.gov/publications/nistpubs/index.html>. This NIST recommendation will be revised or updated as new algorithms are added, and if

cryptographic analysis indicates that some algorithms are weaker than presently believed. The security strengths of SP 800-57 are based on estimates of the amount of computation required to successfully attack the particular algorithm.

*Source:* *Click here to add the Source*

*Impact:* *The specified strength should be sufficient for several decades.*

## 7.1.2 Digital Signature Generation for Audit Records

The purpose of signing election audit records is to authenticate them and prevent their subsequent alteration. A separate hardware *Signature Module (SM)* protects the signature keys and the signature process should the election system software be compromised. The module is "embedded in" (permanently attached to) the voting device to make it difficult to substitute another module.

This guideline does not require that the SM implement all of the cryptographic functionality of the voting device (although the SM might do so), nor does it require that the SM process the signed message directly; it is conventional and acceptable for a host computer system to provide a message digest generated from the message to be signed by a cryptographic hash function and the signature cryptographic module conventionally signs that; standardized digital signature algorithms all apply the private signature key to a message digest rather than the message itself.

The SM is required only in those devices that create electronic audit records, and only for the purpose of creating the audit records. Signature verification and other cryptographic functions need not be implemented in hardware.

→ **7.1.2-A** Audit Record Digital Signature Generation Requirements

Digital signatures that protect election audit records ***SHALL*** be generated in an embedded hardware Signature Module (SM).

*Applies to:* *The generation of those digital signatures that protect or are a part of voting device audit records*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The use of an embedded hardware module for the generation of audit records protects the signature keys and helps to protect the integrity of those records even if the general voting device software is compromised.

*Source:* *Click here to add the Source*

*Impact:* *It is more difficult to create a spurious audit record.*

→ **7.1.2-B** Signature Module (SM)

Voting devices that sign electronic audit records ***SHALL*** contain a hardware cryptographic module, the Signature Module (SM) that is capable of generating and protecting signature key pairs and generating digital signatures.

*Applies to:* *Voting devices that generate electronic election audit records. Signature verification and other cryptographic operations need not be implemented in hardware, but may also be implemented on the embedded signature module.*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

For the purpose of this requirement a "hardware" cryptographic module means a distinct electronic device, typically a preprogrammed, dedicated microcomputer that holds keying material and performs cryptographic operations. Although today this might typically be a single chip, soldered onto a larger motherboard, it is not the intent of this guideline to preclude higher levels of integration.

The requirements for Electronic Records and which specific records are signed are found in Chapter x.

*Source:* *Click here to add the Source*

*Impact:* *This module protects signature keys from incorrect or malicious voting systems software and helps to ensure the integrity of the audit records.*

↳ **7.1.2-B.1** Non-replaceable embedded Signature Module (SM)

The SM ***SHALL*** be an integral, permanently attached component of the voting device.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The signature module is an integral, nonreplicable part of the voting device, to prevent tampering by replacing or substituting another device. For example if there is a motherboard, the module would be soldered to the motherboard of the voting device. If the core of the voting device is contained on a single chip computer, the module would be a distinct, integral, but independent processor on that chip that does not share logic or memory with other functions.

*Source:* *Click here to add the Source*

*Impact:* *It is difficult for an attacker to change or substitute the embedded signature module.*

↳ **7.1.2-B.2** Signature Module Validation Level

The embedded Signature Module ***SHALL*** be validated under FIPS 140-x with an overall level of 2 and level 3 physical security

*Applies to:* *The embedded digital signature module*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Level 3 physical security requires tamper resistance.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

## 7.1.3 Key management for audit signature keys

Digital signatures require the generation and management of signature key-pairs: a private key and a related public key. The private key is used to sign a message (or, more precisely, the cryptographic message digest of the message), while the associated public key is used to verify the signature on a message. Public key-pairs are certified by public key certificates, electronic documents that are generated and digitally signed by some issuer (often called a Certification Authority or "CA"). The certificates bind a name and other associated data to a public key. Each voting device that generates audit records contains a Signature Module (SM) contains a single permanent *Device Signature Key (DSK)* and, at any one time, up to one *Election Signature Key (ESK)*.

A new ESK is generated by the embedded signature module for every election. An ESK public key certificate is signed with the device key, and binds an election key to the name of the voting device and an election identifier. As a part of the election closeout procedure, a signed count of the number of signature operations performed with the ESK is produced, and the private component of the ESK is destroyed, to preclude later addition of the audit record.

The ESM is provisioned by the voting device vendor with a public key certificate for its DSK, which is exported on commend from the ESM, however the ESM creates it's own signature keys internally and does not permit the export of private signature keys. The ESM maintains a copy of its device key certificate and its current election key certificate, and outputs them on request.

### 7.1.3.1 Device Signature Key (DSK)

The device signature key (DSK), a public key-pair, is internally generated by the voting device as a part of its initial configuration. The DSK has a public key

certificate, that certifies the DSK public key. The DSK certificate may be externally (to the ESM) generated and signed by the voting device manufacturer, then installed in the ESM by the manufacturer, or, alternately, it may be generated internally by the ESM and signed by the DSK private key as a self-signed certificate. The purpose of the DSK is to sign certificates for election keys, and Election Closeout Records. Once generated or installed in the DSK, the DSK certificate is permanently stored in the ESM, and never altered, although copies of it may be exported from the ESM. The DSK certificate is an electronic record that binds the DSK to the unique identification of a single voting device (typically the manufacturer's name, the model number of the device, the unique serial number of the device, and its date of manufacture), for the service life of the voting device.

→ **7.1.3.1-A** DSK Generation

The ESM ***SHALL*** securely generate a permanent DSK in the embedded signature module, using an integral nondeterministic random bit generator.

*Applies to:* *voting devices that produce audit records*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

FIPS 186-3 and NIST Special Publication 800-89 give technical requirements for the generation of secure digital signature keys.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **7.1.3.1-B** Device Certificate Generation

There ***SHALL*** be a process for generating an X.509 Device Certificate that binds the DSK public key to the unique identification of the voting device, its date of issue, the name of the issuer of the certificate and, optionally, to other relevant permanent information, and for storing that Device Certificate permanently in the SM.

*Applies to:* *voting devices that produce audit records*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The Device Certificate may be generated in the ESM and self-signed by the DSK, or it may be signed by an separate external Certification Authority (CA) and installed in the ESM by the manufacturer. That CA could be maintained by or for the voting device manufacturer, or on the behalf of the manufacturer. Alternatively it could be maintained by or for the election authority that purchases the voting device. If the Device Certificate is self-signed, then election authorities should maintain accurate,

reliable records of the self-signed certificates of its voting devices. The Device Certificate permanently binds the device's public key to the unique identification of the individual voting device (the same make, model, serial number information placarded on the case of the voting device). The device certificate might also optionally include the name of the owner of the machine, and any other relevant information that would not change over the service life of the voting device.

This guideline does not prescribe a specific Public Key Infrastructure for keeping and verifying the Device Certificates. A public key certificate is not a secret or confidential record, and the device certificate can be stored or distributed in any convenient manner. If the device certificate is self-signed, then election authorities should maintain independent, accurate, reliable records of the self-signed certificates of its voting devices. If a CA signs the certificate, then the public key of the CA should be securely established and maintained. No revocation or certificate status mechanism is required for the Device Certificates.

Although this standard does not require this, a hash (or at least 64-bits from the hash) of the device public key could be used as the device serial number, making the Device Public Key effectively the device serial number.

Note that the requirement to internally generate private keys and certificates implies requirements to implement an approved hash function, and a nondeterministic random number generator.

Also sote that nothing in this section is intended to preclude a crypto module vendor from delivering SM's already initialized with a DSK and device certificate, perhaps accompanied by a placard (see below), to a voting device manufacturer, for incorporation in the voting device.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **7.1.3-C** Device Identification Placard.

A human readable identification placard ***SHALL*** be permanently affixed to the external frame of any device containing an SM that states, at a minimum, the same unique identification of the voting device contained in the device certificate.

*Applies to:* *Voting devices that generate audit records.*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

It is important that election workers be able to identify and track specific voting devices and correlate them with audit records. The placard and the device certificate identity the same device in the same way. The placard may also contain other information and machine readable information as may be convenient.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **7.1.3-D** Device Signature Key Protection

The SM and the process for generating DSKs ***SHALL*** be implemented so that the private component of DSK is created and exists only inside the protected crypto module boundary of the SM, and the key cannot be altered, or exported from the SM. The Device certificate ***SHALL*** also be kept permanently within the SM, however there ***SHALL*** be a mechanism for exporting the certificate from the SM.

*Applies to:* *embedded signature modules of voting devices*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Once the key is installed in the SM it cannot be changed or read out from the module, and any external copy of the key must be destroyed as a part of the process of initializing the SM. The entire process of generating the key may take place in the SM, otherwise a strictly controlled, secure process is required to generate the keys, install them in the modules, and destroy any external copies of the keys.

*Source:* *embedded signature modules of voting devices*

*Impact:* *Click here to add the Impact*

→ **7.1.3-E** Use of Device Signature Key

The SM ***SHALL*** implement and permit only three uses of the DSK:

- to sign Election Certificates;
- to sign Election Closeout Records
- to sign Device Certificates

*Applies to:* *SMs of voting devices that create audit records*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Each generation of a new election signature key is an auditable event, and the two purposes of the DSK are to certify the new ESK, and to certify that an ESK private key has been closed out (destroyed). While the ESK simply signs hashes presented to it by the voting device software, the SM generates, hashes and signs Election Certificates and Election Closeout Records, although partially from text inputs supplied by the voting device.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

## 7.1.4 Election Signature Key (ESK)

The purpose of an ESK is to sign auditable events in the course of a separate election. A voting device that creates audit records generates its own election signature keys, and maintains only one election signature key at a time. The public component of every election signature key generated by the embedded signature module is signed by the device signature key to create an election public key certificate, and when an election is closed out, the private component of that election key is destroyed by the embedded signature module, which produces an election closeout record attesting to that destruction, signed by the device private key.

→ **7.1.4-A** Election Signature Key (ESK) Generation

The embedded signature module ***SHALL*** internally generate election signature key-pairs (ESK) using an integral nondeterministic random bit generator.

*Applies to:* *SMs of voting devices that create audit records*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The ESK private key exists only in the embedded signature module. It is used with the cryptographic hashes of audit records, to create signatures for audit records. The ESK public key is exported from the embedded signature module in an election certificate signed by the DSK.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **7.1.4-B** Election Public Key Certificate

The SM ***SHALL*** generate and output an X.509 public key certificate for each ESK generated, binding public key to the unique identification of the election, the date of issue of the certificate, the identification of the voting machine (the issuer of the certificate) and, optionally, to other election relevant information.

*Applies to:* *SMs of voting devices that create audit records*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

An Election Public Key Certificate binds an ESK public key to a specific election and the unique name of the individual voting device (the issuer of the certificate). The issuer name should be consistent with the name in the Device Certificate. This guideline does not establish a name format for identifying elections, which might differ from jurisdiction to jurisdiction. No revocation or certificate status mechanism is required for the Election Certificates.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **7.1.4-C** Election Counter

The SM ***SHALL*** maintain an election counter that maintains a running count of each ESK generated.

*Applies to:* *Signature Modules of voting devices that create audit records*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Every election signature key created by the SM is numbered and this number is contained in the public key certificate for that key.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **7.1.4-D** Election Key Closeout

The SM ***SHALL*** implement a closeout command that causes an Election Key Closeout record to be created and output, and the private component of the ESK to be destroyed.

*Applies to:* *The SMs of voting devices that create audit records*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

When the election is complete, the ESK private key is destroyed, so that audit records cannot be forged at a later time.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **7.1.4-E** Election Signature Key Use Counter

The embedded signature module ***SHALL*** maintain a counter of the number of times that an ESK is used.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **7.1.4-F** Election Key Closeout Record

The Election Key Closeout Record ***SHALL*** be signed by the DSK and contain at least :

- the election signature public key (or a message digest of that key);
- the ESK number; and
- the final value of the ESK use counter.

*Applies to:* *The SMs of voting devices that create audit records*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The Election Closeout Record provides a signed record attesting to the destruction of the particular ESK and the number of signatures executed with the ESK. The number of signed audit records should match the ESK use counter; this should be checked by tally devices, and any discrepancies flagged and investigated. The format of the Election Closeout Record is not specified and might be either a signed XML object or it might, potentially, use another signed format such as the ASN.1 Cryptographic Message Syntax.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **7.1.4-G** Documentation

The documentation ***SHALL*** include a precise definition of the fields in the Device Certificate, Election Certificate, the naming supported in certificates, the algorithms supported, and the format of the Election Closeout Record

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

# Chapter 8: Setup Validation Requirements

## 8.1 Introduction/Scope

This section provides requirements supporting the capability to verify that voting equipment is set up and configured properly for use in an election. The requirements support the inspection of the voting equipment to determine that: (a) only authorized and jurisdiction certified software is installed; (b) non-authorized, non-certified software is not installed; (c) registers and variables contain proper values; (d) voting equipment components (such as touch screens, batteries, power supplies, etc.) are within proper tolerances, functioning properly, and ready for use in an election. These requirements support the inspection of the voting equipment after voting system (including election specific) software has been installed, logic and accuracy (L&A) testing has been performed, and before voting equipment is re-configured for another election. However, inspection of the voting equipment at other times during the voting process can be supported by the requirements. The verification of the voting equipment can take place at polling sites and/or central election facilities by authorized personnel. The requirements found in this section are derived from requirements found in commercial and federal standards such as Voluntary Voting System Guidelines 2005 [VVSG 2005] and IEEE P1583 Draft Standard for the Evaluation of Voting Equipment [IEEE P1583].

## 8.2 Background

This section provides a brief overview of the components of voting system equipment that can be inspected and the limitations of the inspections. In addition, it includes a discussion of the effects timing of the inspections has on the assurance provided to voting system equipment.

### 8.2.1 Inspection of software installed on voting equipment

Voting equipment can be inspected to locate and identify the software installed on the voting equipment. Voting equipment that stores software on devices with a file system can use directory paths and filenames to locate and identify software. When voting equipment stores software on devices without file systems, a device's storage locations (such as memory addresses) can be used to locate the software. However, other information (such as byte strings) may be needed to identify software residing in the storage locations of the device.

The integrity of software installed on voting equipment can be inspected to determine if software has been modified. Software verification techniques use

software reference information (such as digital signatures) to determine if the software has been modified. Although software validation techniques can detect modifications, they cannot determine the reason a modification to the software occurs – malicious intent or accidental error. Depending on the characteristics of the software to being inspected, the effectiveness of software verification techniques will vary. Static software[1] can be inspected to determine if the software has been modified. The inspection of dynamic software is possible but provides limited information, since determining the events that change the state of the software is impractical.

Software reference information (such as digital signatures) from the VSTL, NSRL, or other notary repositories can be used to determine if nationally or jurisdiction approved software has been modified. However, VSTLs, NSRL, and other notary repositories can only provide software reference information for the voting system software that they receive from vendors, VSTLs, and jurisdictions. Election specific and installation dependant software used by jurisdictions could be provided to the VSTLs, NSRL, and other notary repositories in order for associated software reference information can be generated. In addition, jurisdictions can also generate software reference information associated with election specific and installation dependant software.

### 8.2.2 Inspection of voting equipment registers and variables

The registers and variables of voting equipment can be inspected to determine their contents. Registers and variables containing constant values will contain the same value whenever they are inspected. Registers and variables containing dynamic values – values that change over time, such as accumulation registers – contain different values depending on the when they are inspected and events that have occurred prior to the inspection. In general, the initial values of dynamic registers and variables are known prior to using the voting equipment in specific elections such as accumulation registers with zero values. However, the intermediate and final values of dynamic registers and variables depend on the events that occur during the operation of the voting equipment for an election.

The proper initial and constant values of registers and variables can be determined from documentation provided by vendors and jurisdictions before the voting equipment is used. The proper intermediate and final values of dynamic registers and variables cannot be determined before the voting equipment is used. However, secondary information from the voting system (such as poll check-in records) might be used to derive the proper values of dynamic registers and variables. For example, the value of the register or variable that holds the number of ballots cast on the voting equipment can be compared to the record of the number of voters that used the voting equipment. However, some dynamic registers may require that the registers or variables be summed together in order to determine if they hold

[1] Static software refers to software that not expected to change over time. Dynamic software refers to software that is expected to change over time but the specific time or value of the change is usually unknown in advance.

proper values. For example, if voters select one from a limited list of choices (such as for, against, or abstain) on an issue that are held in different accumulation registers or variables. A summation of the register or variable values can be compared to the record of the number of voters that used the voting equipment.

### 8.2.3 Inspection of the voting system's other properties

In addition to the inspection of the software, registers, and variables, other properties can be inspected to determine if the voting equipment is ready for use in an election. The other properties of the voting equipment that can be inspected include: (a) the connections of the cables (network, power, etc.), (b) the calibration and function of input and output interfaces such as touch screens, (c) the current level of consumables (paper, ink, battery, etc.), and (d) the state of physical mechanisms (such as locks, tamper evident tape, enclosure panels, etc.) used to protect input and output interfaces. In addition, the voting equipment can perform tests to exercise the functionality of voting equipment components to determine if the components are malfunctioning or mis-configured.

### 8.2.4 Personnel and logistics of voting equipment inspections

The inspection of voting equipment can take place at different locations (polling places and central election offices) and times (before and after ballot casting) in the voting process. In addition, the people (election officials and poll workers) performing the inspections can differ. Inspections of the voting equipment only provide information about the state of the voting equipment at the time of the inspection. As a result, a set of inspections taken during various times in the voting process is better than performing a single inspection at a specific point in the voting process.

The variables of when, where, and who performs the inspections of voting equipment impacts the assurance provide by the inspections. If an inspection takes place at the central election offices before the voting equipment is deployed to polling places, there is a window of opportunity for the state of the voting equipment to be altered before cast ballots are captured. If an inspection takes place at the polling place, the window of opportunity for the state of the voting equipment to be altered before cast ballots are captured decreases. However, the people performing the inspections at the central election offices may have better technical skills to perform the inspections properly versus the people at polling places. These three variables (when, where, and who) need to be considered to gain the maximum benefit provided by performing inspections of voting equipment.

The following example demonstrates how the when, where, and who variables related to voting equipment inspections could be varied to perform inspections by different people, at different locations, and at different times during the voting process. Voting equipment inspections could be performed: (a) before the voting equipment leaves the central election offices; (b) after voting equipment arrives at polling places but before it is used to capture cast ballots; (c) after the voting

equipment has finished capturing cast ballots for the election but before it leaves the polling place; and (d) when voting equipment arrives back at the central election offices before the equipment is reconfigured for the next election. This example incorporates multiple inspections throughout the election process performed by both election administrators and poll workers at both central election offices and polling places.

## 8.3 Voting equipment setup validation requirements

### 8.3.1 Voting equipment setup validation process requirement

➞ **8.3.1-A** Model setup validation process user documentation requirement.

Vendors ***SHALL*** provide a model setup validation process that the voting equipment was designed to support and description of the risks of deviating from the process in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

The model setup validation process ensures that the voting equipment is in a proper initial state before capturing or tallying cast ballots.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **8.3.1-B** Model setup validation inspection requirement

A model setup validation process ***SHALL*** at a minimum include the inspection of voting equipment software (See requirements in section 1.3.2), registers and variables (See requirements in section 1.3.3), other voting equipment properties (See requirements section 3.4), and execution of logic and accuracy testing (See Section X.X) related to readiness of use in an election.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (a) and (f)*

*Impact:* *Extends the VVSG 2005 Volume I, Section 7.4.6 (a) and (f) requirements by requiring the execution of logic and accuracy testing and inspection of items other than installed software and register and variable values*

➞ **8.3.1-C** Model setup validation record generation requirement

The model setup validation process ***SHALL*** describe the records that result from performing the setup validation process.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4.2*

*Impact:* *Relates to VVSG 2005 Volume I, Section 5.4.2 requirements about records to be generated for system readiness*

## 8.3.2 Voting equipment software inspection requirements

The requirements found in this subsection provide the ability to determine that unmodified, certified voting system software is installed on voting equipment.

### 8.3.2.1 Software identification verification

➞ **8.3.2.1-A** Installed software identification procedure user documentation requirement

Vendors ***SHALL*** provide the procedures to identify all software installed on voting equipment in the user documentation.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation); Functional test to be performed in requirement **1.3.2.1-C***

DISCUSSION

This requirement provides the ability to identify if the proper software is installed and that no other software is present on voting equipment. This requirement covers software stored on voting equipment with or without a file system. The software distribution requirement X.X.X requires vendors to provide in the user documentation the list of all software installed on voting equipment.

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (b)(ii)*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.4.6 (b)(ii) by specifying that the procedures to identify installed software needs to be documented*

→ **8.3.2.1-B** Installed software identification technical specification TDP documentation requirement

Vendors ***SHALL*** provide the technical specifications of how voting equipment identifies installed software in the TDP.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

The requirement provides implementation information for VSTLs to support the testing of the voting system.

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (c)*

*Impact:* *This is requirement: (1) extends VVSG 2005 Volume I, Section 7.4.6 (c) by requiring technical documentation on how software installed on voting equipment is identified and (2) generalizes VVSG 2005 Volume I, Section 7.4.6 (c) by not assuming that the software being identified is stored in a device with a file system*

→ **8.3.2.1-C** Voting equipment software identification requirement

Voting equipment ***SHALL*** be able to identify all software installed on voting equipment.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Software stored on devices with file systems can use directory paths and filenames to locate and identify software. When software is stored on devices without file systems, a device's storage locations (such as memory addresses) can be used to locate the software. However, other information (such as byte strings) may be needed to identify software residing in the storage locations of the device.

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (c)*

*Impact:* *This requirements extends VVSG 2005 Volume I, Section 7.4.6 (c) by not assuming that the software being identified is stored in a device with a file system*

→ **8.3.2.1-D** Software identification verification log requirement

Software identification verification inspections of voting equipment ***SHALL*** result in the system event log capturing the following information: time and date of the inspection, information that uniquely identifies the software (such as software name, version, build number, etc.) and location (such as full path name or memory address), identifying information of the individual that performed the inspection, and information that uniquely identifies the voting equipment that was inspected.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V, Section 4.3 (Review of design requirement); Functional test to be performed as part of the System Event Logging requirements*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4.2*

*Impact:* *Relates to VVSG 2005 Volume I, Section 5.4.2 requirements about records to be generated for system readiness*

### 8.3.2.2 Software integrity verification

→ **8.3.2.2-A** Software integrity verification requirement

Voting equipment ***SHALL*** verify the integrity of software installed on storage devices using cryptographic software reference information from the NSRL, State, or other designated notary repositories.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Cryptographic software reference information includes digital signatures and hash values. Requirements related to general cryptography are found in Chapter X: Cryptography.

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (b)*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.4.6 (b) by creating a stand-alone requirement to verify that software installed on voting equipment has not been modified*

→ **8.3.2.2-B** Software integrity verification technical specification TDP documentation requirement

Vendors ***SHALL*** provide a technical specification of how the integrity of software installed on storage devices of voting equipment is verified as part of the TDP.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

The requirement provides implementation information for VSTLs to support the testing of the voting system.

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (c)*

*Impact:* *This requirements extends VVSG 2005 Volume I, Section 7.4.6 (c) by requiring technical documentation on how the software integrity is implemented for voting equipment*

→ **8.3.2.2-C** Software integrity verification technique software non-modification requirement

Software integrity verification techniques ***SHALL*** prevent the modification of software installed on voting equipment.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V, Section 4.3 (Verification of design requirements); Functional testing to be performed as part of requirement* ***1.3.2.2-A***

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (b)(iii)*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.4.6 (b)(iii) with some word changes*

→ **8.3.2.2-D** Software integrity verification technique external device requirement

Software integrity verification techniques for election management systems and networked vote capture devices ***SHALL*** use an external device to verify software installed on election management systems and networked vote capture devices.

*Applies to:* *Election management systems, Networked vote capture device*

*Test Reference:* *Volume V, Section 4.3 (Verification of design requirements); Functional testing to be performed as part of requirement* ***1.3.2.2-A***

DISCUSSION

This requirement applies to election management systems and networked vote capture devices. Vote capture devices are considered networked if they communicate with more than one election management system or other vote capture device. Non-networked vote capture devices still must support the general requirement **1.3.2.2-A** of verifying software installed on the device but can use verification techniques that do not require a separate verification device.

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (b)*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.4.6 (b) by explicitly requiring an external device be used as part of verification process of the software installed on election management systems and networked vote capture devices*

→ **8.3.2.2-E** External interface requirement

Election management systems and networked vote capture devices ***SHALL*** provide an external interface to verify the software installed on storage devices of election management systems and networked vote capture devices.

*Applies to:* *Election management system, Networked vote capture device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

This requirement and associated sub-requirements apply to election management systems and networked vote capture devices. Vote capture devices are considered networked if they communicate with more than one election management system or

other vote capture device. Non-networked vote capture devices are not required to support an external interface to verify software installed on the vote capture device. However, non-networked vote capture devices still must support the general requirement **1.3.2.2-A** of verifying software installed on the device but can use verification techniques that do not require external access to the software to be verified.

*Source:* *VVSG 2005, Volume I, Section 7.4.6 (e)*

*Impact:* *This requirement updates to the VVSG 2005 Volume I Section 7.4.6 (e) by rewording the requirement, removing sub-requirements that are covered by requirements found in **1.3.4**, and focusing the scope of the requirement from voting equipment to election management systems and networked vote capture devices*

↳ **8.3.2.2-E.1** External interface no write requirement

The external interface used to verify the software installed on storage devices of election management systems and networked vote capture devices ***SHALL*** prevent writing of software to storage devices of election management systems and networked vote capture devices.

*Applies to:* *Election management system, Networked vote capture device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

This requirement compliments requirement **1.3.2.2-B.1** that requires software verification techniques to prevent modification of software installed on voting equipment.

*Source:* *VVSG 2005, Volume I, Section 7.4.6 (e)*

*Impact:* *This requirement updates the VVSG 2005 Volume I Section 7.4.6 (e) by explicitly disallowing software to be written to storage devices via the external interface and focusing the scope of the requirement from voting equipment to election management systems and networked vote capture devices*

↳ **8.3.2.2-E.2** External interface no load or execute requirement

The external interface used to verify the software installed on storage devices of election management systems and networked vote capture devices ***SHALL*** prevent the loading and execution of software from the external interface on election management systems and networked vote capture devices.

*Applies to:* *Election management system, Networked vote capture device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005, Volume I, Section 7.4.6 (e)*

*Impact:* *This requirement updates the VVSG 2005 Volume I Section 7.4.6 (e) by explicitly disallowing the loading and execution of software from the external interface on election management systems and networked vote capture devices; and focusing the scope of the requirement from voting equipment to election management systems and networked vote capture devices*

↳ **8.3.2.2-E.3** External interface technical specification TDP documentation requirement

Vendors ***SHALL*** provide a technical specification of how the external interface used to verify the software installed on storage devices of election management systems and networked vote capture devices is implemented.

*Applies to:* *Election management system, Networked vote capture device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

This requirement provides implementation information for VSTLs to support the testing of the voting system.

*Source:* *VVSG 2005, Volume I, Section 7.4.6 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.4.6 (e) by requiring a technical documentation on how the external interface used to verify software installed on election management systems and networked vote capture devices is implemented and focusing the scope of the requirement from voting equipment to election management systems and vote capture devices*

→ **8.3.2.2-F** Software integrity verification procedure user documentation requirement

Vendors ***SHALL*** describe the procedures to verify the integrity of software installed on storage devices of voting equipment in the user documentation.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation); Functional test performed by requirement **1.3.2.2-A***

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (b)(ii)*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.4.6 (b)(ii) by specifying that the procedures to verify the integrity of installed software need to be documented*

→ **8.3.2.2-G** Software reference information generation requirement

VSTLs and notary repositories ***SHALL*** generate cryptographic software reference information for the software of voting equipment.

*Applies to:* *N/A*

*Test Reference:* *N/A*

D I S C U S S I O N

Cryptographic software reference information including digital signatures and hash values can be used to determine if software has been modified. Requirements related to general cryptography are found in Chapter X: Cryptography. Requirements related to the generation of cryptographic software reference information by VSTLs and notary repositories are found in Chapter X: Software distribution and installation. This needs to occur but is maybe more a best practice or process requirement as opposed to a requirement for voting equipment.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.2.2-H** Software reference information traceability requirement

Software reference information used to verify the integrity of software installed on voting equipment ***SHALL*** be traceable back to the source that created the reference information.

*Applies to:* *Programmed device*

*Test Reference:* *N/A*

D I S C U S S I O N

Software reference information can be distributed on uniquely identifiable unalterable media or via electronic means with a digital signature generated by the source of the software reference information. This needs to occur but is maybe

more a best practice or process requirement as opposed to a requirement for voting equipment.

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (d)(ii)*

*Impact:* *This requirement is a generalization of VVSG 2005 Volume I, Section 7.4.6 (d)(ii)*

➞ **8.3.2.2-I** Software integrity verification log requirement

Software integrity verification inspections ***SHALL*** result in the system event log capturing the following information: time and date of the verification, information that uniquely identifies the software (such as software name, version, build number, etc.), the software integrity verification technique used, results of the software verification including the cryptographic software reference information used for the verification, identifying information of the individual that performed the verification, and information that uniquely identifies the voting equipment that contained the software that was verified.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V, Section 4.3 (Review of design requirement); Functional Testing to be performed as part of the System Event Logging requirements*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4.2*

*Impact:* *Relates to VVSG 2005 Volume I, Section 5.4.2 requirements about records to be generated for system readiness*

## 8.3.3 Voting equipment register and variable inspection requirements

The requirements found in this subsection apply to registers and variables implemented in both hardware and software. See section 1.2.2 for a discussion of register and variable characteristics and limitations of register and variable inspection.

➞ **8.3.3-A** Static register and variable value user documentation requirement

Vendors ***SHALL*** provide the values of all static registers and variables, except for the values set to conduct a specific election in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (f)(ii)*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.4.6 (f)(ii) with some word changes*

→ **8.3.3-B** Dynamic register and variable value user documentation requirement

Vendors ***SHALL*** provide the initial starting values of all dynamic registers and variables for the voting system, except for the values set to conduct a specific election in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (f)(ii)*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.4.6 (f)(ii) with some word changes*

→ **8.3.3-C** Maximum and minimum register and variable values user documentation requirement

Vendors ***SHALL*** provide the maximum and minimum values that static and dynamic registers and variables can store in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (f)(ii)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.4.6 (f)(ii) by requiring the documentation of register and variable maximum and minimum values in addition to their initial values*

→ **8.3.3-D** Register and variable value inspection procedure user documentation requirement

Vendors ***SHALL*** provide the procedures to inspect the values of all registers and variables of the voting equipment in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation); Functional testing as part of requirement **1.3.3-F***

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (f)(i)*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.4.6 (f)(i) by requiring the procedures used to inspect register and variable values to be documented*

→ **8.3.3-E** Register and variable value inspection technical specification TDP documentation requirement

Vendors ***SHALL*** provide a technical specification of how the inspection of all the voting equipment registers and variables is implemented by the voting equipment in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

This requirement provides implementation information for VSTLs to support the testing of the voting system.

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (f)(i)*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.4.6 (f)(i) by requiring technical documentation on how inspection of registers and variables values is implemented*

→ **8.3.3-F** Register and variable value determination requirement

Voting equipment ***SHALL*** be able to determine all the values of the voting equipment registers and variables.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (f); VVSG 2005 Volume I, Section 2.2.5 (e); VVSG 2005 Volume I, Section 2.2.6 (b)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.4.6 (f) by requiring the register and variable values to be inspected beyond just their static and initial values; The requirement extends VVSG 2005 Volume I, Section 2.2.5 (e) and 2.2.6 (b) by including all registers and variables and not just "candidate" and "active measure" registers*

➔ **8.3.3-G** Register and variable value inspection log requirement

Register and variable inspections of voting equipment ***SHALL*** result in the system event log capturing the following information: time, date, and location of the inspection, information that uniquely identifies the register or variable, the value of each register and variable, identifying information of the individual that performed the inspection, and information that uniquely identifies the voting equipment that was inspected.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.3 (Review of design requirement): Functional testing to be performed as part of the System Event Logging requirements*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4.2; VVSG 2005 Volume I, Section 2.2.5; VVSG 2005 Volume I, Section 2.2.6*

*Impact:* *Relates to VVSG 2005 Volume I, Section 5.4.2 requirements about records to be generated for system readiness; this requirement updates VVSG 2005 Volume I, Section 2.2.5 statement "…**SHALL** provide a formal record…" and VVSG 2005 Volume I, Section 2.2.6 statement "…**SHALL** provide a printed record…" by specifying information to be included in the record*

## 8.3.4 Voting equipment properties inspection requirements

→ **8.3.4-A** Backup power operational range user documentation requirement

Vendors ***SHALL*** provide the nominal operational range for the backup power sources of the voting equipment in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-B** Backup power source charge indicator requirement

Voting equipment ***SHALL*** indicate the remaining charge of backup power sources in quarterly increments (i.e. full, three-quarters full, half full, quarter full, empty) at a minimum without the use of software.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Backup power sources for voting equipment include but are not limited to batteries.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-C** Backup power inspection technical specification TDP documentation requirement

Vendors ***SHALL*** provide a technical specification of how the inspection of the remaining charge of the backup power sources is implemented by the voting equipment in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

This requirement provides implementation information for VSTLs to support the testing of the voting system.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-D** Backup power inspection procedure user documentation requirement

Vendors ***SHALL*** provide the procedures to inspect the remaining charge of the backup power sources of the voting equipment in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1(Review of documentation); Functional testing to be performed as part of requirement **1.3.4-B***

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-E** Cabling connectivity indicator requirement

Voting equipment ***SHALL*** indicate the connectivity of cabling attached to the voting equipment without the use of software.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

For example, LEDs can be used to indicate when power cables are connected and conducting electricity. LEDs can also be used to indicate when network cables are connected and can transmit information.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-F** Cabling connectivity inspection technical specification TDP documentation requirement

Vendors ***SHALL*** provide a technical specification of how the inspection of the connectivity of cabling attached to voting equipment is implemented by the voting equipment in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

This requirement provides implementation information for VSTLs to support the testing of the voting system.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-G** Cabling connectivity inspection procedure user documentation requirement

Vendors ***SHALL*** provide the procedures to inspect the connectivity of the cabling attached to the voting equipment in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation); Functional testing to be performed as part of requirement **1.3.4-E***

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-H** Communications operational status indicator requirement

Voting equipment ***SHALL*** indicate the operational status of the communications capability of the voting equipment.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-I** Communication operational status inspection technical specification TDP documentation requirement

Vendors ***SHALL*** provide a technical specification of how the inspection of the operational status of the communications capability is implemented by the voting equipment in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

This requirement provides implementation information for VSTLs to support the testing of the voting system.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-J** Communications operational status inspection procedure user documentation requirement

Vendors ***SHALL*** provide the procedures to inspect the operational status of the communications capabilities of the voting equipment in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation); Functional testing performed as part of requirement **1.3.4-H***

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-K** Communications on/off indicator requirement

Voting equipment ***SHALL*** indicate when the communications capability of the voting equipment is on or off without the use of software.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

For example, LEDs can be used to indicate when a given device is on or off. Physical switches can be used to physically turn on or off devices.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-L** Communication on/off inspection technical specification TDP documentation requirement

Vendors ***SHALL*** provide a technical specification of how the inspection of the on/off status of the communications capability is implemented by the voting equipment in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

This requirement provides implementation information for VSTLs to support the testing of the voting system.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-M** Communications on/off status inspection procedure user documentation requirement

Vendors ***SHALL*** provide the procedures to inspect the on/off status of the communications capabilities of the voting equipment in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation); Functional testing to be performed as part of requirement **1.3.4-K***

DISCUSSION

*Click here and type the discussion about this requirement*

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-N** Consumables remaining indicator requirement

Voting equipment ***SHALL*** indicate the remaining amount of voting equipment consumables (i.e. ink, paper, etc.) in quarterly increments (i.e. full, three-quarters full, half full, quarter full, empty) at a minimum.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-O** Consumables quantity of voting equipment user documentation requirement

Vendors ***SHALL*** provide a list of consumables associated with the voting equipment including estimated number of usages per quantity of consumable in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-P** Consumable inspection technical specification TDP documentation requirement

Vendors ***SHALL*** provide a technical specification of how the inspection of the remaining amount of each consumable is implemented by the voting equipment in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

Requirement **1.3.4-O** documents the list of consumables used by the voting equipment. This requirement provides implementation information for VSTLs to support the testing of the voting system.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **8.3.4-Q** Consumable inspection procedure user documentation requirement

Vendors ***SHALL*** provide the procedures to inspect the remaining amount of each consumable of the voting equipment in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation); Functional testing to be performed as part of requirement **1.3.4-N***

DISCUSSION

Requirement **1.3.4-O** documents the list of consumables used by the voting equipment.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **8.3.4-R** Calibration determination of voting equipment components requirement

Voting equipment ***SHALL*** be able to determine the calibration of voting equipment components that require calibration.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Examples of voting equipment components that may require calibration are touch screens and optical scan sensors.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-S** Calibration of voting equipment components nominal range user documentation requirement

Vendors ***SHALL*** provide a list of components associated with the voting equipment that require calibration and the nominal operating ranges for each component in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-T** Calibration of voting equipment components inspection technical specification TDP documentation requirement

Vendors ***SHALL*** provide a technical specification of how the inspection of the calibration for each component is implemented by the voting equipment in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Requirement **1.3.4-S** documents the list of voting equipment components that require calibration. This requirement provides implementation information for VSTLs to support the testing of the voting system.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-U** Calibration of voting equipment components inspection procedure user documentation requirement

Vendors ***SHALL*** provide the procedures to inspect the calibration of each component in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation); Functional testing to be performed as part of requirement **1.3.4-R***

D I S C U S S I O N

Requirement **1.3.4-S** documents the list of voting equipment components that require calibration.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-V** Calibration of voting equipment components adjustment technical specification TDP documentation requirement

Vendors ***SHALL*** provide a technical specification of how the adjustment to the calibration of each component is implemented by the voting equipment in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Requirement **1.3.4-S** documents the list of voting equipment components that require calibration. This requirement provides implementation information for VSTLs to support the testing of the voting system.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-W** Calibration of voting equipment components adjustment procedure user documentation requirement

Vendors ***SHALL*** provide the procedures to adjust the calibration of each component in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation); Functional test to be performed as part of requirement **1.3.4-X***

D I S C U S S I O N

Requirement **1.3.4-S** documents the list of voting equipment components that require calibration.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-X** Calibration of voting equipment components adjustment requirement

Voting equipment ***SHALL*** be able adjust the calibration of voting equipment components that require calibration.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-Y** External interface secure protection requirement

Voting equipment ***SHALL*** be able to secure external interfaces not being used by the voting equipment.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Techniques and mechanisms used to secure external interfaces can be found in Chapter X: Physical Security.

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (e)(i)*

*Impact:* *This requirement generalizes and extends VVSG 2005 Volume I, Section 7.4.6 (e)(i) to all external interfaces of the voting equipment not just external interfaces used in software verification*

→ **8.3.4-Z** External interface secure protection procedure user documentation requirement

Vendors ***SHALL*** provide the procedures to secure external interfaces not being used by the voting equipment.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation); Functional testing to be performed as part of requirement **1.3.4-Y***

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **8.3.4-AA** External interface secure protection technical specification TDP documentation requirement

Vendors ***SHALL*** provide a technical specification of how external interfaces are secured when not being used by the voting equipment in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

Techniques and mechanisms used to secure external interfaces can be found in Chapter X: Physical Security. This requirement provides implementation information for VSTLs to support the testing of the voting system.

*Source:* *VVSG 2005 Volume I, Section 7.4.6 (e)(i), (ii), and (iii)*

*Impact:* *This requirement generalizes VVSG 2005 Volume I, Section 7.4.6 (e)(i), (ii), and (iii) by applying the requirement to all external interfaces and removing the restriction on the physical security techniques used to secure external interfaces*

→ **8.3.4-BB** Model checklist of properties to be inspected user documentation requirement

Vendors ***SHALL*** provide a model checklist of other properties of the voting equipment to be inspected, including a description of the risks on not performing a given inspection in the user documentation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Voting equipment may have other properties that need to be inspected that are not covered in Section 1.3.4. This requirement provides a mechanism for the properties not covered in Section 1.3.4 to be captured.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **8.3.4-CC** Minimal voting equipment properties covered by model checklist requirement

The model checklist of other properties of the voting system to be inspected ***SHALL*** at a minimum include the inspection of backup power sources, cabling, communications capabilities, consumables, calibration of voting equipment components, general physical features of the voting equipment, and securing external interfaces of the voting equipment not being used.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Voting equipment may have other properties that need to be inspected that are not covered in Section 1.3.4. This requirement provides a mechanism for the properties not covered in Section 1.3.4 to be captured.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **8.3.4-DD** Vote equipment property inspection log requirement

Inspections of voting equipment properties ***SHALL*** result in the system event log capturing the following information: time, date, and location of the inspection, a description of the inspections performed, results of each inspection, identifying information of the individual that performed the inspection, and information that uniquely identifies the voting equipment that was inspected.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.3 (Review of design requirement); Functional Testing to be performed as part of the System Event Logging requirements*

DISCUSSION

Click here and type the discussion about this requirement

| | |
|---|---|
| *Source:* | *VVSG 2005 Volume I, Section 5.4.2* |
| *Impact:* | *Relates to VVSG 2005 Volume I, Section 5.4.2 requirements about records to be generated for system readiness* |

### 8.3.5 References

[VVSG 2005] 2005 Voluntary Voting System Guidelines, Election Assistance Commission

[IEEE P1583] IEEE P1583™/D5.3.2 Draft Standard for the Evaluation of Voting Equipment, December 6, 2004.

[TGDC 16-05] Technical Guideline Development Committee Resolution #16-05: Setup Validation, January 2005.

# Chapter 9: Software Distribution and Installation Requirements

## 9.1 Introduction/Scope

This section covers requirements for the distribution of voting system software between voting system vendors, third party software vendors, Voting System Test Laboratories (VSTLs), jurisdictions, and repositories such as the National Software Reference Laboratory (NSRL). The requirements support traceability back to a certified reference version of the voting system software. This traceability provides the basis for verifying that software on voting equipment is certified voting system software. In addition, this section provides requirements that support the installation of software on storage devices of voting equipment. This section does not provide requirements for the evaluation of voting system software for conformance to coding and quality standards of the Voluntary Voting System Guidelines (VVSG). (See Section X: Engineering Practices/Coding) The requirements found in this section are derived from requirements found in the VVSG 2005.

## 9.2 Background

In general, the term software refers to source code, executable code, and other digital data such as configuration or input/output files. In the context of interpreted languages, the source and executable code is one and the same. In addition, two software characteristics are helpful to understand the limitations of verifying software integrity.

The first characteristic is whether or not software changes over time due to execution, installation, or other activities. Dynamic software is expected to change in unpredictable ways over time, while static software is not expected to change once a specified event occurs. When identifying static software, specifying the event after which the software is not expected to change is critical. Examples of dynamic software are temporary and swap space files found on computer systems. Examples of static software are ballot definition files approved by jurisdictions for use in elections. The distinction between dynamic and static software is required to understand the usefulness of verifying software from a modification perspective. Static software can be verified since the software is not expected to change after a specific event. Dynamic software can be verified when initially installed on voting equipment. However the initial installation, the usefulness of dynamic software verification is limited since determining the events that change the state of the software is impractical.

The second characteristic is how software is stored on devices. Some devices use a file system to organize and store software, while other devices do not use a file system. An example of a device with a file system is a computer hard drive. An example of a device that may not have a file system is a Programmable Read Only Memory (PROM). The distinction of devices with and without file systems provides insight into how software stored on the device may be identified. Devices with files system can identify software by directory paths and file names while devices without file systems may identify software by the storage locations on the device (such as memory addresses). General storage devices are designed so that software stored on the device is externally accessible. However, some devices such as Programmable Interface Controllers (PICs) store software to be executed by the device but are not designed to have the software externally accessible. The level of external access provided by devices is required to understand the constraints in verifying the integrity of the software stored on the device. Devices that provide external access to software can verify software installed on the device but devices that do not provide external access to cannot verify software once installed on the device. In general, software can be verified before the software is installed on a specific device.

### 9.2.1 Types of voting system software

There are four types of software used to implement voting system equipment: (1) voting application software, (2) election specific software, (3) third party software, and (4) installation software. Voting application software is developed by voting system vendors to perform voting specific tasks such as casting ballots, tallying election results, and generating reports. Voting application software is developed and executed using third party software such as compilers and operating systems. Election specific software is developed and created by jurisdictions for a specific election such as ballot definition files. Third party software is developed by non-voting system vendors to perform general tasks not specifically related to voting. Third party software is supplied to voting system vendors for use in the development of voting system software and provides functionality to voting equipment. Third party software includes but is not limited to printer drivers, display drivers, operating systems, software development tools, and databases. Installation software is used to install and configure the voting system software, election specific software, and third party software on voting equipment.

### 9.2.2 Distribution of voting system software

This section briefly describes the parties that receive voting system software. The distribution of voting system software between parties must detect and prevent modification of the software. The distribution mechanisms (such as physically on CD-RWs, memory cards, and hard drives; or electronically via email, FTP, and Websites) for voting system software must provide for traceability back to a uniquely identifiable reference version of the software on unalterable media. Requirements related to the distribution of voting system software between parties are provided in Section 1.3.

Voting system vendors develop and maintain voting system software used by voting equipment. Voting system vendors receive software supplied by third party vendors to develop voting system software and provide functionality to voting equipment. Voting system vendors provide software to Voting System Test Laboratories (VSTLs) as part of the certification process. Voting System Test Laboratories (VSTLs) provide a certified copy of voting system software (executable and source code) to the voting system vendor. Along with voting equipment, voting system vendors provide voting system software to their customers.

Third party vendors develop and maintain software used to perform general tasks not specifically related to voting. Third party vendors provide software to voting system vendors to develop voting system software and provide functionality to voting equipment. Third party vendors may provide software to Voting System Testing Laboratories (VSTLs) as part of the certification process and jurisdictions that receive voting equipment. In general, the software provided by third party vendors is in the form of executable code. However, third party vendors may provide source code as part of contractual obligations or open source agreements.

Voting System Testing Laboratories (VSTLs) receive voting system software (as well as voting equipment) from voting system vendors and non-voting specific software from third party vendors as part of the certification process. VSTLs and voting system vendors perform a witness build of the voting system software using source code supplied by the voting system vendors. VSTLs integrate the executable code from the witness build and third party software to verify that no other software modifications are required for the voting equipment to function. VSTLs provide copies of the certified voting system software (executable and source code) to the voting system vendor, the national certification authority, repositories (such as the National Software Reference Library (NSRL)), and jurisdictions.

Repositories receive voting system software (source and executable code) that has been certified from Voting System Test Laboratories (VSTLs). Repositories may receive non-voting specific software from third party vendors and election specific software such as ballot definition files from jurisdictions. Repositories must handle software properly to insure that the software in their possession does not get modified; or released to parties without appropriate approvals. However, repositories may be compelled to release software they possess to comply with court orders. Repositories can be described based on the type of service they provide: escrow, notary, and distribution. Escrow repositories hold software they receive until formal requests for the software are received and approved. Notary repositories use software they receive to generate software integrity information (such as digital signatures or hash values) which can be used to verify the integrity of the piece of software. Notary repositories distribute software integrity information but they do not distribute the voting software or the software used to generate the software integrity information. Distribution repositories provide software they receive to parties approved by the owner of the software. Note that a single repository may provide one or more of the repository services (escrow, notary and distribution). The National Software Reference Library (NSRL) is an example of a notary repository that currently generates software integrity information in the form of hash

values. Since source code is not provided to the NSRL, the NSRL only generates software integrity information for executable code.

Jurisdictions install voting system software on voting equipment in order to conduct elections. Jurisdictions receive certified voting system software from voting system vendors, Voting System Test Laboratories, or distribution repositories. Jurisdictions may receive non-voting specific software from third party vendors. Jurisdictions may test the certified voting system software (source and executable code) to determine if the software conforms to jurisdictional regulations. Jurisdictions develop and create election specific software such as ballot definition and configuration files that can be provided to repositories or other jurisdictions as needed. Jurisdictions can receive software integrity information from notary repositories such as the National Software Reference Library (NSRL) to verify the integrity of voting system software.

# 9.3 Software Distribution Requirements

## 9.3.1 General Documentation Requirements

### 9.3.1.1 Software Identification and Documentation for Technical Data Package (TDP)

→ **9.3.1.1-A** Software list technical data package (TDP) documentation requirement

Vendors ***SHALL*** provide a list of all software related to the voting system in the technical data package (TDP).

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

This requirement establishes a list of the software used by the voting system. All software related to a voting system includes voting application, election specific, third party, and installation software as described in Section 1.2.2. The software may be in the form of source code, executable code, or both as described in Section 1.2.1.

*Source:* *Click here to add the Source*

*Impact:* *This requirement is related to requirement **3.1.1-A (h)** of VVSG 2007 Volume IV but does not include documentation of the directory listing (which is captured in requirement **1.3.1.1-B.1**)*

→ **9.3.1.1-B** Software information TDP documentation requirement

Vendors ***SHALL*** provide at a minimum in the TDP the following information for each piece of software related to the voting system: software product name, software version number, software vendor name, software vendor contact information, type of software (application, election specific, installation, or third party), list of software documentation, component identifier(s) (such as filename(s)) of the software, type of software component (executable code, source code, or data), whether the software component is static or dynamic (as described in Section 1.2), and the specific event causing a software component to become static.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *This requirement is related to requirement **3.1.1-A (e)** of VVSG 2007 Volume IV but is limited to software installed on voting equipment and does not distinguish between COTS and vendor developed software; requirement **3.1.1-B** of VVSG 2007 Volume IV but specifies more information related to the software*

↳ **9.3.1.1-B.1** Software location information TDP documentation requirement

As part of the TDP, vendors ***SHALL*** provide the location (such as full path name or memory address) and storage device (such as type and part number of storage device) where each piece of software is installed on the voting equipment.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

This requirement applies to software installed on voting equipment. The full directory path is the final destination of the software when installed on the voting equipment with a file system.

*Source:* *Click here to add the Source*

*Impact:* *This requirement is related to requirement **3.1.1-A (h)** of VVSG 2007 Volume IV but does not include documentation associated with the software (which is captured in general requirement*

***1.3.1.1-B**); and requirement **2.5.2.2-E** of VVSG 2007 Volume V titled Benchmark directory listings; and extends to include not only directory locations by memory address for storage media without file systems*

↳ **9.3.1.1-B.2** Static software event TDP documentation requirement

As part of the TDP, vendors ***SHALL*** provide the specific event(s) associated with static software that causes the software to become static.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Section 1.2 provides a discussion on static and dynamic software. For example, events that cause software to become static may be the compilation of source code into executable code or the installation of software on voting equipment.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.3.1.1-B.3** Software functionality for voting equipment TDP documentation requirement

As part of the TDP, vendors ***SHALL*** document the functionality provided to the voting equipment by the software installed on the voting equipment.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

This requirement provides implementation information for VSTLs to support the testing of voting system.

*Source:* *Click here to add the Source*

*Impact:* *This requirement is related to requirements **3.1.1-A (a)** and **(b)** of VVSG 2007 Volume IV but is limited to software installed on voting equipment*

↳ **9.3.1.1-B.4** Software dependencies and interaction TDP documentation requirement

As part of the TDP, vendors ***SHALL*** map the dependencies and interactions between software installed on the voting equipment.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1(Review of documentation)*

D I S C U S S I O N

This requirement provides implementation information for VSTLs to support the testing of voting system.

*Source:* *Click here to add the Source*

*Impact:* *This requirement is related to requirements **3.1.1-A (a)** and **(b)** of VVSG 2007 Volume IV but is limited to software installed on voting equipment; and specifically calls out mapping of dependences and interactions*

### 9.3.1.2 Software Identification and Documentation for User Documentation

➞ **9.3.1.2-A** Software list user documentation requirement

Vendors ***SHALL*** provide a list of all software including installation software to be installed on the voting equipment in the user documentation.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Software to be installed on the voting equipment includes executable code, configuration files, data files, and election specific software.

*Source:* *Click here to add the Source*

*Impact:* *This requirement is related to requirement **3.1.1-A (h)** of VVSG 2007 Volume IV but does not include documentation of the directory listing (which is captured in requirement **1.3.1.1-B.1**)*

↳ **9.3.1.2-A.1** Software information user documentation requirement

Vendors ***SHALL*** provide at a minimum in the user documentation the following information for each piece of software to be installed on voting equipment:

software product name, software version number, software vendor name, software vendor contact information, type of software (application, election specific, installation, or third party), list of software documentation, component identifier(s) (such filename(s)) of the software, type of software component (executable code, source code, or data), whether the software component is static or dynamic (as described in Section 1.2), and the specific event causing a software component to become static.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *This requirement is related to requirement **3.1.1-A (e)** of VVSG 2007 Volume IV but is limited to software installed on voting equipment and does not distinguish between COTS and vendor developed software; requirement **3.1.1-B** of VVSG 2007 Volume IV but specifies more information related to the software*

↳ **9.3.1.2-A.2** Software location information user documentation requirement

Vendors ***SHALL*** provide in the user documentation the location (such as full path name or memory address) and storage device (such as type and part number of storage device) where each piece of software is installed on the voting equipment.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

This requirement applies to software installed on voting equipment. The full directory path is the final destination of the software when installed on the voting equipment with a file system.

*Source:* *Click here to add the Source*

*Impact:* *This requirement is related to requirement **3.1.1-A (h)** of VVSG 2007 Volume IV but does not include documentation associated with the software (which is captured in general requirement **1.3.1.2-A.1**); and requirement **2.5.2.2-E** of VVSG 2007 Volume V titled Benchmark directory listings; and extends to include not only directory locations by memory address for storage media without file systems*

↳ **9.3.1.2-A.3** Static software event user documentation requirement

Vendors ***SHALL*** provide in the user documentation the specific event(s) associated with static software that causes the software to become static.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

Section 1.2 provides a discussion on static and dynamic software. For example, a configuration file may be considered static once installation events occur.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

## 9.3.2 Software Distribution Package Requirements

Software distribution packages are used to distribute software between different parties. Software distribution packages contain software from voting system vendors, third party vendors, voting system test laboratories, repositories, and jurisdictions. The software contained on software distribution packages include voting application software, election specific software, installation software, third party software, and software integrity information.

→ **9.3.2-A** Software distribution package master copy establishment requirement

A software distribution package master copy ***SHALL*** be established from which copies are created and distributed.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

Software is traceable back to a software distribution package master copy containing the software. Copies of software distribution packages can be distributed on via modifiable media (physically on CD-RWs, memory cards, and hard drives; or electronically via email, FTP, and Websites) since digital signatures are created as part of software distribution packages. (See requirement **1.3.2-F**)

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.3.2-A.1** Master copy creation record requirement

A master copy creation record ***SHALL*** be created that includes at a minimum: the unique identifier of the record; the unique identifier of the master copy; the type of unalterable storage media containing the master copy; time, date, and location the master copy was created; name(s), affiliation(s), and signature(s) of the people present during the creation of the master copy; name and version of the software distribution package; the name, version and certification number (if certified) of the voting system; identifiers of the software components (such as filename(s)) in the software distribution package; location of software components in the software distribution package; and the digital signature algorithm used to sign the contents of the software distribution package.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.3.2-A.2** Master copy storage media requirement

A software distribution package master copy ***SHALL*** be stored on unalterable storage media.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

D I S C U S S I O N

Unalterable storage media includes technology such as a CD-R, but not CD-RW.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.3.2-A.3** Copy creation record requirement

A copy creation record ***SHALL*** be created that includes at a minimum: the unique identifier of the master copy; the distribute mechanism for the copy; time, date, and location the copy was created; name(s), affiliation(s) and signature(s) of the people present during the creation of the copy; and the

contact information (title, organization, address, phone number, email address, etc.) for the organizations or people to whom copies were distributed.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

Copies of software distribution packages can be distributed on via modifiable media (physically on CD-RWs, memory cards, and hard drives; or electronically via email, FTP, and Websites) since digital signatures are created as part of software distribution packages. (See requirement **1.3.2-F**)

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.3.2-A.4** Master copy and copy creation record storage media requirement

The master copy and copy creation records ***SHALL*** be made on unalterable storage media.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

D I S C U S S I O N

Unalterable storage media includes technology such as a CD-R, but not CD-RW.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.3.2-A.5** Master copy retention requirement

VSTLs, vendors, repositories, and NSRL ***SHALL*** retain the master copy of software distribution packages and associated records until notified by the national certification authority that they can be archived.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.2-B** Human readable software distribution package identification file requirement

Software distribution packages ***SHALL*** contain a separate human readable file that provides at a minimum: the name and version of the software distribution package; the unique identifier of the master copy; the name, version, certification number (if certified) of the voting system; and the algorithm used to create digital signatures for the contents of the software distribution package (see requirement **1.3.2-F**).

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

D I S C U S S I O N

Binary document formats and text containing markup tags are not considered human-readable. Applications may generate such documents, but it must also provide the functionality to render those documents in human-readable form (e.g., by including the necessary reader application).

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.2-C** Human readable software distribution package content file requirement

Software distribution packages ***SHALL*** contain a separate human readable file that provides at a minimum the following information for each component within the software distribution package: software component identifier (such as filename), software vendor name, software product name, software version, and component location within the software distribution package (such as the full directory path to the file or archive containing the file or memory addresses).

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

D I S C U S S I O N

Binary document formats and text containing markup tags are not considered human-readable. Applications may generate such documents, but it must also provide the functionality to render those documents in human-readable form (e.g., by including the necessary reader application).

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **9.3.2-D** Software distribution archive files format requirement

When software distribution packages use archive files to hold multiple software components, the archive files ***SHALL*** be generated using algorithms and file formats in common usage.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

D I S C U S S I O N

Some commonly used archive files include but are not limited to zip, gz, and tarbz2.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **9.3.2-E** Full directory path for files within an archive file requirement

The full directory path and filename of archive files ***SHALL*** be used as the full directory path for the files within the archive.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **9.3.2-F** Software distribution package digital signature requirement

Software distribution packages ***SHALL*** contain digital signatures for each software component contained within the software distribution package.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

DISCUSSION

Digital signatures are generated for the un-archived forms of each of the software files as well as archive files. See Section X: Cryptography for requirements related to digital signatures.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.3.2-F.1** Software distribution package digital signature generation requirement

Software distribution packages ***SHALL*** contain at least digital signatures generated by the organization that created the software distribution package.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.3.2-F.2** Software distribution package digital signature format requirement

Digital signatures ***SHALL*** be stored in a non-proprietary standard data format as part of the software distribution package.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

DISCUSSION

Some non-proprietary standard data formats for digital signatures include IETF RFC 3852: Cryptographic Message Syntax (CMS), RSA Public Key Cryptographic Standard #7: Cryptographic Message Syntax Standard, W3C XML-Signature Syntax and Processing.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.2-G** Software distribution package physical media labeling requirement

Each piece of physical media used for software distribution packages ***SHALL*** be labeled on an external surface of the media including at a minimum: the

organization that created the media; the creation date of the media; unique identifier of the media (such as a serial number); software distribution package name and version; whether the software has been certified or not; and the name, version, and certification number (if certified) of the voting system.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

Each piece of media needs to be uniquely identifiable even if the pieces contain the same information in order to support traceability. These requirements apply to master copies of software distribution packages since they are required to be stored on unalterable media (See requirement **1.3.2-A.2**).

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.2-H** Physical media digital signature requirement

Each piece of physical media used for software distribution packages ***SHALL*** contain a digital signature generated by the creator (such as VSTL, vendor, repository, or jurisdiction) covering the entire contents of the media.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

D I S C U S S I O N

The binary image refers to the complete contents of the physical media as a whole. A binary image of physical media may contain multiple files. See Section X: Cryptography for requirements related to digital signatures.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

## 9.3.3 Voting System Software Build Requirements

### 9.3.3.1 Build Documentation Requirements for Voting System Software

**9.3.3.1-A** Build environment software and hardware TDP documentation requirement

As part of the TDP, vendors ***SHALL*** provide a list of all software and hardware required to assemble the build environment used to create executable code including application logic, border logic, and third party logic.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Third party software (such as operating systems, compilers, and libraries) required to build voting system software are captured by this requirement.

*Source:* *Click here to add the Source*

*Impact:* *This requirement is a generalization of the requirement found at Section **2.4.5.2-B** of Volume IV of VVSG 2007 by focusing on all software and hardware needed to build the executable code and not just COTS compilers and assemblers*

**9.3.3.1-B** Build environment assembly procedures TDP documentation requirement

As part of the TDP, vendors ***SHALL*** document the procedures to assemble the build environment(s) used to create executable code including application logic, border logic, and third party logic.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.1.2*

*Impact:* *This requirement extends the requirement found at Section 5.6.1.2 of the EAC Testing and Certification Program Manual [EAC 2007] by requiring vendors to document the procedures used to establish the build environment*

→ **9.3.3.1-C** Voting system software build procedures TDP documentation requirement

As part of the TDP, vendors ***SHALL*** document the procedures used to build the voting system software executable code including application logic, border logic, and third party logic.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.3.1-D** Voting system software source code TDP requirement

As part of the TDP, vendors ***SHALL*** provide a software distribution package on unalterable storage media containing source code of voting system software including application logic, border logic, and third party logic.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

See Section 1.3.2 requirements related to software distribution packages, which include digital signatures for each piece of software contained in the software distribution package. Unalterable storage media includes technology such as a CD-R, but not CD-RW.

*Source:* *Click here to add the Source*

*Impact:* *This requirement is related to the requirement found at 2.4.7.2-E in Volume IV of VVSG 2007 but specifies how the source code should be packaged*

### 9.3.3.2 Build Environment Establishment

When a previously certified version of the voting system software exists and software updates are being created, see Section 1.3.3.4.

→ **9.3.3.2-A** VSTL build environment assembly requirement

The VSTL ***SHALL*** assemble the build environment(s) used to create executable code including application logic, border logic, and third party logic.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.1.2*

*Impact:* *This requirement does not modify the requirement found in Section 5.6.1.2 of the EAC Testing and Certification Program Manual [EAC 2007]; this requirement supercedes requirement **2.5.2.3-A** of VVSG 2007 Volume V and extends the requirement by applying it to the build environment assembly*

↳ **9.3.3.2-A.1** Build environment assembly witness requirement

At least one representative from the VSTL and vendor ***SHALL*** witness the assembly of the build environment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6*

*Impact:* *This requirement does not modify the requirement found in Section 5.6 of the EAC Testing and Certification Program Manual [EAC 2007] requiring a representative from both the vendor and VSTL to be present during the build; this requirement supercedes requirement **2.5.2.3-A** of VVSG 2007 Volume V and extends the requirement to apply to the build environment assembly*

↳ **9.3.3.2-A.2** Build environment establishment record requirement

A representative from the VSTL ***SHALL*** create a build environment establishment record that includes at a minimum: a unique identifier (such as a serial number) for the record; a list of unique identifiers of unalterable storage media associated with the record; the time, date, and location the build environment was established; names, affiliations, and signatures of all people present; copies of the procedures used to assemble the build environment; list of software and hardware used to establish the build environment; and the voting system associated with the build environment.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.9*

*Impact:* *This requirement updates the requirement found in Section 5.9 of the EAC Testing and Certification Program Manual [EAC 2007] by specifying the information needed to be documented when establishing the build environment.*

↳ **9.3.3.2-A.3** Build environment software and hardware procurement requirement

The VSTL ***SHALL*** obtain the software and hardware required to establish the build environment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Requirement **1.3.3.1-A** documents the software and hardware required to assemble the build environment.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.3.3.2-A.4** Open market procurement of third party software and hardware requirement

The VSTL ***SHALL*** obtain third party software and hardware required to assemble the build environment from the open market.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *This requirement is related to requirement **3.1.1-C** of VVSG 2007 Volume IV but is specific to software for the build environment instead of the voting equipment; extends the requirement to build environment hardware; and does not require a "certification" of the procurement from the manufacturer, licensed dealer, or distributor; this requirement supercedes requirement **2.5.2.3-B** of VVSG 2007 Volume V, uses the term third party software instead of the term COTS, and extends the requirement by applying it to the build environment*

↳ **9.3.3.2-A.5** Erasable storage media preparation requirement

The VSTL ***SHALL*** remove any previously stored information on erasable storage media in preparation for using the media to assemble the build environment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

The purpose of this requirement is to prepare erasable storage media for use by the build environment. The requirement does not require the prevention of previously stored information leakage or recovery. Simply deleting files from file systems, flashing memory cards, and removing electrical power from volatile memory satisfies this requirement.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.1.1*

*Impact:* *This requirement is the same as the requirements found in Section 5.61.1 of the EAC Testing and Certification Program*

*Manual [EAC 2007] except for requiring the use of a COTS product to perform the cleaning*

↳ **9.3.3.2-A.6** Build environment assembly requirement

The VSTL ***SHALL*** use the procedures found in the TDP to assemble the build environment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Requirement **1.3.3.1-B** documents the procedures to assemble the build environment. VSTLs can have vendors assist in the assembly of the build environment.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.1.2*

*Impact:* *This requirement extends the requirement found at Section 5.6.1.2 of the EAC Testing and Certification Program Manual [EAC 2007] by requiring VSTLs to use the document procedures provided by vendors to establish the build environment; See requirement **1.3.3.1-B***

↳ **9.3.3.2-A.7** Build environment assembly deviation record requirement

The VSTL ***SHALL*** document as part of the build environment establishment record the reason for any deviation from assembly procedures found in the TDP.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

Requirement **1.3.3.1-B** documents the procedures used to assemble the build environment.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.9*

*Impact:* *This requirement updates the requirement found in Section 5.9 of the EAC Testing and Certification Program Manual [EAC 2007] by specifying that deviation from vendor provided procedures to be documented when establishing the build environment.*

↳ **9.3.3.2-A.8** Build environment digital signature verification requirement

When digital signatures are associated with software, the VSTL ***SHALL*** verify digital signatures before using the software for the build environment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.2.1*

*Impact:* *This requirement applies concept of the requirement found in Section 5.6.2.1 of the EAC Testing and Certification Program Manual [EAC 2007] to software associated with the build environment; requirement is also related to requirement **3.1.1-C** of VVSG 2007 Volume IV but does not require a "certification" of the procurement from the manufacturer, licensed dealer, or distributor and is limited to the build environment*

↳ **9.3.3.2-A.9** Build environment digital signature verification record requirement

The results of digital signature verification including who generated the signature ***SHALL*** be part of the build environment establishment record.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.9*

*Impact:* *This requirement updates the requirement found in Section 5.9 of the EAC Testing and Certification Program Manual [EAC 2007] by specifying the results of digital signature verification needs to be documented as part of the record when establishing the build environment.*

↳ **9.3.3.2-A.10** Build environment pre-build binary image copy requirement

The VSTL ***SHALL*** copy the binary image of the assembled build environment to unalterable storage media.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

D I S C U S S I O N

This requirement creates a snapshot of the build environment before it is used to build the voting system software executable code. Unalterable storage media includes technology such as a CD-R, but not CD-RW.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.3.3.2-A.11** Build environment pre-build binary image digital signature requirement

The VSTL ***SHALL*** create and include a digital signature for the binary image of the assembled build environment on the unalterable storage media.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

D I S C U S S I O N

See the Section X: Cryptography for requirements related to digital signatures.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.1.3*

*Impact:* *This requirement constrains the requirement found in Section 5.6.1.3 of EAC Testing and Certification Program Manual [EAC 2007] to the use of a digital signature from using a "file signature" which could be a hash value or digital signature*

### 9.3.3.3 Build of Voting System Software Executable Code

When a previously certified version of the voting system software exists and software updates are being created, see Section 1.3.3.4.

→ **9.3.3.3-A** Use of established build environment requirement

The VSTL ***SHALL*** build the executable code including application logic, border logic, and third party logic of the voting system using the established build environment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

The build environment is established using the requirements in section 1.3.3.2.

*Source:* *Click here to add the Source*

*Impact:* *This requirement supercedes requirement **2.5.2.3-A** of VVSG 2007 Volume V*

↳ **9.3.3.3-A.1** Voting system software build witness requirement

At least one representative from the VSTL and vendor ***SHALL*** witness the build of executable code including application logic, border logic, and third party logic of the voting system.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6*

*Impact:* *This requirement does not modify the requirement found in Section 5.6 of the EAC Testing and Certification Program Manual [EAC 2007] requiring a representative from both the vendor and VSTL to be present during the build; this requirement supercedes requirement **2.5.2.3-A** of VVSG 2007 Volume V*

↳ **9.3.3.3-A.2** Voting system software build record requirement

A representative from the VSTL ***SHALL*** create an executable code build record that includes at a minimum: a unique identifier (such as a serial number) for the record; a list of unique identifiers of unalterable storage media associated with the record; the time, date, and location of the build; names, affiliations, and signatures of all people present; filenames of the source code and resulting executable code; voting system software version; name and version of the voting system (including certification number, if possible); and copies of the procedures used to build the voting system software executable code.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.9*

*Impact:* *This requirement updates the requirement found in Section 5.9 of the EAC Testing and Certification Program Manual [EAC 2007] by specifying the information needed to be documented when creating executable code.*

↳ **9.3.3.3-A.3** Voting system software digital signature verification requirement

The VSTL ***SHALL*** validate vendor digital signatures on voting system software source code before placing source code on the build environment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

Requirement **1.3.3.1-D** requires vendors to provide voting system software source code with digital signatures as part of the TDP.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.2.1*

*Impact:* *This requirement differs from the requirement found in Section 5.6.2.1 of the EAC Testing and Certification Program Manual [EAC 2007] by constraining the verification to digital signature from a "file signature" (which could be a hash value or digital signature); extends 5.6.2.1 by specifying the verification to happen before software is installed on the build environment; and does not call for the digital signature of the build environment to be verified before installing the source code.*

↳ **9.3.3.3-A.4** Voting system software digital signature verification result record requirement

The results of digital signature validation including who generated the signature ***SHALL*** be part of the executable code build record for voting system software.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.9*

*Impact:* *This requirement updates the requirement found in Section 5.9 of the EAC Testing and Certification Program Manual [EAC 2007] by specifying the results of digital signature verification needs to be documented as part of the record when building the executable code.*

↳ **9.3.3.3-A.5** Voting system software build requirement

The VSTL ***SHALL*** use the procedures found in the TDP to build the voting system software executable code including application logic, border logic, and third party logic.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

Requirement **1.3.3.1-C** documents the procedures to build voting system software executable code. VSTLs can have vendors assist in building of the voting system software executable code.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.3*

*Impact:* *This requirement extends the requirement found at Section 5.6.3 of the EAC Testing and Certification Program Manual [EAC 2007] by requiring VSTLs to use the document procedures provided by vendors to build the executable code; See requirement **1.3.3.1-C***

↳ **9.3.3.3-A.6** Voting system software executable code build deviation record requirement

The VSTL ***SHALL*** document as part of the executable code build record the reason for any deviation from build procedures found in the TDP.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1*

DISCUSSION

Requirement **1.3.3.1-C** documents the procedures to build voting system software executable code.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.9*

*Impact:* *This requirement updates the requirement found in Section 5.9 of the EAC Testing and Certification Program Manual [EAC 2007] by specifying that deviation from vendor provided procedures to be documented when building executable code.*

↳ **9.3.3.3-A.7** Build environment post build binary image requirement

After voting system software executable code including application logic, border logic, and third party logic has been built, the VSTL ***SHALL*** copy the binary image of the build environment (including source and executable code) to unalterable storage media.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

DISCUSSION

This requirement creates a snapshot of the build environment after it has been used to build voting system software executable code. Unalterable storage media includes technology such as a CD-R, but not CD-RW.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.2.3*

*Impact:* *This requirement differs from the requirement found in Section 5.6.2.3 of the EAC Testing and Certification Program Manual [EAC 2007] by creating the binary image after, instead of before, the software executable code has been built*

↳ **9.3.3.3-A.8** Build environment post build binary image digital signature requirement

After voting system software executable code including application logic, border logic, and third party logic has been built, the VSTL ***SHALL*** create a digital signature for the binary image of the build environment (including source and executable code); and include the digital signature on the unalterable storage media with the binary image.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.4*

DISCUSSION

See the Section X: Cryptography for requirements related to digital signatures.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.2.2*

*Impact:* *This requirement differs from the requirement found in Section 5.6.2.2 of the EAC Testing and Certification Program Manual [EAC 2007] by creating a digital signature on the binary image after the software executable code has been built as opposed to a "file signature" which could be a hash value or digital signature before the software executable code is built; although requirement 5.6.3.1 of the EAC Testing and Certification Program Manual requires "file signatures" for executable code*

### 9.3.3.4 Build of Previously Certified Voting System Software Executable Code

The following voting system software build requirements apply when updates to previously certified voting system software has occurred. These requirements assume the original build environment can be used to create the updated software and a significant portion of original software is not being updated. If the original build environment cannot be used, then the requirements of Section 1.3.3.2 and 1.3.3.3 apply.

→ **9.3.3.4-A** Original certified voting system software identification requirement

As part of the TDP, vendors ***SHALL*** provide the certification number associated with the voting system software to be updated.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.3.4-B** Updated voting system software source code requirement

As part of the TDP, vendors ***SHALL*** provide a software distribution package on unalterable storage media containing source code of the updated voting system software including application logic, border logic, and third party logic.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

See Section 1.3.2 requirements related to software distribution packages, which include digital signatures for each piece of software contained in the software distribution package. Unalterable storage media includes technology such as a CD-R, but not CD-RW.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.3.4-C** Updated voting system software build procedure TDP documentation requirement

As part of the TDP, vendors ***SHALL*** document the procedures used to build the updated voting system software including application logic, border logic, and third party logic using the post build environment associated with the originally certified voting system software.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.3.4-D** Updated voting system software build witness requirement

At least one representative from the VSTL and vendor ***SHALL*** witness the establishment of the post build environment associated with the originally certified voting system software; and build of the updated voting system software executable code including application logic, border logic, and third party logic.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6*

*Impact:* *This requirement does not modify the requirement found in Section 5.6 of the EAC Testing and Certification Program Manual [EAC 2007] requiring a representative from both the vendor and VSTL to be present during the build; this requirement supercedes requirement **2.5.2.3-A** of VVSG 2007 Volume V*

➞ **9.3.3.4-E** Original post build environment re-establishment requirement

The VSTL ***SHALL*** establish the build environment using the post build environment binary image associated with the originally certified voting system software.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Requirements **1.3.3.3-A.5** and **1.3.3.3-A.6** create the post build binary image of the original build of the certified voting system software developed by the vendor. If the VSTL does not posses the required hardware and software to create the build environment then Requirements **1.3.3.2-A.3** and **1.3.3.2-A.4** apply.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.4.1 and 5.6.4.2*

*Impact:* *This requirement extends the requirement found in Section 5.6.4.1 and 5.6.4.2 by explicitly stating the original build environment needs to be established*

↳ **9.3.3.4-E.1** Erasable storage media preparation requirement

The VSTL ***SHALL*** remove previously stored information on erasable storage media in preparation for using the media to establish the build environment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

The purpose of this requirement is to prepare the erasable storage media for use by the original post build environment. The requirement does not require the prevention of previously stored information leakage or recovery. Simply deleting files from the file system, flash memory cards, and removing electrical power from volatile memory satisfy this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.1.1*

*Impact:* *This requirement is the same as the requirements found in Section 5.61.1 of the EAC Testing and Certification Program Manual [EAC 2007] except for requiring the use of a COTS product to perform the cleaning*

↳ **9.3.3.4-E.2** Original post build environment re-establishment digital signature verification requirement

The VSTL ***SHALL*** verify the digital signature of the post build binary image associated with the originally certified voting system software before using the binary image to establish the build environment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.4.1*

*Impact:* *This requirement does not modify the requirement found in Section 5.6.4.1 of the EAC Testing and Certification Program Manual [EAC 2007] that states the file signature of the build environment needs to be verified before use*

↳ **9.3.3.4-E.3** Original post build environment re-establishment digital signature verification record requirement

The result of digital signature verification including who generated the signature ***SHALL*** be part of the original post build environment establishment record.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.9*

*Impact:* *This requirement updates the requirement found in Section 5.9 of the EAC Testing and Certification Program Manual [EAC 2007] by specifying the results of digital signature verification needs to be documented as part of the record when establishing the build environment*

↳ **9.3.3.4-E.4** Original post build environment re-establishment record requirement

A representative from the VSTL ***SHALL*** create an original post build environment establishment record that includes at a minimum: a unique identifier (such as a serial number) for the record; a list of unique identifiers of unalterable storage media associated with the record; the time, date, and location the original post build environment was established; names, affiliations, and signatures of all people present; copies of the procedures used to assemble the original post build environment; list of software and hardware used to establish the original post build environment; and the voting system associated with the original post build environment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.9*

*Impact:* *This requirement updates the requirement found in Section 5.9 of the EAC Testing and Certification Program Manual [EAC 2007] by specifying the information needed to be documented when establishing the build environment.*

➞ **9.3.3.4-F** Build of the updated voting system software executable code requirement

The VSTL ***SHALL*** build the executable code including application logic, border logic, and third party logic of the updated voting system software.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.4.2*

*Impact:* *This requirement does not modify the requirement found in Section 5.6.4.2 of the EAC Testing and Certification Program Manual [EAC 2007] that states the executable files are created; this requirement supercedes requirement **2.5.2.3-A** of VVSG 2007 Volume V*

↳ **9.3.3.4-F.1** Updated voting system software source code digital signature verification requirement

The VSTL ***SHALL*** verify the digital signature of updated voting system software source code before placing the updated source code on the build environment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.4.2*

*Impact:* *This requirement modifies the requirement found in Section 5.6.4.2 of the EAC Testing and Certification Program Manual [EAC 2007] by constraining the verification to digital signature from a "file signature" (which could be a hash value or digital signature); extends 5.6.2.1 by specifying the verification to happen before software is installed on the build environment; and does not call for the digital signature of the build environment to be verified before installing the source code.*

↳ **9.3.3.4-F.2** Updated voting system software source code digital signature verification record requirement

The result of digital signature verification including who generated the signature ***SHALL*** be part of the updated voting system software build record.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Requirement **1.3.3.4-B** requires vendors to provide voting system software source code with digital signatures as part of the TDP.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.9*

*Impact:* *This requirement updates the requirement found in Section 5.9 of the EAC Testing and Certification Program Manual [EAC 2007] by specifying the results of digital signature verification needs to be documented as part of the record when building the executable code.*

↳ **9.3.3.4-F.3** Updated voting system software build procedure requirement

The VSTL ***SHALL*** use the procedures found in the TDP to build the updated voting system software executable code including application logic, border logic, and third party logic.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Requirement **1.3.3.4-C** documents the procedures to build the updated voting system software executable code. VSTLs can have vendors assist in building of the updated voting system software executable code.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.4.2*

*Impact:* *This requirement extends the requirement found in Section 5.6.4.2 of the EAC Testing and Certification Program Manual [EAC 2007] by specifying the use of the vendor supplied procedures to build the updated voting system software*

↳ **9.3.3.4-F.4** Updated voting system software build record requirement

A representative from the VSTL ***SHALL*** create an executable code build record that includes at a minimum: a unique identifier (such as a serial number) for the record; a list of unique identifiers of unalterable storage media associated with the record; the time, date, and location of the build; names, affiliations, and signatures of all people present; filenames of the source code and resulting executable code; voting system software version; name and version of the voting system (including certification number, if possible); and copies of the procedures used to build the updated voting system software executable code.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.9*

*Impact:* *This requirement updates the requirement found in Section 5.9 of the EAC Testing and Certification Program Manual [EAC 2007] by specifying the information needed to be documented when creating updated executable code.*

↳ **9.3.3.4-F.5** Updated build environment post build binary image requirement

After updated voting system software executable code including application logic, border logic, and third party logic has been built, the VSTL ***SHALL*** copy the binary image of the updated build environment (including source and executable code) to unalterable storage media.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

This requirement creates a snapshot of the updated build environment after it has been used to build the updated voting system software executable code. Unalterable storage media includes technology such as a CD-R, but not CD-RW.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.2.3*

*Impact:* *This requirement differs from the requirement found in Section 5.6.2.3 of the EAC Testing and Certification Program Manual [EAC 2007] by creating the binary image after, instead of before, the updated software executable code has been built*

↳ **9.3.3.4-F.6** Updated build environment post build binary image digital signature requirement

After updated voting system software executable code including application logic, border logic, and third party logic has been built, the VSTL ***SHALL*** create a digital signature for the binary image of the updated build environment (including source and executable code); and include the digital signature on the unalterable storage media with the binary image.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

See the Section X: Cryptography for requirements related to digital signatures.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.2.2*

*Impact:* *This requirement differs from the requirement found in Section 5.6.2.2 of the EAC Testing and Certification Program Manual [EAC 2007] by creating a digital signature on the binary image after the software executable code has been built as opposed to a "file signature" which could be a hash value or digital signature before the software executable code is built; although requirement 5.6.3.1 of the EAC Testing and Certification Program Manual requires "file signatures" for updated executable code*

### 9.3.4 Voting System Test Laboratories (VSTL) Software Distribution Packages

→ **9.3.4-A** VSTL software distribution package containing voting system software source and executables requirement

The VSTL ***SHALL*** create a software distribution package master copy containing the source and executable code from the witness build of the voting system software.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

This requirement establishes the software distribution package master copy that supports traceability of voting system software source and executable code back to the VSTL. Requirement **1.3.2-A.2** requires software distribution package master copies to be on unalterable media. Requirement **1.3.2-F** requires digital signatures for each software component contained in the software distribution package. Requirement **1.3.2-A.2** requires VSTLs to retain software distribution package master copies until notified by the EAC.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.3.1*

*Impact:* *This requirement differs from the requirement found in Section 5.6.3.1 of the EAC Testing and Certification Program Manual [EAC 2007] by using a digital signature instead of a "file signature" which could be a hash value or digital signature; and*

*extends the requirement to include source code as well as the executable code*

→ **9.3.4-B** VSTL software distribution package containing configuration files, installation programs and third party developed software requirement

The VSTL ***SHALL*** create a software distribution package master copy containing configuration files, installation programs, and third party software to be installed on voting equipment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

This requirement establishes the software distribution package master copy that supports traceability of configuration files, installation programs, and third party software to be installed on voting equipment back to the VSTL. Requirement **1.3.2-A.2** requires software distribution package master copies to be on unalterable media. Requirement **1.3.2-F** requires digital signatures for each software component contained in the software distribution package. Requirement **1.3.2-A.2** requires VSTLs to retain software distribution package master copies until notified by the EAC.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.3.1 and 5.6.3.3*

*Impact:* *This requirement differs from the requirements found in Section 5.6.3.1 and 5.6.3.3 of the EAC Testing and Certification Program Manual [EAC 2007] by using a digital signature instead of a "file signature" which could be a hash value or digital signature; and extends the requirements by including configuration files and third party software*

→ **9.3.4-C** VSTL software distribution packages for vendors, NSRL, and EAC requirement

The VSTL ***SHALL*** provide copies of the software distribution packages containing the source and executable code from the witness build, build environment pre- and post-build binary images, and other software to be installed on voting equipment (configuration files, installation programs, and third party software) to the vendor, NSRL, or a designated national respository.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

This requirement requires VSTLs to provide a complete copy of the voting system software to the vendor, the national certification authority, and NSRL. Copies of software distribution packages can be distributed on via modifiable media (physically on CD-RWs, memory cards, and hard drives; or electronically via email, FTP, and Websites) since digital signatures are created as part of software distribution packages. (See requirement **1.3.2-F**). When copies of a software distribution package are created, requirement **1.3.2-A.3** requires a record to be produced.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.4-D** VSTL software distribution packages for other parties

The VSTL ***SHALL*** provide copies of the software distribution packages containing a complete set or subset the source and executable code from the witness build, build environment pre- and post-build binary images, and other software to be installed on voting equipment (configuration files, installation programs, and third party software) to parties approved by the vendor.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

This requirement allows VSTLs to provide complete or partial copies of the voting system software to parties approved by the vendor. Copies of software distribution packages can be distributed on via modifiable media (physically on CD-RWs, memory cards, and hard drives; or electronically via email, FTP, and Websites) since digital signatures are created as part of software distribution packages. (See requirement **1.3.2-F**). When copies of a software distribution package are created, requirement **1.3.2-A.3** requires a record to be produced.

*Source:* *EAC Testing and Certification Program Manual [EAC 2007], Section 5.6.2.4, 5.6.3.2, 5.7.1-5*

*Impact:* *This requirement extends the requirements found in Section 5.6.2.4, 5.6.3.2, and 5.7.1-5 of the EAC Testing and Certification Program Manual [EAC 2007] by requiring configuration files and third party software; providing the software distribution packages to the vendor, EAC, and NSRL as opposed on unnamed repositories; and differs by using a digital signatures instead of a "file signatures" which could be hash values or digital signatures*

## 9.3.5 Repository Software Distribution Packages

→ **9.3.5-A** Repository software distribution package request process documentation requirement

The repository ***SHALL*** publicly document the process used to request copies of the software distribution packages (including associated documentation) from the repository.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1(Review of documentation)*

D I S C U S S I O N

Vendor approval may be required for release for software considered in intellectual property and needs to be reflected in the request process. Copies of software distribution packages can be distributed on via modifiable media (physically on CD-RWs, memory cards, and hard drives; or electronically via email, FTP, and Websites) since digital signatures are created as part of software distribution packages. (See requirement **1.3.2-F**). When copies of a software distribution package are created, requirement **1.3.2-A.3** requires a record to be produced.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Source*

→ **9.3.5-B** Repository digital signature verification requirement

The repository ***SHALL*** verify the digital signatures associated with software are valid before creating a software distribution package master copy containing the software.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

In general, the digital signatures verified by repositories will be generated by VSTLs, the national certification authority, and jurisdictions.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.3.5-B.1** Repository digital signature verification result record requirement

Results of digital signature verifications including the source of the signature ***SHALL*** be part of the creation record of software distribution package master copies created by the repository.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.5-C** Repository software distribution package requirement

Distribution, escrow, and notary repositories ***SHALL*** create software distribution package master copies containing software received from VSTLs, the national certification authority, and jurisdictions.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

Distribution, escrow, and notary repositories received software distribution packages created by VSTLs, the national certification authority, and jurisdictions. This requirement establishes software distribution package master copies that support traceability of voting system software back to the repository. See Section 1.2.2 for a description services provided by repositories. Requirement **1.3.2-A.2** requires software distribution package master copies to be on unalterable media. Requirement **1.3.2-F** requires digital signatures for each software component contained in the software distribution package. Requirement **1.3.2-A.2** requires repositories to retain software distribution package master copies until notified by the the national certification authority.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.5-D** Notary repositories software integrity information software distribution package requirement

Notary repositories ***SHALL*** create software distribution package master copies containing software reference integrity generated by the repository for software received from VSTLs, the national certification authority, and jurisdictions.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

This requirement establishes software distribution package master copies that support traceability of software integrity information for voting system software back to the notary repository. Requirement xx in Setup Validation requires notary repositories to create a software distribution package master copy containing the software reference information they generate for voting system software. See Section 1.2.2 for a description services provided by repositories. Requirement **1.3.2-A.2** requires software distribution package master copies to be on unalterable media. Requirement **1.3.2-F** requires digital signatures for each software component contained in the software distribution package. Requirement **1.3.2-A.2** requires repositories to retain software distribution package master copies until notified by the the national certification authority.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.5-E** Distribution and escrow repository software distribution package copy requirement

A distribution or escrow repository ***SHALL*** provide copies of the software distribution packages they create to parties that follow the repositories request process (see requirement **1.3.5-A**).

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

This requirement allows distribution and escrow repositories to provide the software distribution package they create to parties that follow the request process documented by requirement **1.3.5-A**. Vendor approval may be required for release for software considered in intellectual property and needs to be reflected in the request process of the distribution and escrow repository. Copies of software

distribution packages can be distributed on via modifiable media (physically on CD-RWs, memory cards, and hard drives; or electronically via email, FTP, and Websites) since digital signatures are created as part of software distribution packages. (See requirement **1.3.2-F**). When copies of a software distribution package are created, requirement **1.3.2-A.3** requires a record to be produced.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.5-F** Notary repository software distribution package copy requirement

A notary repository ***SHALL*** provide copies of software distribution packages containing software integrity information generated by the repository to parties that follow the repository's request process (see requirement **1.3.5-A**).

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

This requirement allows notary repositories to provide the software integrity information they create for voting system software to parties that follow the request process documented by requirement **1.3.5-A**. Copies of software distribution packages can be distributed on via modifiable media (physically on CD-RWs, memory cards, and hard drives; or electronically via email, FTP, and Websites) since digital signatures are created as part of software distribution packages. (See requirement **1.3.2-F**). When copies of a software distribution package are created, requirement **1.3.2-A.3** requires a record to be produced.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

## 9.3.6 Jurisdiction Software Distribution Packages

→ **9.3.6-A** Election specific software distribution package requirement

The jurisdiction ***SHALL*** create a software distribution package master copy containing election specific software such as ballot definition files.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

This requirement establishes software distribution package master copies that support traceability of election specific software back to the jurisdiction. Requirement **1.3.2-A.2** requires software distribution package master copies to be on unalterable media. Requirement **1.3.2-F** requires digital signatures for each software component contained in the software distribution package.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.6-B** Installation software distribution package requirement

The jurisdiction ***SHALL*** create a software distribution package master copy containing installation software used to install software on voting equipment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

This requirement establishes software distribution package master copies that support traceability of installation software used to install software on voting equipment back to the jurisdiction. Requirement **1.3.2-A.2** requires software distribution package master copies to be on unalterable media. Requirement **1.3.2-F** requires digital signatures for each software component contained in the software distribution package.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.3.6-C** Jurisdictionally altered software distribution package requirement

The jurisdiction ***SHALL*** create a software distribution package master copy containing voting system software altered to meet jurisdictional requirements and has passed jurisdictional testing and certification.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

This requirement establishes software distribution package master copies that support traceability of jurisdictionally altered voting system software back to the jurisdiction. Requirement **1.3.2-A.2** requires software distribution package master copies to be on unalterable media. Requirement **1.3.2-F** requires digital signatures for each software component contained in the software distribution package.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **9.3.6-D** Jurisdiction software distribution packages copy requirement

The jurisdiction ***SHALL*** provide copies of the software distribution packages created by the jurisdiction to repositories and other jurisdictions as required by the jurisdiction.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

D I S C U S S I O N

See Section 1.3.2 requirements related to copies of software distribution packages.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

## 9.4 Software Installation Requirements

➞ **9.4-A** Software list user documentation requirement

Vendors ***SHALL*** provide a list of all software to be installed on voting equipment in the user documentation.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1(Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *This requirement is related to requirement **3.1.1-A (h)** of VVSG 2007 Volume IV but does not include documentation associated with the software or the directory listing (which is captured by requirement **1.3.1.2-A.2**); his requirement is a generalization of the requirement found at Section **2.4.5.2-A** and **C** of Volume IV of VVSG 2007 by focusing on all software to be installed on voting equipment and not just operating systems and COTS runtime environments*

↳ **9.4-A.1 2**Election specific software identification user documentation requirement

Vendors ***SHALL*** identify election specific software in the user documentation.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **9.4-B** Installation software and hardware user documentation requirement

Vendors ***SHALL*** provide a list of software and hardware required to install software on voting equipment in the user documentation.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1(Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **9.4-C** Software installation procedure user documentation requirement

Vendors ***SHALL*** document the procedures used to install software on voting equipment in user documentation.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation); Functional Test performed as part of Requirement **1.4-H***

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume III, Section 2.2.3(a)*

*Impact:* *This requirement generalized the requirement found in Section 2.2.3(a) of VVSG 2005 Volume III by not distinguishing between*

*software related to ballots or the general voting application; this requirement is related to requirement **3.1.1-A (h)** of VVSG 2007 Volume IV specifically the order in which the software is installed; extends the requirement by requiring the documentation of the software installation procedure; this requirement supercedes requirement **3.3.4** of VVSG 2007 Volume IV*

↳ **9.4-C.1** No compiler installation requirement

The procedures used to install software on voting equipment ***SHALL*** result in no compilers being installed on voting equipment.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation); Functional Test performed as part of Requirement **1.4-H***

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.4-C.2** Voting equipment configuration baseline binary image creation requirement

To replicate voting equipment configurations, the procedures ***SHALL*** create a baseline binary image of the initial voting equipment configuration on an unalterable storage media with a digital signature.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

Unalterable storage media includes technology such as a CD-R, but not CD-RW.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.4-C.3** Voting equipment configuration replication requirement

The procedures ***SHALL*** use the baseline binary image of the initial voting system configuration on an unalterable storage media (See requirement **1.4-C.2**) to replicate the voting equipment configuration on other voting equipment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

Unalterable storage media includes technology such as a CD-R, but not CD-RW.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.4-D** Software installation record creation requirement

A software installation record ***SHALL*** be created that includes at a minimum: a unique identifier (such as a serial number) for the record; a list of unique identifiers of unalterable storage media associated with the record; the time, date, and location of the software installation; names, affiliations, and signatures of all people present; copies of the procedures used to install the software on the voting equipment; the certification number of the voting system; list of the software installed on the voting equipment; and a unique identifier (such as a serial number) of the voting equipment on which the software is installed.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1(Review of documentation)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.4-E** Software installation mode restriction requirement

Voting systems ***SHALL*** only allow software to be installed while the voting equipment is in pre-voting mode.

*Applies to:* *Programmed Device, EMS*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

See Section X: Access Control for modes specified for voting systems.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.4-F** Software installation individual authentication requirement

Voting systems ***SHALL*** authenticate the individual(s) installing software before allowing software to be placed on the voting equipment.

*Applies to:* *Programmed Device, EMS*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

See Section X: Access Control for requirements related to authentication.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.4-F.1** Software installation administrator group or role requirement

Voting systems ***SHALL*** only allow authenticated administrators to install software on voting equipment.

*Applies to:* *Programmed Device, EMS*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

See Section X: Access Control for groups and roles specified for voting systems. The access control section requires individuals with the administrator group or role to be authenticated using two-factor authentication (such as a smartcard and password).

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.4-F.2** Software installation central election official group or role requirement

Voting systems ***SHALL*** only allow authenticated central election officials to only install election specific software and data files on voting equipment.

*Applies to:* *Programmed Device, EMS*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

See Section X: Access Control for groups and roles specified for voting systems. The access control section requires individuals with the central election official group or role to be authenticated using at a minimum a username and password.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.4-G** Software installation procedures usage documentation requirement

Software on voting equipment ***SHALL*** only be able to be installed using the procedures in the user documentation.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Requirement **1.4-C** requires vendors to document the procedures used to install software on voting equipment

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.4-H** Procurement of voting system software requirement

Voting system software to be installed on voting equipment ***SHALL*** be obtained from VSTLs or distribution repositories.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

See Section 1.2.2 for a description services provided by repositories.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.4-I** Open market procurement of third party software requirement

Third party software to be installed on voting equipment ***SHALL*** be obtained from the open market.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *This requirement is related to requirement **3.1.1-C** of VVSG 2007 Volume IV but does not specifically require a "certification" of the procurement from the manufacturer, licensed dealer, or distributor; this requirement supercedes requirement **2.5.2.3-B** of VVSG 2007 Volume V and uses the term third party software instead of the term COTS,*

→ **9.4-J** Software digital signature verification requirement

A VSTL, NSRL, or notary repository digital signature associated with the software ***SHALL*** be successfully validated before placing the software on voting equipment.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

This requirement checks that software is an unaltered version of the software traceable back to a VSTL, NSRL, or notary repository.

*Source:* *Click here to add the Source*

*Impact:* *This requirement is related to requirement **3.1.1-C (h)** of VVSG 2007 Volume IV titled "User doc, traceability of procured software" by using digital signatures to provide traceability but does not distinguish between third party and vendor developed software*

↳ **9.4-J.1** Software installation programs digital signature verification requirement

Software installation programs ***SHALL*** validate a VSTL, NSRL, or notary repository digital signature of the software before installing software on the voting equipment.

*Applies to:* *Programmed Device, EMS*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.4-J.2** Software digital signature verification record requirement

The results of digital signature verifications including who generated the signature ***SHALL*** be part of the software installation record.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.4-K** Erasable storage media preparation requirement

Any previously stored information on erasable storage media of voting equipment ***SHALL*** be removed from the media before installing software on the media.

*Applies to:* *Programmed Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

The purpose of this requirement is to prepare erasable storage media for use by the voting equipment. The requirement does not require the prevention of previously stored information leakage or recovery. Simply deleting files from file systems, flashing memory cards, and removing electrical power from volatile memory satisfies this requirement.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.4-L** Installation media digital signature requirement

Installation media used to install software on voting equipment ***SHALL*** only contain software with digital signatures from the national certification authority, NSRL, jurisdiction, or notary repository.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.4-M** Installation media unalterable storage media requirement

Unalterable storage media ***SHALL*** be used to install software on voting equipment.

*Applies to:* *Programmed Device*

*Test Reference:* *N/A*

DISCUSSION

Unalterable storage media includes technology such as a CD-R, but not CD-RW.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.4-N** Software installation error alert media requirement

When installation of software fails, voting systems ***SHALL*** provide an externally visible error message identifying the software that has failed to be installed on the voting equipment.

*Applies to:* *Programmed Device, EMS*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

See Section **4.1.4** for additional requirements related to error messages.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **9.4-O** Voting system software installation logging requirement

Voting systems ***SHALL*** be able to log at a minimum the following information associated with each piece of software installed: who installed the software including their group or role, the date and time of the installation; the

software's filename and version; the location where the software is installed (such as directory path or memory addresses); if the software was installed successfully or not; and the digital signature validation results including who generated the signature.

*Applies to:* *Programmed Device, EMS*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

See Section X: System Event Logging for requirements related to logging systems of voting equipment.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **9.4-P** Voting system configuration file(s) access requirement

Voting systems ***SHALL*** authenticate the individual(s) before allowing access to voting system configuration file(s).

*Applies to:* *Programmed Device, EMS*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

See Section X: Access Control for requirements related to authentication.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.4-P.1** Configuration file administrator group or role requirement

Voting systems ***SHALL*** only allow authenticated administrators to access and modify voting equipment configuration files.

*Applies to:* *Programmed Device, EMS*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

See Section X: Access Control for groups and roles specified for voting systems.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.4-P.2** Configuration file central election official group or role requi

Voting systems ***SHALL*** only allow authenticated central election officials to only access and modify election specific configuration files.

*Applies to:* *Programmed Device, EMS*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

See Section X: Access Control for groups and roles specified for voting systems.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.4-P.3** Configuration file access authentication requirement

For each configuration file to be accessed, voting systems ***SHALL*** perform an authentication of the individual attempting to access the configuration file.

*Applies to:* *Programmed Device, EMS*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **9.4-P.4** Configuration file access logging requirement

Voting systems ***SHALL*** be able to log at a minimum the following information associated with configuration file accesses: who accessed the configuration file including their group or role, the date and time of the access; the configuration file's filename; an indication of the configuration file was modified; and the location of the configuration file (such as directory path or memory addresses).

*Applies to:* *Programmed Device, EMS*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

See Section X: System Event Logging for requirements related to logging systems of voting equipment.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

## 9.5 References

[VVSG 2005] 2005 Voluntary Voting System Guidelines, Election Assistance Commission

[Berger1] Memorandum from Stephen Berger, Subject: Project Plan for Development of a Trusted Software Delivery and Verification System, April 14, 2006

[Berger2] Memorandum from Stephen Berger, Subject: Delivery and Validation of Trusted Software, April 24, 2006

[EAC 2007] Election Assistance Commission, Testing and Certification Program Manual, version 1.0, January 1, 20077

# Chapter 10: Access Control

## 10.1 Introduction/Scope

The purpose of access controls is to limit the rights of authorized users, systems, applications, or processes and prevent unauthorized use of a resource or use of a resource in an unauthorized manner. The core components of access control include identification, authentication, enforcement, and policy. Access control mechanisms authenticate, authorize, and log access to resources to protect voting system integrity, availability, confidentiality, and accountability. The intent of the standard is that access controls should provide reasonable assurance that voting system resources such as data files, application programs, underlying operating systems, and voting system equipment are protected against unauthorized access, operation, modification, disclosure, loss, or impairment.

This section addresses documentation and voting system capabilities that limit and detect access to critical voting system components in order to guard against loss of system and data integrity, availability, confidentiality, and accountability in voting systems. Access controls may be implemented in the voting software or provided by the underlying operating system or separate application programs.

Access controls include physical controls, such as keeping voting devices in locked rooms to limit physical access, and technical controls, such as security software programs designed to prevent and detect unauthorized access to resources. The access controls contained in this section address security software programs; see Section X, Physical Security for further information on physical and hardware security for voting systems.

## 10.2 Access control requirements

This subsection defines the access control requirements for voting systems. It outlines the various measures that the vendors and the voting system shall perform to ensure the security of the voting system. These recommendations apply to the full scope of voting system functionality, including functionality for defining the ballot and other pre-voting functions, as well as functions for casting and storing votes, vote reporting, system logging, and maintenance of the voting system

### 10.2.1 General access control requirements

General requirements address the high level functionality of a voting system. These are the fundamental access control requirements upon which other requirements in this section are based.

➞ **10.2.1-A** Access control mechanisms requirement

The voting system ***SHALL*** provide access control mechanisms designed to permit authorized access to the voting system and to prevent unauthorized access to the voting system.

*Applies to:* *Voting device*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Access controls support the following security principles in terms of voting systems:

- Confidentiality of casting and storing of votes and voter anonymity.
- Integrity of event logs, electronic records, and vote reporting.
- Availability of the voting ballot and the ability to cast, store, and report votes.
- Accountability of actions by identifying and authenticating users.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring access control mechanisms.*

➞ **10.2.1-B** Access control for software and files requirement

The voting system ***SHALL*** provide controls that permit or deny access to voting system software and files as well as third party software and files.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Third party software and files include the operating system, drivers, databases, etc.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring controlled access to voting system components.*

➞ **10.2.1-C** Access control states requirement

The voting system access control mechanisms ***SHALL*** distinguish at least the following states: pre-voting, activated, suspended, and post-voting.

*Applies to:* *Vote-capture device*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

See Section 9.2 Vote-capture Device State Model. The various states and their relation to access control are described in Table 1 Voting System States.

*Source:* *VVSG 2005 Volume I, Section 7.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2 by establishing voting system states in relation to access control.*

| STATE | DESCRIPTION |
|---|---|
| Pre-voting | This state includes activities that occur prior to voting, such as loading the ballot definition. This state may enter Activated state. |
| Activated | This state includes voting activities such as casting, printing, or spoiling a ballot. This state may enter Suspended state or Post-voting state. |
| Suspended | This state suspends voting activities when entered from the Activated state by an authorized voting official for reasons such as off hours during early voting. To resume voting activities an authorized voting official exits this state and enters the Activated state. |
| Post-voting | This state includes activities that occur after voting, such as ballot counting and reporting. An authorized voting official enters this state from the Activated state. |

Table 10-3 Voting System States

➞ **10.2.1-D** Access control state creation requirement

The voting system ***SHALL*** allow the administrator group or role to create additional states.

*Applies to:* *Vote-capture device*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2 by permitting the creation of additional voting system states in relation to access control.*

→ **10.2.1-E** Access control state functions requirement

The voting system ***SHALL*** allow the administrator group or role to configure access control functions available in each state.

*Applies to:* *Vote-capture device*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2 by establishing voting system functions for each state in relation to access control.*

→ **10.2.1-F** Different access control for voting system states requirement

The voting system ***SHALL*** apply different access controls for each state.

*Applies to:* *Vote-capture device*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Activated state should offer a strict subset of functions limited to voting only. Pre-voting and Post-voting states and other defined states may be used for other functions such as defining the ballot, collecting votes, updating software, and performing other administrative and maintenance functions. For more examples see Table 3, Roles and States Access Matrix.

*Source:* *VVSG 2005 Volume I, Section 7.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2 by permitting access control flexibility for each voting system state of operation.*

→ **10.2.1-G** One cast ballot per voting session requirement

In Activated state, the voting system ***SHALL*** enforce that only one ballot is cast within the voting session.

*Applies to:* *Vote-capture device*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Within the Activated state a voting session is defined as the period of time between ballot activation and printing, casting, or spoiling a ballot. For more see Section 9.2 Vote-capture Device State Model.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.1 (c)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.1 (c) by requiring only one cast ballot per voting session.*

→ **10.2.1-H** Least privilege requirement

The voting system ***SHALL*** implement the least privilege principle for default access control permissions.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring least privilege access control permissions.*

→ **10.2.1-I** Privilege escalation requirement

The voting system ***SHALL*** prevent a lower-privilege process from modifying a higher-privilege process.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume II, Section 6.4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1 by preventing unauthorized process modification.*

➞ **10.2.1-J** Privileged operations requirement

The voting system ***SHALL*** ensure that an administrator authorizes each privileged operation.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume II, Section 6.4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2 by requiring authorization of privileged operations.*

## 10.2.2 Access control documentation requirements

Documentation requirements address the minimum access control information necessary for testing and implementation of the voting system. This includes both public and private information. User documentation includes all public information that is provided to the end users. The Technical Data Package (TDP) includes the user documentation along with other private information that is viewed only by the test labs.

➞ **10.2.2-A** General user and TDP documentation requirement

Vendors ***SHALL*** provide user and TDP documentation of access control capabilities of the voting system.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring user and TDP documentation for voting system access control capabilities.*

→ **10.2.2-B** Access control implementation, configuration, and management user documentation requirement

Vendors ***SHALL*** provide user documentation containing guidelines and usage instructions on implementing, configuring, and managing access control capabilities.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by providing examples of user documentation components.*

→ **10.2.2-C** Access control policy template user documentation requirement

Vendors ***SHALL*** provide, within the user documentation, an access control policy template or instructions to facilitate the implementation of the access control policy and associated access controls on the voting system.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

Access control policy requirements include the minimum baseline policy definitions necessary for testing and implementation of the voting system. The policies may be pre-defined within the voting system or provided as guidelines in the documentation.

*Source:* *VVSG 2005 Volume I, Section 7.2.1*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.2.1 by requiring an access control policy template.*

→ **10.2.2-D** Model access control policy user documentation requirement

Vendors ***SHALL*** provide, within the user documentation, a model access control policy under which the voting system was designed to operate and a description of the hazards of deviating from this policy.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

The model access control policy includes the assumptions that were made when the system was designed, the justification for the policy, and the hazards of deviating from the policy.

*Source:* *VVSG 2005 Volume I, Section 7.2.1*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.2.1 by requiring a model access control policy.*

→ **10.2.2-E** General access control technical specification TDP documentation requirement

Vendors ***SHALL*** provide descriptions and specifications of all access control mechanisms of the voting system including management capabilities of authentication, authorization, and passwords in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.4*

D I S C U S S I O N

Access control mechanisms include those that are designed to permit authorized access to the voting system and prevent unauthorized access to the voting system. Specific examples of access control measures include but are not limited to: Use of data and user authorization, security kernels, computer-generated password keys, and special protocols.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by providing examples of TDP documentation components.*

➞ **10.2.2-F** Unauthorized access technical specification TDP documentation requirement

Vendors ***SHALL*** provide descriptions and specifications of methods to prevent unauthorized access to the access control mechanisms of the voting system in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.4*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring the TDP to include information on methods to restrict access to the access control mechanisms.*

➞ **10.2.2-G** Access control dependant voting system mechanisms TDP documentation requirement

Vendors ***SHALL*** provide descriptions and specifications of all other voting system mechanisms that are dependent upon, support, and interface with access controls in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.4*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring the TDP to include information on any other voting system mechanisms that interoperate with voting system access control.*

## 10.2.3 Access control identification requirements

Identification requirements provide controls for accountability when operating and administering a voting system. Identification applies to users, systems, applications, and processes.

→ **10.2.3-A** Access control identification requirement

The voting system ***SHALL*** identify users, systems, applications, and processes to which access is granted and the specific functions and data to which each entity holds authorized access. Identification ***SHALL*** be performed using identity-based or role-based methods.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Identity-based identification explicitly identifies a user, system, application, or process by the use of a unique system-wide identifier. Each identity has defined permissions in the voting system. Accountability is provided for each identity within the voting system. In this scenario, voters must remain anonymous and be identified through a double or triple blind generation process. Role-based identification identifies users, systems, applications, and processes based on roles in an organization. Each role has defined permissions within the voting system. Users authenticate to the voting system then assume a role. Accountability is provided for each user and assumed role within the voting system. Voters remain anonymous through the use of a generic voter role. Identity-based and role-based access control methods both use rules to define permissions. Rules may be used in a voting system to provide access policies for either identity-based or role-based access control.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.1 (a)*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.2.1.1 (a) by requiring that they voting system identify systems, applications, and processes, in addition to users. It also requires that identification uses either identity-based or role-based methods.*

→ **10.2.3-B** Role-based access control standard requirement

Voting systems that implement role-based access control ***SHALL*** follow the standards and recommendations outlined in the *ANSI INCITS 359-2004 American National Standard for Information Technology – Role Based Access Control* document.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.1 (a)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.1 (a) by requiring role-based methods to follow ANSI INCITS 359-2004.*

➞ **10.2.3-C** Access control roles identification requirement

The voting system ***SHALL*** identify, at a minimum, the categories for groups or roles outlined in Table 2. These categories ***SHALL*** be identified by identity-based or role-based methods. Each category may apply to different states and perform different functions.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

A group in a voting system is defined as a set of users, systems, applications, or processes who share the same set of privileges and access permissions. In role-based access control methods a role serves the same purpose as a group. In identity-based access control methods groups are created, members are assigned to the groups, and permissions and privileges are applied to the group as a whole. The term groups and roles are often used interchangeably.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.1 (a)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.1 (a) by establishing minimum group or role categories. It also allows each category to apply to different states of operation and perform different functions.*

➞ **10.2.3-D** Group member identification requirement

Members within all groups except the voter group ***SHALL*** be identified individually and explicitly.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 4.4*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.1 (a)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.1 (a) by requiring members of groups to be identified explicitly, while maintaining voter anonymity.*

| GROUP OR ROLE | DESCRIPTION |
|---|---|
| Voter | The voter can only cast or cancel a ballot. The voter cannot activate a session; the poll worker activates the session by checking in the voter and activating the ballot format. Members of this group or role are not identified since voters must remain anonymous. |
| Election Judge | The election judge has the ability to open the polls, close the polls, and generate reports. |
| Poll Worker | The poll worker checks in voters and activates the ballot format. |
| Central Election Official | The central election official loads ballot definitions. |
| Administrator | The administrator updates and configures the system and troubleshoots system problems. |
| System | The system includes applications and processes at interact with the voting system. |

Table 10-4 Voting System Groups/Roles and Descriptions

➞ **10.2.3-E** Access control configuration requirement

The voting system ***SHALL*** allow the administrator group or role to configure the permissions and functionality for each identity, group or role, to include account and group/role creation, modification, and deletion.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Each group/role may or may not have permissions for every state. Additionally the permissions that a group/role has for a state may be restricted to certain functions. Table 3 shows an example matrix of group or role to state access rights.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.1 (a)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.1 (a) by allowing configuration flexibility for permissions and functionality for each identity, group, or role.*

| ROLE/STATES | PRE-VOTING | ACTIVATED | SUSPENDED | POST-VOTING |
|---|---|---|---|---|
| VOTER | N/A | Cast and cancel ballots | N/A | N/A |
| ELECTION JUDGE | Open polls | Close polls | Enter and Exit suspended state | Generate reports |
| POLL WORKER | N/A | Activate ballot format | N/A | N/A |
| CENTRAL ELECTION OFFICIAL | Define and load ballot | Handle fled voters and recover from errors | N/A | N/A |
| ADMINISTRATOR | Full access | Full access | Full access | Full access |
| SYSTEM | Custom per application or process | Custom per application or process | Custom per application or process | Custom per application or process |

Table 10-5 Roles and States Access Matrix

→ **10.2.3-F** Voter anonymity preservation requirement

The voting system ***SHALL*** preserve voter anonymity.

*Applies to:* *Vote-capture device*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

The voting system must not link the voter authorization with the vote cast.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.1*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.1 by requiring voter anonymity in regards to access control.*

## 10.2.4 Access control authentication requirements

Authentication establishes the validity of the identity of the user, system, application, or process interacting with the voting system. Authentication is based on the identification provided by the user, system, application, or process interacting with the voting system. Authentication is generally classified in one of the following three categories:

(a) Something the user knows – This is usually a password, pass phrase, or PIN.

(b) Something the user has – This is usually a security token that may be either hardware or software based, such as a smart card.

(c) Something the user is – This is usually a fingerprint, retina patter, voice pattern or other biometric data.

Traditional password authentication is a single factor authentication method. A more secure method of authentication combines the various methods of authentication into two-factor authentication, or multi-factor authentication. For example, a user may use a security token and a passphrase for authentication. Using multi-factor provides stronger authentication than single factor. There are also cryptographic-based authentication methods such as digital signatures and challenge-response authentication which are either software based or security tokens.

→ **10.2.4-A** Minimum authentication mechanism requirement

The voting system ***SHALL*** authenticate users, systems, applications, and processes using at a minimum PIN or activation code.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Table 4 provides the minimum authentication methods required for each group or role. Stronger authentication methods than the minimum may be used for each group or role.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (e) by requiring a minimum level of robustness for user authentication mechanisms.*

→ **10.2.4-B** Multiple authentication mechanism requirement

The voting system ***SHALL*** provide multiple authentication methods to support multi-factor authentication.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

This requirement is needed to support the multi-factor authentication of the administrator group or role of requirement 1.2.4-C. Multi-factor authentication

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (e) by requiring multi-factor authentication mechanisms.*

→ **10.2.4-C** Administrator group or role multi-factor authentication requirement

The voting system ***SHALL*** authenticate the administrator group or role with a multi-factor authentication mechanism.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (e) by requiring multi-factor authentication for the voting system administrator group or role.*

| GROUP OR ROLE | MINIMUM AUTHENTICATION METHOD |
|---|---|
| Voter | Pin or activation code |
| Election Judge | User name and password |
| Poll Worker | N/A – poll worker does not authenticate to voting system |
| Central Election Official | User name and password |
| Administrator | Two-factor authentication |
| System | User name and password |

Table 10-6 Minimum Authentication Methods for Groups and Roles

→ **10.2.4-D** Prohibition of hard coded authentication data requirement

Voting system software ***SHALL*** not contain hard coded authentication data.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 4.4*

DISCUSSION

Authentication data includes passwords, passphrases, and private keys.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (a)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (a) by prohibiting hard coded authentication data on the voting system.*

→ **10.2.4-E** Secure storage of authentication data requirement

When private or secret authentication data is stored in the voting system, it ***SHALL*** be protected to ensure that the privacy and secrecy is not violated.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Ensuring the privacy and secrecy of stored data may involve the use of encryption.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (g)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (g) by requiring securely stored private or secret authentication data.*

→ **10.2.4-F** Setting and changing of passwords, pass phases, and keys requirement

The voting system ***SHALL*** allow the administrator group or role to set and change passwords, pass phrases, and keys.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

This requirement support jurisdictions have different policies regarding passwords, pass phrases, and keys.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (e) by allowing the administrator group or role flexibility in creation and modification of passwords, pass phrases, and keys.*

→ **10.2.4-G** Creation and disabling of privileged accounts requirement

The voting system ***SHALL*** allow privileged accounts to be disabled and allow new individual privileged accounts to be created.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Privileged accounts include any accounts within the operating system, voting system software, or other third party software with elevated privileges such as administrator, root, maintenance accounts, etc.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by allowing the creation of and disabling of privileged accounts.*

→ **10.2.4-H** Privileged account user documentation requirement

The vendor ***SHALL*** disclose and document information on all privileged accounts included on the voting system.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1*

DISCUSSION

Information on privileged accounts include the name of the account, purpose, capabilities and permissions, and how to disable the account in the user documentation.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring the disclosure of privileged accounts and related information.*

→ **10.2.4-I** Account lock out requirement

The voting system ***SHALL*** lock out users, applications, or processes after a specified number of consecutive failed access attempts within a pre-defined time period.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring account lockout after a specified number of consecutive failed access attempts.*

→ **10.2.4-J** Account lock out configuration requirement

The voting system ***SHALL*** allow the administrator group or role to configure the account lock out policy including the time period within which failed attempts must occur, the number of consecutive failed access attempts allowed before lock out, and the length of time the account is locked out.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by allowing the administrator group or role flexibility in configuring the account lockout policy.*

→ **10.2.4-K** Account lock out application requirement

The voting system ***SHALL*** allow the administrator group or role to apply account lock out policies to specified accounts.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by allowing the administrator group or role flexibility in applying the account lockout policy.*

→ **10.2.4-L** User name and password management requirement

If the voting system uses a user name and password authentication method, it ***SHALL*** allow the administrator to enforce password strength, histories, and expiration.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (e) by requiring strong passwords, password histories, and password expiration.*

↳ **10.2.4-L.1** Password strength configuration requirement

The voting system ***SHALL*** allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per *NIST 800-63 Electronic Authentication Guideline* standards.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (e) by allowing the administrator group or role flexibility in configuring password strength. It also requires the use of NIST 800-63 standards.*

↳ **10.2.4-L.2** Common word usage for password configuration requirement

The voting system ***SHALL*** restrict the use of common words for passwords.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (e) by restricting common words in passwords.*

↳ **10.2.4-L.3** Password history configuration requirement

The voting system ***SHALL*** enforce password histories and allowing the administrator to configure the history length.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (e) by allowing the administrator group or role flexibility in configuring password history.*

↳ **10.2.4-L.4** Account information for password restriction requirement

The voting system ***SHALL*** ensure that the username or other associated information is not used in the password.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (e) by restricting the use or usernames and related information in passwords.*

↳ **10.2.4-L.5** Automated password expiration requirement

The voting system ***SHALL*** provide a means to automatically expire unchanged passwords in accordance with the voting jurisdiction's policies.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (e) by requiring the expiration of unchanged passwords.*

↳ **10.2.4-L.6** Password expiration warning requirement

The voting system ***SHALL*** provide users advance warning that their passwords are going to expire if they are not changed.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (e) by requiring advanced warning or password expiration to users.*

↳ **10.2.4-L.7** Length of time between password change and advance warning configuration requirement

The voting system ***SHALL*** permit system administrators to specify the length of time between password changes and the length of advance warning provided to users to change passwords.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (e) by allowing the administrator group or role flexibility in configuration of password expiration and warnings.*

➞ **10.2.4-M** Security token management requirement

If the voting system uses security tokens for authentication, it ***SHALL*** allow the administrator to program and reset the security token.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by including the use of security tokens and allowing the administrator group or role flexibility in configuring the security token.*

↳ **10.2.4-M.1** Mutual authentication between security token and voting device requirement

The voting system ***SHALL*** provide mutual authentication between the security token to the voting device.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring mutual authentication of the security token and the voting device.*

↳ **10.2.4-M.2** Security token encryption requirement

The voting system ***SHALL*** encrypt the contents on the security tokens.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Contents of the security token include the private keys.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (g)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (g) by requiring encryption of security token contents.*

↳ **10.2.4-M.3** Security token elevated access requirement

The voting system ***SHALL*** support an administrator security token that allows elevated access privileges.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Elevated access privileges include changing states and ending the election.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring the support of an administrator security token.*

↳ **10.2.4-M.4** Security token personal identification number (PIN) requirement

The voting system ***SHALL*** enable a personal identification number (PIN) on security tokens.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring the use of a security token PIN.*

↳ **10.2.4-M.5** Voter security token one time use requirement

The voting system ***SHALL*** reset the voter security token to ensure that it can only be used for a single voting session.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring the ability to reset voter security tokens for each use.*

↳ **10.2.4-M.6** Voter security token functionality limit requirement

The voting system ***SHALL*** deny voter security tokens access to any functions beyond casting or spoiling a vote.

*Applies to:* *Vote-capture device*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by restricting the use of security token functionality to casting or spoiling a vote.*

→ **10.2.4-N** Voter mutual authentication requirement

The voting system ***SHALL*** provide mutual authentication between the voter and the voting device.

*Applies to:* *Voting device*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Voters may be authenticated via smartcard, token, pin, or access code.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (e)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (e) by requiring mutual authentication between the voter and the voting device.*

## 10.2.5 Access control authorization requirements

Authorization is the process of determining access rights based on authentication of a user, system, application, or process within a voting system. Authorization permits or denies access to an object by a subject. Subjects may be users, systems, applications, or processes that interact with the voting system. Objects may be files or programs within the voting system.

→ **10.2.5-A** Account access to election data authorization requirement

The voting system ***SHALL*** ensure that only authorized accounts have access to election data.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (a)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (a) by restricting access to election data to authorized accounts.*

→ **10.2.5-B** Separation of duties requirement

The voting system ***SHALL*** enforce separation of duty across subjects based on user identity, groups, or roles.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring separation of duty.*

→ **10.2.5-C** Dual person control requirement

The voting system ***SHALL*** provide dual person control for administrative activities.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (a) by requiring dual person control for administrative activities.*

→ **10.2.5-D** Explicit authorization requirement

The voting system ***SHALL*** explicitly authorize subjects' access based on access control lists or policies.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (a)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (a) by requiring explicit authorization of subjects based on access control policies.*

→ **10.2.5-E** Explicit deny requirement

The voting system ***SHALL*** explicitly deny subjects access based on access control lists or policies.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (a)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (a) by requiring explicit denying of subjects access based on access control policies.*

→ **10.2.5-F** Authorization identification requirement

The voting system ***SHALL*** identify each person, application, or process entity to who access is granted (other than voters, who ***SHALL*** be only identified generically), and restrict access to the specific functionality and data to which access is unauthorized.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2 (a)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 (a) by requiring identification-based authorization.*

➞ **10.2.5-G** Authorization limits requirement

The voting system ***SHALL*** limit the length of authorization to a specific time, time interval, or voting state.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.1 (b)*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.1 (b) by requiring limitations on authorization by time or state.*

## 10.2.6 Remote access control enforcement requirements

Voting systems may use telecommunications to communicate between system components and locations. For example, voting systems may communicate on a network to transmit data to a central system. The voting systems may also be accessed remotely for administration and software installation. When using network communications with a voting system, additional security controls should be implemented to protect the data in transit, including authentication and access control information.

➞ **10.2.6-A** Access control for remote access requirement

Voting systems that use network communications between components or other forms of remote access ***SHALL*** be subject to the same access control requirements as standalone voting systems.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring access control for remote access capabilities.*

→ **10.2.6-B** Remote access account, group, and roles restriction requirement

The voting system ***SHALL*** restrict remote access to an administrator subgroup with limited permission and functionality.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by restricting the accounts, groups, or roles that are accessed remotely.*

→ **10.2.6-C** Remote access state restriction requirement

The voting system ***SHALL*** restrict remote access to certain states.

*Applies to:* *Vote-capture device*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

For example, denying remote access functionality during Activated state.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by restricting remote access to certain states.*

→ **10.2.6-D** Remote access strong authentication requirement

The voting system ***SHALL*** apply strong authentication methods over remote access per *NIST 800-63 Electronic Authentication Guideline* standards for Level 4 authentication.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

The *NIST 800-63 Electronic Authentication Guideline* recommends Level 4 authentication to provide the highest practical remote network authentication assurance. Level 4 authentication requires a physical hardware token and is based on proof of possession of the token through a FIPS 140-2 Level 2 or higher cryptographic protocol.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring strong authentication for remote access. It also requires the use of NIST 800-63 standards for Level 4 authentication.*

→ **10.2.6-E** Node-based access control requirement

The voting system ***SHALL*** perform node-based access control and blocking all ports, network interfaces, and other nodes by default.

*Applies to:* *Voting device with operating system*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Node-based access control includes both standard network interfaces and modem communications. This provides a bi-directional firewalling capability. This access control mechanism should passively prohibit, but not reject, unauthorized network communications. Prohibition of the transaction is termination of the network transaction without return communication to the originating host indicating that the communication has been specifically denied. Rejection is an explicit return communication to the initiating computer that the transaction is unauthorized. These return transactions often contain illuminating information about the host or the access control mechanism. Armed with this expanded information, an attacker can evolve their attack to a more educated and specific effort, increasing probability of a successful attack. See NIST Special Publication 800-41 – Guidelines on Firewalls and Firewall Policy [WACK02] for more information on node-based access control.

*Source:* *VVSG 2005 Volume I, Section 7.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2 by requiring node-based access control.*

# Chapter 11: System Integrity Management

## 11.1 Introduction/Scope

This chapter is a guideline for securely deploying and maintaining Voting System electronic devices across all system modes of voting. It is inclusive of platform security configuration including network interfaces. In many ways, security of the electronic devices is subject to the current Voting System mode. Perhaps more importantly, the Voting System mode is an indicator of who requires access to any given device. This factor significantly influences security measures.

There are some similarities between voting machines and gaming machines. As a method of assuring completeness of requirements, the Nevada Gaming Commission's [NGC06] technical standards on gaming machines were consulted for applicability.

## 11.2 System Integrity Management Requirements

### 11.2.1 Error Condition Requirements

Error condition requirements mandate properties of voting system state once an error has occurred, including voting system functionality, security, and error alerting.

➔ **11.2.1-A** Documenting Failure and Resumption Process

Vendors ***SHALL*** document the electronic device failure process inclusive of ramifications to device, application, and ballot security including steps to resume normal functionality.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation); Functional test as part of **1.2.1-B***

D I S C U S S I O N

*Source:* *Volume I, 2.1.1(d)*

*Impact:* *This requirement expands the requirement found at 2.1.1. (d) in Volume I of VVSG 2005 to require vendors to document security ramifications of the Electronic Device failure process.*

→ **11.2.1-B** Compliance with Failure and Resumption Process

Electronic devices ***SHALL*** act in accordance with the vendor-documented failure and resumption process.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

*Source:* *Volume I, 2.1.1(d)*

*Impact:* *This requirement augments the requirement found at 2.1.1. (d) in Volume I of VVSG 2005 by requiring that vendors document failure and resumption process.*

→ **11.2.1-C** Error Message Requirement

When an error occurs, electronic devices ***SHALL*** generate a visual and audio error message including instructions and statements about the current state of the electronic device, user instructions, and explicit confirmation of ballot status for any ballots being processed at the time of failure.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

This requirement ensures that errors are quickly observed and that any public observers receive appropriate assurance of the state of the device.

*Source:* *Volume I, 2.1.5.1(b)ii*

*Impact:* *This requirement augments the requirement found at 2.1.5.1 (b)ii volume I of the VVSG 2005 by mandating explicit confirmation of ballot status in the event a ballot is being processed at time of error and an audio message be generated.*

## 11.2.2 Electronic Device Requirements

Electronic device requirements are minimum safeguards for voting platforms once the platform is deployed.

➞ **11.2.2-A** Protecting Secondary Storage Device Requirement

Electronic devices ***SHALL*** use FIPS validated encryption to protect the firmware, operating system, voting software applications, configuration parameters, temporary and swap files, and data files while the voting system is at rest and not powered.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 4.4 (Inspection of Design)*

D I S C U S S I O N

The non-volatile storage device where the voting system operating system, voting software application, configuration data, and user input data are stored is encrypted to protect against offline attack. If a disk based storage device is used then full disk encryption software or hardware can be implemented to protect the content of the disk drive. See Chapter XX Cryptography for requirements other related to cryptography.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-3*

*Impact:* *New Requirement*

➞ **11.2.2-B** Storage Encryption Failure Recovery Documentation Requirement

As part of the user documentation, vendors ***SHALL*** provide the procedures used to recover and repair an encrypted storage device that is subjected to a physical or software failure.

*Applies to:* *Voting Systems*

*Test Reference:* *Volume V, Section 4.1 (Review of Documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control CP-10*

*Impact:* *New Requirement*

→ **11.2.2-C** Protecting The Integrity Of The Boot Process Requirement

Before boot up or initialization, electronic devices ***SHALL*** verify the integrity of the components used to boot up or initialize the electronic device.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

A tamper-resistant hardware module can be used to store the signature of the components that are required to boot the electronic device. The device will not boot if the files have been modified or the boot storage has been removed from the voting system.

*Source:* *Volume I, Section 7.4.6*

*Impact:* *This requirement augments the requirements found at Section 7.4.6 in Volume I of the VVSG 2005 by mandating explicitly requiring integrity checking of components used to boot up or initialize electronic device.*

→ **11.2.2-D** Monitoring The State Of The Electronic Device Requirement

Electronic devices ***SHALL*** detect, report, and alert changes made to voting system state and system configuration by performing verifications of cryptographic checksums (hash values or digital signatures) on the set of critical software objects (e.g., binaries) specified by the vendor (See requirement 1.2.2-E).

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Testing)*

D I S C U S S I O N

The list of critical software objects of the electronic device to monitor is documented in requirement **1.2.2-E**.

*Source:* *Volume I, Section 7.4.6*

*Impact:* *This requirement augments the requirement found at Section 7.4.6 in Volume I of the VVSG 2005 by mandating regular integrity checking of critical software objects via cryptographic checksum.*

→ **11.2.2-E** Critical Software Object List Documentation Requirement

As part of the TDP, vendors ***SHALL*** provide a list of all critical software objects (e.g., binaries) of the electronic device to be monitored.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Examples of critical software objects to monitor are electronic device binaries, Voting System application binaries, and configuration files.

*Source:* *Volume I, Section 7.4.6*

*Impact:* *This requirement augments the requirement found at Section 7.4.6 in Volume I of the VVSG 2005 by mandating vendors provide an inventory of critical software objects.*

→ **11.2.2-F** Electronic Device Health Monitoring Health Requirement

Electronic devices ***SHALL*** check, alert, and log the voting system's health by monitoring the state of the critical security components, security configurations, and electronic processes specified by the vendor (See requirement 1.2.2-G).

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Volume I, Section 7.4.6*

*Impact:* *This requirement augments the requirement found at Section 7.4.6 in Volume I of the VVSG 2005 by mandating explicitly listing components, policies, and processes subject to health monitoring.*

→ **11.2.2-G** Critical Security Components, Policies, and Processes List Documentation Requirement

As part of the TDP, vendors ***SHALL*** provide a list of the critical security components, security configurations, and electronic processes of the electronic device to be monitored for health.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Volume I, Section 7.4.6*

*Impact:* *This requirement augments the requirement found at Section 7.4.6 in Volume I of the VVSG 2005 by mandating that vendors provide an inventory of components, policies, and processes for health monitoring.*

→ **11.2.2-H** Integrity Verification Of Binaries Before Execution or Memory Load Requirement

Electronic devices ***SHALL*** verify the digital signatures or cryptographic hashes of the binaries (e.g., device drivers, library files, applications, and utilities) before they are executed or loaded into memory.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Volume I, Section 7.4.6(b)*

*Impact:* *This requirement augments the requirement found at Section 7.4.6(b) in Volume I of the VVSG 2005 by mandating digital signatures or cryptographic hashes as a mechanism for verifying the integrity of binaries and by specifying that binary integrity checking must be performed before binaries are executed or loaded into memory.*

→ **11.2.2-I** Implementing an application white list

Electronic devices ***SHALL*** have a mechanism to register all software applications necessary for the functionality of the Voting System. The registration mechanism ***SHALL*** include use of a digital signature or cryptographic hash for integrity checking.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Volume I, Section 7.4.6(b)*

*Impact:* *This requirement augments the requirement found at Section 7.4.6(b) in Volume I of the VVSG 2005 by mandating a mechanism to register permitted applications.*

➞ **11.2.2-J** Enforcing an application white list

Electronic devices ***SHALL*** deny all software applications from executing except for those registered in the list of software that are allowed to run on the electronic device based on their digital signature or cryptographic hash.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Volume I, Section 7.4.6(b)*

*Impact:* *This requirement augments the requirement found at Section 7.4.6(b) in Volume I of the VVSG 2005 by mandating use of a permitted application list (aka white list) as an enforcement mechanism each time an application executes.*

➞ **11.2.2-K** Protecting The Core Kernel Code And Data Requirement

Electronic devices with an operating system kernel ***SHALL*** implement a mechanism to prevent un-trusted code or data from patching or otherwise modifying the kernel.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control SI-7*

*Impact:* *New Requirement*

**11.2.2-L** Protecting Electronic Device Memory Against Buffer Overflow/Overrun Requirement

Electronic devices ***SHALL*** have a mechanism to protect against buffer overflow/overrun attacks that prevents the execution of code on the stack or the heap, checks that the stack has not been modified, and randomizes data in a process's address space.

*Applies to:* *Electronic Device*

*Test Reference:* *TBD*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control SI-10*

*Impact:* *New Requirement*

**11.2.2-M** Documenting functionality and required privilege of services and processes

Vendors ***SHALL*** document the function and corresponding privilege requirements for each service and/or process of the electronic device.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

By bundling unrelated functions of a service or process, vendors sometimes enable select functions to run at an authorization level beyond necessity. Keeping these functions separated will allow each function to execute with the lowest necessary privilege, thereby minimizing privilege escalation attacks through that function.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-62*

*Impact:* *New Requirement*

**11.2.2-N** Separating functionality of services and processes

The services on an electronic device ***SHALL*** be separated based on functionality, so that unrelated functions are not bundled into a single service or process.

*Applies to:* *Electronic Device*

*Test Reference:* *TBD*

D I S C U S S I O N

By bundling unrelated functions of a service or process, vendors sometimes enable select functions to run at an authorization level beyond necessity. Keeping these functions separated will allow each function to execute with the lowest necessary privilege, thereby minimizing privilege escalation attacks through that function.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-62*

*Impact:* *New Requirement*

→ **11.2.2-O** Sandboxing Applications Requirement

Electronic devices ***SHALL*** logically separate each application such that applications can only access resources necessary for normal functionality.

*Applies to:* *Electronic Device*

*Test Reference:* *TBD*

D I S C U S S I O N

Logically separating applications such that only required resources can be accessed is often referred to as “sandboxing” an application. It is meant to ensure that subversion of an application’s native security will not result in access beyond normal resources.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-6, SC-2*

*Impact:* *New Requirement*

→ **11.2.2-P** Preventing Automatic Execution Of Data On Removable Media Requirement

Electronic devices ***SHALL*** not access, open, or run contents that are stored on removable media without user intervention and authorization.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-83*

*Impact:* *New Requirement*

## 11.2.3 Removable Media Requirements

While removable media is used in a number of precincts as a part of the voting process, removable media is sometimes a mechanism to propagate malicious code or exfiltrate data from electronic devices. For this reason, removable media requirements focus on enabling use of removable media, while protecting the electronic device.

→ **11.2.3-A** Restricting The Use Of Removable Media Requirement

Electronic devices ***SHALL*** disable all removable media interfaces that are not needed for each voting system mode.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-6*

*Impact:* *New Requirement*

→ **11.2.3-B** Restricting The Insertion Of Removable Media Requirement

Each removable media interface of electronic devices that cannot be disabled ***SHALL*** have a mechanism to physically or logically secured the interface from the insertion of removable media.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Physically securing the removable media interface prevents the insertion of removable media. Logically securing the removable media interface prevents the use of removable media inserted into the electronic device. See Chapter XX: Physical Security for requirement related to physical security.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-3, AC-6*

*Impact:* *New Requirement*

→ **11.2.3-C** Removable Media Authentication Requirement

Electronic devices ***SHALL*** verify the authenticity of inserted removable media before permitting the use of the removable media.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-3*

*Impact:* *New Requirement*

→ **11.2.3-D** Restricting The Removal Of Removable Media Requirement

Each removable media interface of electronic devices that cannot be disabled ***SHALL*** have a mechanism to physically or logically secured the interface from the removal of removable media.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Physically securing the removable media interface prevents the removal of removable media. Logically securing the removable media interface prevents the removal of removable media from the electronic device (e.g., ejecting a CD; dismounting a USB flash drive). See Chapter XX: Physical Security for requirement related to physical security.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control MP-2, AC-3*

*Impact:* *New Requirement*

→ **11.2.3-E** Restricting Access To Removable Media Requirement

Electronic devices ***SHALL*** prevent voters from having direct logical access to information on removable media (i.e., the electronic device can access the removable media to perform authorized actions on behalf of a voter).

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-3*

*Impact:* *New Requirement*

➞ **11.2.3-F** Protecting Information On Removable Media Requirement

Electronic device ***SHALL*** protect the integrity of sensitive information on removable media that is not physically secured by signing or cryptographically hashing the information.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-3*

*Impact:* *New Requirement*

## 11.2.4 Backup and Recovery Requirements

Backup and recovery requirements describe minimum authorization, auditing, and protective measures, without regard to specific media. Additional requirements for backup of audit data can be found in 1.2.6 - Event Logging and Audit Requirements.

➞ **11.2.4-A** Restricting The Performance Of Backups Requirement

Electronic devices ***SHALL*** only permit backup operations while not Activated mode.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control SC-2*

*Impact:* *New Requirement*

→ **11.2.4-B** File System Based Storage Backup Requirement

Electronic devices with file system based storage ***SHALL*** be capable of backing up files on internal storage or removable media.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control CP-9*

*Impact:* *New Requirement*

→ **11.2.4-C** Authenticity and Integrity of Backup Information Requirement

Electronic devices ***SHALL*** sign or cryptographically hash backups so that their authenticity and integrity can be verified in the future.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control CP-9*

*Impact:* *New Requirement*

→ **11.2.4-D** Protecting Personally Identifiable Information On Backups Requirement

Electronic devices ***SHALL*** be capable of encrypting personally identifiable information stored in backups to protect its confidentiality.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control CP-9*

*Impact:* *New Requirement*

➞ **11.2.4-E** Restricting The Performance Of Restorations Requirements

Electronic devices ***SHALL*** only permit restore operations while not Activated mode.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Testing)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control SC-2*

*Impact:* *New Requirement*

➞ **11.2.4-F** File System Based Storage Performance Of Restorations Requirements

Electronic devices with file system based storage ***SHALL*** be capable of restoring files onto internal storage or removable media after first verifying the authenticity and integrity of the backup.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Testing)*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control CP-10*

*Impact:* *New Requirement*

## 11.2.5 Malicious Software Protection Requirements

As described in the National Institute of Standards and Technology Special Publication 800-83 [MELL05], malicious software, also known as malicious code and Malware, refers to a program that is inserted into a system, usually covertly,

with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim. For a number of reasons, Electronic Devices associated with Voting Systems may be targeted by Malware. Malware is inclusive of viruses, worms, Trojan horses, and malicious mobile code, as well as combinations of these, known as blended attacks. Malware also includes attacker tools such as backdoors, rootkits, and keystroke loggers. Given this understanding of Malware, requirements focus on preventing occurrences of Malware on Electronic Devices.

→ **11.2.5-A** Installing Malware Detection Software Requirement

Electronic devices ***SHALL*** protect themselves from known Malware that targets their operating systems, services, and applications.

*Applies to:* *Electronic Device*

*Test Reference:* *TBD*

D I S C U S S I O N

Types of electronic devices most likely to be targets of Malware are those running personal computer operating systems (e.g., Windows, Unix, Linux, Mac OS X) or embedded operating systems based on personal computer operating systems (e.g., Windows CE, embedded Linux).

*Source:* *Volume I, Section 7.4.2*

*Impact:* *This requirement augments the requirement found at Section 7.4.2 in Volume I of VVSG 2005 previous requirements by specifying installation of Malware detection/scanning software.*

→ **11.2.5-B** Scanning Removable Media for Malware Requirement

Electronic devices ***SHALL*** run Malware detection software against removable media to verify no Malware is present before accepting any data from the removable media.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Volume I, Section 7.4.2*

*Impact:* *This requirement augments the requirement found at Section 7.4.2 in Volume I of VVSG 2005 by specifying scanning of removable media for Malware.*

→ **11.2.5-C** Periodic Malware Scanning Requirement

Electronic devices ***SHALL*** be scanned for Malware at least once every 24 hours during operation, including Malware specifically targeted at Voting Systems.

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Volume I, Section 7.4.2*

*Impact:* *This requirement augments the requirement found at Section 7.4.2 in Volume I of VVSG 2005 by specifying scanning of removable media for Malware.*

→ **11.2.5-D** Real-time Malware Scanning Requirement

Electronic devices ***SHALL*** provide real-time Malware scanning (e.g., documents before they are opened in applications).

*Applies to:* *Electronic Device*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Volume I, Section 7.4.2*

*Impact:* *This requirement augments previous the requirement found at Section 7.4.2 in Volume I of the VVSG 2005 by real-time scanning for Malware.*

## 11.2.6 References

[NGC06] Nevada Gaming Commission and State Gaming Control Board, Technical Standards for Gaming Devices and On-Line Slot Systems, March 2006, available at http://gaming.nv.gov/stats_regs/reg14_tech_stnds.pdf

[SOUP05] Murugiah Souppaya, John P. Wack, Karen Kent, National Institute of Standards and Technology Special Publication 800-70: Security Configuration Checklist Program for IT Products – Guidance for Checklists Users and Developers, May 2005, available at http://csrc.nist.gov/checklists/docs/SP_800-70_20050526.pdf

[MELL05] Peter Mell, Karen Kent, Joseph Nusbaum, National Institute of Standards and Technology Special Publication 800-83: Guide to Malware Incident Prevention and Handling, November 2005, available at http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf

# Chapter 12: Communication Security

## 12.1 Introduction/Scope

This chapter is a guideline for protecting Voting System electronic device network communications. These requirements are meant to be additive to the security requirements specified in the other parts of the VVSG. In many ways, security of the electronic devices is subject to the current Voting System mode. Perhaps more importantly, the Voting System mode is an indicator of who requires access to any given device. This factor significantly influences security measures. The requirements of this chapter apply only to voting system modes where networking can be enabled – modes other than the Activated mode.

There are some similarities between voting machines and gaming machines. As a method of assuring completeness of requirements, the Nevada Gaming Commission's [NGC06] technical standards on gaming machines were consulted for applicability.

The Communication Security section is generally organized according to the TCP/IP **{** XE " Transmission Control Protocol/Internet Protocol (TCP/IP)" **}** communication model (also known as "4-layer computer communication reference model"). TCP/IP is widely used throughout the world to provide network communications. TCP/IP communications are composed of four layers that work together. When a user wants to transfer data across networks, the data is passed from the highest layer through intermediate layers to the lowest layer, with each layer adding additional information. The lowest layer sends the accumulated data through the physical network; the data is then passed up through the layers to its destination. Essentially, the data produced by a layer is encapsulated in a larger container by the layer below it. The four TCP/IP layers, from highest to lowest, are shown in the figure below.

| |
|---|
| **Application Layer{** XE " Transmission Control Protocol/Internet Protocol (TCP/IP):Application layer" **}.** This layer sends and receives data for particular applications, such as Domain Name System (DNS), HyperText Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP). |
| **Transport Layer{** XE " Transmission Control Protocol/Internet Protocol (TCP/IP):Transport layer" **}.** This layer provides connection-oriented or connectionless services for transporting application layer services between networks. The transport layer can optionally assure the reliability of communications. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are commonly used transport layer protocols. |

| |
|---|
| **Network Layer{** XE " Transmission Control Protocol/Internet Protocol (TCP/IP):Network layer" **}.** This layer routes packets across networks. Internet Protocol (IP) is the fundamental network layer protocol for TCP/IP. Other commonly used protocols at the network layer are Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP). |
| **Data Link Layer{** XE " Transmission Control Protocol/Internet Protocol (TCP/IP):Data link layer" **}.** This layer handles communications on the physical network components. The best-known data link layer protocol is Ethernet. |

Figure 12-3 Description of the TCP/IP 4 Layer Communication Model

# 12.2 Communication Security Requirements

A listing of the requirements sections is shown below. Requirements sections are organized based on the 4-layer computer communication reference model. Additionally, Data Transmission is organized in a separate section.

12.2.1 Physical Communication Security Requirements

12.2.2 Data Transmission Security Requirements

12.2.3 Logical Communication Security Requirements

12.2.4 References

## 12.2.1 Physical Communication Security Requirements

This section describes secure configuration of Voting System electronic devices at the physical layer of the 4-layer computer communication model.

→ **12.2.1-A** Prohibiting wireless technology

Electronic devices ***SHALL*** not be enabled or installed with any wireless technology (e.g., Wi-Fi, wireless broadband, Bluetooth) except for infrared technology when the signal path is shielded to prevent the escape of the signal and saturation jamming of the signal.

*Applies to:* *Electronic Devices*

*Test Reference:* *TBD*

D I S C U S S I O N

The transient and mobile properties of wireless networks are more threatening than enabling to the voting process. Wireless interfaces which are inadvertently or purposefully enabled at an electronic device are likely to leave those platforms

exposed to attack and exploit, with exfiltration, manipulation, or destruction of data a possible outcome.

*Source:* *Volume I, Section 7.7*

*Impact:* *This requirement supercedes all previous requirements documented in Volume I, Section 7.7 of VVSG 2005 by prohibiting usage of wireless technology except for infrared technology when the physical path is protected for Voting System electronic devices.*

→ **12.2.1-B** Prohibiting dependency on public communication networks

Electronic devices ***SHALL*** not be dependent on public communication networks (including, but not limited to the Internet and modem usage through public telephone networks).

*Applies to:* *Electronic Devices*

*Test Reference:* *TBD*

DISCUSSION

The use of public communications networks would greatly increase the exposure of electronic devices for voting to attack and exploitation. Functions such as software patch distribution may be performed either manually or through a dedicated, standalone network which is not connected to any public communications network.

*Source:* *Volume I, Section 7.6*

*Impact:* *This requirement supercedes all previous requirements documented in Volume I, Section 7.6 of VVSG 2005 by prohibiting usage of public communication networks for Voting System electronic devices.*

→ **12.2.1-C** Limiting network interfaces based on voting mode

Electronic devices ***SHALL*** have the ability to enable or disable physical network interfaces (including modems) based upon the Voting System mode.

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Making an electronic device accessible on a network significantly increases the risk of that device to attack and exploitation. Election Officials need the ability to enable a physical network interface for use during a particular voting system mode and to

disable other network interfaces that are not needed during that mode. This reduces the exposure of the electronic devices to network-based attacks.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-6*

*Impact:* *New Requirement*

➞ **12.2.1-D** Limiting the number of network interfaces

Electronic devices ***SHALL*** have at most a single active network interface (including a modem) at any given time.

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

Complexity of communication and exposure to vulnerability increases for electronic devices when they are networked to more than one network.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-6*

*Impact:* *New Requirement*

➞ **12.2.1-E** Implementing unique network identification

Each electronic device ***SHALL*** have a unique physical address/identifier for each network interface.

*Applies to:* *Electronic Devices*

*Test Reference:* *TBD*

DISCUSSION

Most networking protocols require a unique physical address or other identifier for each network interface so that each network interface attached to a particular network can be uniquely identified. For example, Ethernet requires that each network interface have a unique media access code (MAC) address. Having such an identifier for each network interface is also beneficial for security because it permits each electronic device on a network to be uniquely identified.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control IA-3*

*Impact:* *New Requirement*

## 12.2.2 Data Transmission Security Requirements

This section describes requirements of how Voting System electronic devices should protect information as it traverses network connections to other electronic devices. This section does not include guidelines on cryptographic techniques for ensuring integrity, confidentiality, identification/authentication, and non-repudiation of network transactions. Please see Chapter XX: Cryptography for a more in-depth treatment of those topics.

→ **12.2.2-A** Documenting network processes and applications

Vendors ***SHALL*** provide a listing of all network communication processes and applications necessary for the electronic device to function properly.

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 4.1 (Review of Documentation)*

D I S C U S S I O N

Understanding required network processes and applications is necessary for understanding the attack exposure of any given electronic device.

*Source:* *Volume I, Section 7.5.1(b)ii*

*Impact:* *This requirement augments the requirement found at Section 7.5.1(b)ii in Volume I of the VVSG 2005 by mandating documentation of valid processes and applications associated with network ports and protocols.*

→ **12.2.2-B** Prohibiting unnecessary communication between electronic devices

Electronic devices ***SHALL*** prohibit intercommunications between electronic devices except where necessary for normal function.

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

In the interest of reducing the number of nodes accessing a given platform and potentially the voting data thereof, devices which have no need to interact over the network should be locally prohibited from those interactions. This reduces possible sources of network attack.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-6*

*Impact:* *New Requirement*

→ **12.2.2-C** Implementing integrity of data in transit

Electronic devices ***SHALL*** provide integrity protection for data in transit through generation of cryptographic checksums for outbound traffic and verification of cryptographic checksums for inbound traffic.

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Integrity protection ensures that any inadvertent or intentional alterations to data are detected by the recipient. Integrity protection for data in transit may be provided through the use of various protocols, such as IPsec VPNs and SSL/TLS. See Chapter XX: Cryptography for more information on requirements related to cryptography.

*Source:* *Volume I, Section 7.5.1(a)*

*Impact:* *This requirement modifies the requirement found at Section 7.5.1(a) in Volume I of the VVSG 2005 by specifying the use of cryptographic checksums (digital signatures and hashes) to be used to ensure information integrity in transit.*

## 12.2.3 Logical Communication Security Requirements

This section describes secure configuration of Voting System electronic devices at the network, transport, and application layers of the 4-layer computer communication model.

→ **12.2.3-A** Implementing unique system identifiers

Each electronic device ***SHALL*** have a unique system identifier (ID).

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

System ID can be in the form of a unique system or device account that can be used as a mechanism to filter the type of packets that are allowed or dropped by the device.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control IA-3*

*Impact:* *New Requirement*

→ **12.2.3-B** Prohibiting unauthenticated communications

Electronic devices ***SHALL*** mutually authenticate using the devices' unique system IDs before any additional network data packets are processed.

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Mutual authentication provides assurance that each electronic device is legitimate. Mutual authentication can be performed using various protocols, such as IPsec and SSL/TLS.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control IA-3*

*Impact:* *New Requirement*

→ **12.2.3-C** Limiting network ports and shares and associated network services and protocols

Electronic devices ***SHALL*** have only the network ports and shares active and network services and protocols enabled as specified in requirement **1.2.3-D**.

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Limiting network ports and shares and associated network services and protocols reduces the "attack surface" of the electronic devices. Attackers will have a diminishing chance of successful remote attack with each network port, share, service, and protocol that is disabled.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-6*

*Impact:* *New Requirement*

→ **12.2.3-D** Documenting network ports and shares and associated network services and protocols

Vendors ***SHALL*** document all necessary network ports, shares, services, and protocols for the electronic device to function properly.

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 4.1 (Review of Documentation)*

DISCUSSION

Understanding required network ports, shares (both visible and hidden/administrative), services, and protocols is necessary for understanding the attack exposure of any given electronic device. Based on local risk decisioning, election officials will utilize the listing of required network ports, shares, services, and protocols to adjust configuration of an electronic device and the corresponding attack exposure.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-6*

*Impact:* *New Requirement*

→ **12.2.3-E** Minimizing information available to remote users and devices

Per requirement **1.2.3-F**, electronic devices ***SHALL*** display no more information than necessary to unauthenticated remote users and devices via active network ports and shares.

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

DISCUSSION

This requirement is meant to minimize the amount and depth of information available to malicious network entities accessing the electronic device remotely. Information available through banners, help functions, and direct interaction with available ports and shares often gives remote attackers illuminating information about the electronic device. Armed with this expanded information, an attacker can evolve their attack to a more educated and specific effort, increasing probability of a successful attack.

*Source:* *[SCAM01]*

*Impact:* *New Requirement*

→ **12.2.3-F** Documenting information available to remote users and devices

Vendors ***SHALL*** define the minimum amount of information available that needs to be made visible to unauthenticated remote users and devices via active network ports and shares.

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 4.1 (Review of Documentation); Functional test as part of requirement **1.2.3-E***

D I S C U S S I O N

This requirement is meant to document the minimum amount and depth of information available to malicious network entities accessing the electronic device remotely. Information available through banners, help functions, and direct interaction with available ports and shares often gives remote attackers illuminating information about the electronic device. Armed with this expanded information, an attacker can evolve their attack to a more educated and specific effort, increasing probability of a successful attack.

*Source:* *[SCAM01]*

*Impact:* *New Requirement*

→ 12.2.3-G Limiting remote activities

Electronic devices ***SHALL*** enable remote access only when not in Activated mode.

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Making an electronic device accessible on a network significantly increases the risk of that electronic device to attack and exploitation.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control AC-6*

*Impact:* *New Requirement*

→ **12.2.3-H** Monitoring of host and network communication for attack and policy compliance

Electronic devices ***SHALL*** monitor inbound and outbound network communication for evidence of attack and security usage non-compliance.

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

Security usage non-compliance refers to instances where electronic device users are disobeying local policy.

See NIST Special Publication 800-94 – Guide to Intrusion Detection and Prevention Systems [SCAR07] for more information on host and network communication monitoring and attack prevention.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control SI-4, SI-10*

*Impact:* *New requirement*

→ **12.2.3-I** Prevention of host and network communication based attacks

Electronic devices ***SHALL*** provide the capability to prevent inbound and outbound network attack.

*Applies to:* *Electronic Devices*

*Test Reference:* *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

See NIST Special Publication 800-94 – Guide to Intrusion Detection and Prevention Systems [SCAR07] for more information on host and network communication monitoring and attack prevention.

*Source:* *NIST Special Publication 800-53 Revision 1, Security Control SI-4, SI-10*

*Impact:* *New requirement*

## 12.2.4 References

[NGC06] Nevada Gaming Commission and State Gaming Control Board, Technical Standards for Gaming Devices and On-Line Slot Systems, March 2006, available at http://gaming.nv.gov/stats_regs/reg14_tech_stnds.pdf

[WACK02] John Wack, Ken Cutler, Jamie Pole, National Institute of Standards and Technology Special Publication 800-41: Guidelines on Firewalls and Firewall Policy, January 2002, available at http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

[BURR06] William Burr, Donna Dodson, W. Timothy Polk, National Institute of Standards and Technology Special Publication 800-63: Electronic Authentication Guideline, April 2006, available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[KENT06] Karen Kent, Murugiah Souppaya, National Institute of Standards and Technology Special Publication 800-92: Guide to Computer Security Log Management, September 2006, available at http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

[SCAM01] Joel Scambray, Stuart McClure, George Kurtz, Hacking Exposed: Network Security Secrets and Solutions, Second Edition, 2001

[SCAR07] Karen Scarfone, Peter Mell, National Institute of Standards and Technology Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems, February 2007, available at http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

# Chapter 13: System Event Logging

## 13.1 Introduction/Scope

An *event* is something that occurs within a voting system and a *log* is a record of these events that have occurred. Each log entry contains information related to a specific event. Logs are used for error reporting, auditing, troubleshooting problems, optimizing performance, recording the actions of users, and providing data useful for investigating malicious activity.

Event logs are typically divided into two categories: system events and audit records. System events are operational actions performed by voting system components, such as shutting down the voting system, starting a service, usage information, client requests, and other information. Audit records contain security event information such as successful and failed authentication attempts, file accesses, and security policy changes. Other applications and third party software, such as antivirus software and intrusion detection software also record audit logs. For the purpose of this chapter system event logging will be used to include both system and audit logs for the voting system.

This chapter describes voting system capabilities that perform system event logging to assist in voting system troubleshooting, recording a history of voting system activity, and detecting unauthorized or malicious activity. It also describes the use of log management to protect the confidentiality and integrity of logs, while also ensuring their availability. The voting system software, operating system, and/or applications may perform the actual system event logging. There may be multiple logs in use on a single system.

The requirements in this section protect against the following intermediate attack goals:

- The ability of an attacker to undetectably alter the logs
- The ability of an attacker to remove an entry from the log
- The ability of an attacker to create an entry in the log

## 13.2 System Event Logging Requirements

This section defines the event logging requirements for voting systems. It outlines the various measures that the vendors and the voting system shall provide to ensure the functionality, performance, and security of the voting system event logging. These recommendations apply to the full scope of voting system functionality, including voting, pre- and post-voting activities, and maintenance of the voting system.

## 13.2.1 General System Event Logging Requirements

General requirements address the high level functionality of a voting system. These are the fundamental event logging requirements upon which other requirements in this section are based.

→ **13.2.1-A** Event logging mechanisms requirement

The voting system ***SHALL*** provide event logging mechanisms designed to record voting system activities.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.3*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by including a high level event logging design requirement.*

→ **13.2.1-B** Integrity protection requirement

The voting system ***SHALL*** enable file integrity protection for stored log files as part of the default configuration.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.4*

D I S C U S S I O N

File integrity protection includes techniques such as a digital signature that would alert to data modification and tampering.

*Source:* *VVSG 2005 Volume I, Section 5.4.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4.2 by requiring event log encryption and file integrity protection as part of the default settings.*

→ **13.2.1-C** Ballot secrecy requirement

The voting system logs ***SHALL*** not violate ballot secrecy.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:*

*Impact:*

→ **13.2.1-D** Event characteristics logging requirement

The voting system ***SHALL*** log at a minimum the following data characteristics for each type of event:

- System ID
- Unique event ID and/or type
- Timestamp
- Success or failure of event, if applicable
- User ID triggering the event, if applicable
- Resources requested, if applicable.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring a minimum set of log data characteristics for each event.*

↳ **13.2.1-D.1** Timekeeping requirement

Timekeeping mechanisms ***SHALL*** generate time and date values.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring time keeping.*

↳ **13.2.1-D.2** Time precision requirement

The precision of the timekeeping mechanism ***SHALL*** be able to distinguish and properly order all audit records.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

For example, if the minimum possible time between events creating audit records is 1 second, then time must be recorded with a precision of no worse than ½ second (the Nyguist rate).

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring time precision.*

↳ **13.2.1-D.3** Timestamp data requirement

Timestamps ***SHALL*** include date and time, including hours, minutes, and seconds.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Even if the accuracy of the clock leaves something to be desired, the seconds are useful to discern burst and gaps in the event stream.

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring specific timestamp characteristics.*

↳ **13.2.1-D.4** Timestamp compliance requirement

Timestamps ***SHALL*** comply with ISO 8601 by providing all four digits of the year and include the time zone.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring timestamp compliance.*

↳ **13.2.1-D.5** Clock synchronization requirement

The voting system ***SHALL*** provide clock synchronization.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

This requirement is needed to adjust clocks that drift from reference times such as provided by NIST and USNO.

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring clock synchronization.*

↳ **13.2.1-D.6** Clock drift minimum requirement

The voting system ***SHALL*** limit clock drift to a minimum of 1 minute within a 15 hour period after initialization.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

The accuracy of the timekeeping mechanism relative to UTC (Coordinated Universal Time) may depend on application of a vendor-specified clock initialization procedure. NIST and USNO time references are far more accurate, and higher accuracy is desirable, but many clock mechanism exhibit significant drift due to temperature, etc. and simple correction methods for a fast local clock might violate the monotonic time requirement.

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring a clock drift minimum.*

→ **13.2.1-E** Minimum event logging requirement

The voting system ***SHALL*** log at a minimum the system events described in Table 1.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Table 1 presents a minimum list of system events to be logged. The table also includes an "applies to" reference specifying the class of devices that are subject to each requirement.

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring a minimum set of events to log.*

↳ **13.2.1-E.1** Minimum logging disabling requirement

The voting system ***SHALL*** ensure that the minimum event logging in Table 1 cannot be disabled.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by prohibiting disabling of the minimum set of events to log.*

| SYSTEM EVENT | DESCRIPTION | APPLIES TO |
|---|---|---|
| **GENERAL VOTING SYSTEM** | | |
| Machine generated error and exception messages | Examples of machine generated error and exception messages include but are not limited to:<br>♦ The source and disposition of system interrupts resulting in entry into exception handling routines.<br>♦ Messages generated by exception handlers.<br>♦ The identification code and number of occurrences for each hardware and software error or failure.<br>♦ Notification of physical violations of security<br>♦ Other exception events such as power failures, failure of critical hardware components, data transmission errors or other types of operating | Voting Device |

| SYSTEM EVENT | DESCRIPTION | APPLIES TO |
|---|---|---|
| | anomalies. | |
| Critical system status messages | Critical system status messages other than information messages displayed by the system during the course of normal operations.<br><br>Examples of critical system status messages include but are not limited to:<br><br>♦ Diagnostic and status messages upon startup.<br>♦ The "zero totals" check conducted before opening the polling place or counting a precinct centrally.<br>♦ For paper-based systems, the initiation or termination of card reader and communications equipment operation.<br>♦ Printer errors. | Voting Device |
| Non-critical status messages | Non-critical status messages that are generated by the machine's data quality monitor or by software and hardware condition monitors. | Voting Device |
| Events that require election official intervention | Events that require election official intervention, so that each election official access can be monitored and access sequence can be constructed. | Voting devices with operating systems |
| Operating system shutdown and restarts | Both normal and abnormal operation system shutdowns and restarts. | Voting devices with operating systems |
| Changes to system configuration settings | Configuration settings include registry keys, kernel parameters, logging settings, and other voting system parameters. | Voting device |
| Integrity checks for executables, configuration files, data, and logs. | Integrity checks alert to possible tampering with files and data. | Voting devices with operating systems |
| The addition, modification, and deletion of files. | Files that are added, modified, or deleted from the voting system. | Voting devices with operating systems |
| System readiness results | System readiness results include at a minimum the following information:<br><br>♦ System pass or fail of hardware and software test for system readiness.<br><br>♦ Identification of the software release, | Voting devices |

| SYSTEM EVENT | DESCRIPTION | APPLIES TO |
|---|---|---|
| | identification of the election to be processed, polling place identification, and the results of the software and hardware diagnostic tests.<br>♦ Pass or fail of ballot style compatibility and integrity test.<br>♦ Pass or fail of system test data removal.<br>♦ Zero totals of data paths and memory locations for vote recording. | |
| Removable media events | Removable media that is inserted into or removed from the voting device. | Voting devices |
| Backup and restore | Successful and failed attempts to perform backups and restores. | Voting devices with operating systems |
| **AUTHENTICATION AND ACCESS CONTROL** | | |
| Authentication related events | Authentication related events include, but are not limited to the following:<br>♦ Login/logoff events (both successful and failed attempts)<br>♦ Account lockout events<br>♦ Password changes | Voting devices with operating systems |
| Access control related events | Access Control related events include, but are not limited to the following:<br>♦ Use of privileges (such as a user running a process as an administrator)<br>♦ Attempts to exceed privileges<br>♦ All access attempts to application and underlying system resources<br>♦ Changes to the access control configuration of the voting system | Voting devices with operating systems |
| User account and role (or groups) management activity | User account and role management activity includes, but is not limited to the following:<br>♦ Addition and deletion of user accounts and roles.<br>♦ User account and role suspension and reactivation<br>♦ Changes to account or role security attributes such as password length, access levels, login | Voting devices with operating systems |

| SYSTEM EVENT | DESCRIPTION | APPLIES TO |
|---|---|---|
| | restrictions, permissions, etc.<br>♦ Administrator account and role password resets | |
| **APPLICATIONS** | | |
| Changes to application configuration settings | Changes to application configuration settings include, but are not limited to the following:<br>♦ Changes to critical function settings. At a minimum critical application function settings include location of ballot, contents of the ballot, vote tally processes, location of logs, and voting system configuration parameters.<br>♦ Changes to system parameters such as enabling and disabling services<br>♦ Starting and stopping application processes | Voting device |
| Abnormal application exits | All abnormal application exits. | Voting device |
| Application installations | All application installation. | Voting device |
| Application and operating system patching | All patching to applications and the operating system. | Voting device |
| Successful and failed database connection attempts (if a database is utilized). | All database connection attempts. | Voting devices with operating systems |
| **CRYPTOGRAPHIC FUNCTIONS** | | |
| Changes to cryptographic keys | At a minimum critical cryptographic settings include key addition, key removal, and re-keying. | Voting device |
| **VOTING FUNCTIONS** | | |
| Ballot definition and modification | During election definition and ballot preparation, the system may provide logging information for the preparation of the baseline ballot formats and modifications to them including a description of the modification and corresponding dates. Logging information includes at a minimum, but is not limited, to the following:<br>♦ The account name that made the modifications<br>♦ A description of what was modified including the | Voting devices with operating systems |

| SYSTEM EVENT | DESCRIPTION | APPLIES TO |
|---|---|---|
| | file name, location, and the content changed<br>♦ The date and time of the modification. | |
| Voting events | Voting events include:<br>♦ Opening and closing polls<br>♦ Canceling a vote during verification<br>♦ Fled voters<br>♦ Results of exporting logs to tabulation center. | Voting device |

Table 13-7 Minimum Events to Log

## 13.2.2 System Event Logging Documentation Requirements

Documentation requirements address the minimum event logging information necessary for testing and implementation of the voting system. This includes both public and private information. User documentation includes all public information that is provided to the end users. The Technical Data Package (TDP) includes the user documentation along with other private information that is viewed only by the test labs.

→ **13.2.2-A** General user and TDP documentation requirement

Vendors ***SHALL*** provide user and TDP documentation of event logging capabilities of the voting system.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring vendors to provide user and TDP documentation for event logging.*

↳ **13.2.2-A.1** User documentation for system event logging requirement

Vendors ***SHALL*** provide user documentation that describes system event logging capabilities and usage.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring vendors to provide user documentation for system event logging usage.*

↳ **13.2.2-A.2** TDP for event logging design and implementation requirement

Vendors ***SHALL*** provide a technical data package that describes system event logging design and implementation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring vendors to provide user documentation for system event logging usage.*

➞ **13.2.2-B** Log format documentation requirement

Vendors ***SHALL*** publicly publish fully documented log format information.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

The log format and the meaning of all possible types of log entries must be fully documented in sufficient detail to allow independent vendors to implement utilities

to parse the log file. This documentation must be publicly available, not just in the TDP.

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring vendors to provide user and TDP documentation for event logging.*

### 13.2.3 System Event Log Management Requirements

Log management is the process for generating, transmitting, storing, analyzing, and disposing of log data. Log management primarily involves protecting the integrity of logs, while also ensuring their availability. It also ensures that records are stored in sufficient detail for an appropriate period of time.

A log management infrastructure consists of the hardware, software, networks, and media used to generate, transmit, store, and analyze log data. The events outlined in this section may be logged as part of the underlying operating system, the voting system application, or other third party applications.

→ **13.2.3-A** Default logging policy requirement

The voting system ***SHALL*** implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring vendors to provide a suggested logging policy.*

→ **13.2.3-B** Reporting log failures, clearing, and rotation requirement

The voting system ***SHALL*** report logging failures, log clearing, and log rotation.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring reporting of log failures, clearing, and rotation.*

→ **13.2.3-C** Log format requirement

The voting system ***SHALL*** maintain a standard log format, such as XML, or include a utility that can convert the logs into a standard format for offline viewing.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.3*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring a standard log format.*

→ **13.2.3-D** Event log deletion capability requirement

The voting system ***SHALL*** be capable of allowing the administrator to delete previous event logs prior to starting a new election.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring event log data deletion capabilities.*

→ **13.2.3-E** Event log retention capability requirement

The voting system ***SHALL*** be capable of retaining the event log data from previous elections.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

In practice, previous event logs are typically cleared prior to the start of a new election. In some cases, jurisdictions may want to maintain previous event logs on the voting system. Event log data may be retained according to various methods including log file size, log entry counts, and time settings.

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring event log data retention capabilities.*

↳ **13.2.3-E.1** Log retention settings capability requirement

The voting system ***SHALL*** have the capability for administrators to modify the log data retention settings including the actions to take when a log reaches its maximum retention such as overwriting logs, rotating logs, or halting logging.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Many event logs have a maximum size for storage, such as storing the 10,000 most recent events, or keeping 100MB of log data. When the log storage capacity is reached, the log may overwrite old data with new data or stop logging altogether.

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring flexibility for administrators to configure event log data retention settings and actions.*

→ **13.2.3-F** Log rotation capability requirement

The voting system ***SHALL*** be capable of rotating the event log data to manage log file growth.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Log file rotation may involve regular, such as hourly, nightly, or weekly, moving of an existing log file to some other file name and/or location and starting fresh with an empty log file. Jurisdictions should ensure that the log rotation procedure includes a labeling method to identify the type of log, the system that created the logs, and the date of the logs.

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring event log rotation capabilities.*

↳ **13.2.3-F.1** Log rotation configuration capability requirement

The voting system ***SHALL*** have the capability for the administrators to modify the log rotation settings including the deletion of old log files.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring flexibility for administrators to configure event log rotation settings and actions.*

→ **13.2.3-G** Event log access requirement

The voting system ***SHALL*** restrict event log access to write or append-only for privileged logging processes and read-only for administrator accounts or roles.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Certain applications and processes need write and/or append access to system event logs in order to create entries. Administrator accounts or roles need read access for log analysis and other log management activities.

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring restricted access to event logs.*

→ **13.2.3-H** Event log separation requirement

The voting system ***SHALL*** ensure that each election's event logs are separable from each other.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring event log separation.*

→ **13.2.3-I** Event log export requirement

The voting system ***SHALL*** export event logs at the end of an election.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

For more information see the Chapter X, Electronic Records.

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring event log export.*

→ **13.2.3-J** Log viewing and analysis requirement

The voting system ***SHALL*** include an application or program to view, analyze, and search both current and rotated event logs.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring event log analysis capabilities.*

→ **13.2.3-K** Event logging malfunction requirement

The voting system ***SHALL*** halt voting activities and create and alert if the logging system malfunctions or is disabled.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring the ability to halt voting activities if the logging system malfunctions or is disabled.*

→ **13.2.3-L** Log file capacity requirement

The voting system ***SHALL*** alert the system administrator at user-defined intervals as the logs being to fill.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

D I S C U S S I O N

User defined intervals for system event log capacity may include alerting when logs are 50%, 75%, and 95% full.

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring administrator alerting as event logs reach capacity.*

→ **13.2.3-M** Event logging suspension requirement

The voting system ***SHALL*** suspend voting if the logs fill to a user-defined capacity.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring voting suspension due to event logs reaching capacity.*

## 13.2.4 System Event Log Protection Requirements

Because logs contain voting system event records, they need to be protected from breaches of their integrity and availability. Logs that are secured improperly in storage or in transit might also be susceptible to intentional and unintentional alteration and destruction. This could cause a variety of impacts, including allowing malicious activities to go unnoticed and manipulating evidence to conceal the identity of a malicious party. For example, many rootkits are specifically designed to alter logs to remove any evidence of the rootkits' installation or execution.

Data retention requirements might require log storage for a longer period of time than the original log sources can support, which necessitates establishing log archival processes. The integrity and availability of the archived logs also need to be protected.

→ **13.2.4-A** General event log protection requirement

The voting system ***SHALL*** protect event log information from unauthorized access, modification, and deletion.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.3*

DISCUSSION

See Chapter X, Access Control, for information on user and process identification, authentication, authorization, and access control permissions. See Chapter Y, Cryptography, for information on file encryption and integrity protection including encryption algorithms, hash functions, digital signatures, and key management.

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring high-level event log protection.*

→ **13.2.4-B** Modification protection requirement

The voting system ***SHALL*** protect logs from modification.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 5.2*

DISCUSSION

There are several ways to protect logs from modification including using operating system level security mechanisms to prevent deletion of the logs and enforce append-only access, use of append-only media, and use of cryptographic techniques [4].

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring write-once media or other persistent storage.*

➔ **13.2.4-C** Event log archival protection requirement

If the voting system provides log archival capabilities, it ***SHALL*** ensure the integrity and availability of the archived logs.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.3*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 5.4*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 5.4 by requiring high-level protection of archived logs.*

## 13.2.5 References

[1] NIST Special Publication (SP) 800-92. *Guide to Computer Security Log Management*.

[2] NIST SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*.

[3] NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

[4] Kelsey, John and Holt, Jason. *Using Cryptographic Logging to Improve Voting Security*. National Institute of Standards and Technology.

# Chapter 14: Physical Security

## 14.1 Introduction/Scope

The objective of the voting system physical security measures is to prevent undetected, unauthorized physical access to voting systems. It is assumed that adversaries have financial resources, technical savvy, and possibly insider presence to exploit vulnerabilities within voting systems. When in use, the physical security required for voting systems is relatively low compared to other types of moderate or high impact systems. Though voting areas should be private enough to maintain a voter's right to a secret ballot, the machines are generally not isolated. An attempt to physically open or disassemble a machine would likely not go unnoticed by poll workers. Similarly, a plot to tamper with the machines after the polls are closed would require a large conspiracy amongst poll workers, as an individual working alone would likely be noticed gaining access to machines outside of normal operating procedures. Voting systems also spend a considerable amount of time in storage or otherwise secured by means that could afford "open" though unauthorized access by well placed insiders. In that case, time and privacy are on the side of the adversary. One could not hope to stop an adversary from gaining access to the machine but one can hope to find evidence of their handywork.

The effectiveness of all technical security safeguards is based, in part, on the assumption, either explicit or implicit, that all components have adequate physical security protection. Any unauthorized physical access must leave physical evidence that an unauthorized event has taken place.

This section outlines physical security requirements for voting systems both in use and in storage. It does not address the physical characteristics of polling places.

## 14.2 Physical Security Requirements for Voting Systems

This subsection defines the physical security requirements for voting systems. It details countermeasures to be implemented by vendors in order to ensure the physical integrity of the voting systems.

## 14.2.1 Physical Port and Access Least Functionality Requirement

➞ **14.2.1-A** Physical Port and Access Point Requirement

The voting system ***SHALL*** only have physical ports and access points that are essential to voting operations such as voting machine upgrades and maintenance, and voting system testing and auditing.

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section 4.3 (Verification of Design Requirements)*

D I S C U S S I O N

Examples of physical ports are USB ports, floppy drives and network connections. Examples of access points are doors, panels and vents.

*Source:* *NIST Special Publication SP800-53 Recommended Security Controls for Federal Information Systems; Configuration Management, CM-7 Least Functionality*

*Impact:*

➞ **14.2.1-B** Physical Port and Access Point Documentation Requirement

As part of the technical data package and user documentation, Vendor ***SHALL*** provide a listing of all ports and access points.

*Applies to:* *Voting System*

*Test Reference:* *Volume V-Section 4.1 (Review of Documentation)*

D I S C U S S I O N

*Source:*

*Impact:*

## 14.2.2 Voting System Boundary Protection Requirements

➞ **14.2.2-A** Physical Port Shutdown Requirement

If a physical connection between voting system components is broken during Activated or Suspended Mode, the affected voting machine port ***SHALL*** be automatically disabled.

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

*Source:* *NIST Special Publication SP800-53 Recommended Security Controls for Federal Information Systems; Systems and Communications Protection, SC-7 Boundary Protection*

*Impact:*

→ **14.2.2-B** Physical Component Alarm Requirement

The voting system ***SHALL*** produce an audible and visual alarm if a connected component is disconnected during the Activated mode

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

*Source:* *NIST Special Publication SP800-53 Recommended Security Controls for Federal Information Systems; Physical and Environmental Protection, PE-6 Monitoring Physical Access*

*Impact:*

→ **14.2.2-C** Physical Component Event Log Requirement

An event log entry that identifies name of effected device ***SHALL*** be generated if a voting system component is disconnected during the Activated mode.

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

See section XX for general requirements related to content of event logs.

*Source:* *NIST Special Publication SP800-53 Recommended Security Controls for Federal Information Systems; Physical and Environmental Protection, PE-8 Access Records*

*Impact:*

➞ **14.2.2-D** Physical Port Re-enablement Requirement

Ports disabled during Activated or Suspended Mode ***SHALL*** only be re-enabled by authorized administrators.

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

See section XX on Access Control.

*Source:* *NIST Special Publication SP800-53 Recommended Security Controls for Federal Information Systems; Systems and Communications Protection, SC-7 Boundary Protection*

*Impact:*

## 14.2.3 Information Flow Requirement

➞ **14.2.3-A** Physical Port Restriction Requirement

Voting systems ***SHALL*** be designed with the capability to restrict physical access to voting machine ports that accommodate removable media, with the exception of ports used to activate a voting session.

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section 4.3 (Design Review)*

D I S C U S S I O N

Floppy, CD or DVD drives might be essential to voting operations during Pre-voting and Post-voting phases of the voting cycle such as machine upgrade, maintenance and testing. Therefore, they will be accessible only to authorized personnel. They should not be accessible to voters during Activated and Suspended phases of the voting cycle. It is paramount that the floppy, CD and DVD drives are not accessed without detection. Vendor may provide for and recommend a combination of procedures and physical measures that allow election officials to differentiate authorized from unauthorized access during all modes of operation such as a system that relies on tamper resistant tape or tags coded with consecutive serial numbers.

*Source:* *NIST Special Publication SP Recommended Security Controls for Federal Information Systems; Physical and Environmental Protection, PE-3 Physical Access Control, PE-4 Access Control for Transmission Medium*

*Impact:*

→ **14.2.3-B** Physical Port Tamper Evidence Requirement

Voting systems ***SHALL*** be designed with the capability to give a physical indication of tampering or unauthorized access to ports and all other access points.

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section 4.3 (Design Review)*

D I S C U S S I O N

Vendor may provide for and recommend a combination of procedures and physical measures that allow election officials to monitor and control access points such as a system that relies on tamper resistant tape of tags coded with consecutive serial numbers.

*Source:* *NIST Special Publication SP800-53 Recommended Security Controls for Federal Information Systems; Physical and Environmental Protection, PE-6 Monitoring Physical Access*

*Impact:*

→ **14.2.3-C** Physical Port Disabling Capability Requirement

Voting machines ***SHALL*** be designed such that physical ports can be manually disabled by an authorized administrator.

*Applies to:* *Voting system*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

*Source:* *NIST Special Publication SP800-53 Recommended Security Controls for Federal Information Systems; Access Control, AC-19 Access Control for Portable and Mobile Devices*

*Impact:*

→ **14.2.3-D** Door Cover and Panel Security Requirement

Access points such as covers and panels ***SHALL*** be secured by locks or by tamper evidence and tamper resistance countermeasures.

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section 4.3 (Design Review)*

DISCUSSION

*Source:* *UL 291, Standard for Automated Teller Systems, Section 5.6.9*

*Impact:*

→ **14.2.3-E** Secure Ballot Box Requirement

Ballot boxes ***SHALL*** be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.

*Applies to:* *Voting system*

*Test Reference:* *Volume V- Section 5.2 (Functional Test), Volume V- Section 4.3 (Design Review)*

DISCUSSION

The goal here is to ensure that poll workers or observers would easily notice if someone has tampered with the ballot box. This requirement can be achieved through locks or seals as a part of tamper evidence and tamper resistance countermeasures described by the use procedures and supplied by the manufacturer.

*Source:*

*Impact:*

## 14.2.4 Physical Encasing Lock and Key Requirements

→ **14.2.4-A** Physical Encasing Lock Requirement

Voting systems ***SHALL*** only make use of locks that have been evaluated to the listing requirements of UL 437 for door locks and locking cylinders or higher.

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

DISCUSSION

*Source:* *UL 437, Standard for Key Locks*

*Impact:*

→ **14.2.4-B** Physical Encasing Lock Access Requirement

Voting systems ***SHALL*** be designed with countermeasures which give a physical indication that unauthorized attempts have been made to access locks.

*Applies to:* *Voting system*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

*Source:*

*Impact:*

→ **14.2.4-C** Locking System Key Requirement

The locking system used in the voting system ***SHALL*** make use of keys that are unique to a jurisdiction.

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section XX (Vendor Attestation)*

D I S C U S S I O N

Election officials may want keying schemes that are more or less restrictive in accordance with their election management practices. The requirement does not mandate a unique key for each piece of voting equipment; but requires vendors to be able to provide a unique key for the voting equipment of a jurisdiction. Note, the requirement does not require vendors to be able to provide unique keys for voting equipment below the jurisdiction level. The requirement supports the ability for different jurisdictions to have unique keys for their equipment, but does not prohibit the use of a common key across jurisdictions.

*Source:*

*Impact:*

## 14.2.5 Unauthorized Physical Access Requirement.

➞ **14.2.5-A** Unauthorized Physical Access Requirement

Any unauthorized physical access ***SHALL*** leave physical evidence that an unauthorized event has taken place.

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

Vendor may provide for and recommend a combination of procedures and physical measures that allow election officials to differentiate authorized from unauthorized access during all modes of operation such as a system that relies on tamper evidence tape or tags coded with consecutive serial numbers.

*Source:*

*Impact:*

➞ **14.2.5-B** Unauthorized Physical Access Documentation Requirement

Vendor ***SHALL*** provide a list of all voting system components to which access must be restricted and a description of the function of each said component.

*Applies to:* *Voting System*

*Test Reference:* *Volume V-Section 4.1 (Review of Documentation)*

D I S C U S S I O N

This list may be included in the technical data package a well as in the user documentation.

*Source:*

*Impact:*

➞ **14.2.5-C** Unauthorized Physical Access Capability Requirement

Voting system ***SHALL*** produce an audible and visual alarm if access to a restricted voting system component is gained during Activated mode.

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

DISCUSSION

See [Usability and Accessibility Section XX] for requirements related to use of color.

*Source:* *NIST Special Publication SP800-53 Recommended Security Controls for Federal Information Systems; Physical and Environmental Protection, PE-2 Physical Access Authorizations*

*Impact:*

## 14.2.6 Physical Countermeasure Use and Testing Documentation Requirements

→ **14.2.6-A** Technical Data Package Documentation Requirement

Vendor ***SHALL*** provide a technical data package that documents the design and implementation of all physical security controls for the voting system and its components.

*Applies to:* *Voting System*

*Test Reference:* *Volume V-Section 4.1 (Review of Documentation)*

DISCUSSION

*Source:*

*Impact:*

→ **14.2.6-B** User Documentation Requirement

Vendor ***SHALL*** provide user documentation explaining the implementation of all physical security controls for the voting system, including model procedures necessary for effective use of countermeasures.

*Applies to:* *Voting System*

*Test Reference:* *Volume V-Section 4.1 (Review of Documentation)*

DISCUSSION

*Source:*

*Impact:*

## 14.2.7 Power Supply Requirements

→ **14.2.7-A** Back-up Power Requirement

Any physical security countermeasures that require power supplies ***SHALL*** have a back up power supply

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

*Source:* *NIST Special Publication SP800-53 Recommended Security Controls for Federal Information Systems; Physical and Environmental Protection, PE-11 Emergency Power*

*Impact:*

→ **14.2.7-B** Power Outage Alarm Requirement

A physical security countermeasure that switches from its primary power supply to its back-up power supply ***SHALL*** give an audible and visual alarm.

*Applies to:* *Voting System*

*Test Reference:* *Volume V- Section 5.2 (Functional Test)*

D I S C U S S I O N

See [Usability and Accessibility Section XX] for requirements related to use of color.

*Source:*

*Impact:*

→ **14.2.7-C Power Usage Requirement**

Vendor ***SHALL*** provide a list of all physical security countermeasures that require power supplies.

*Applies to:* *Voting System*

*Test Reference:* *Volume V-Section 4.1 (Review of Documentation)*

D I S C U S S I O N

*Source:*

*Impact:*

## 14.3 References:

ASTM Standard E 1459-92, Standard Guide for Physical Evidence Labeling (2005). American Society for Testing and Materials publication. Washington, DC: U.S. Government Printing Office.

DCID 6/3, Director of Central Intelligence Directive 6/3 Protecting Sensitive Compartmented Information within Information Systems. (2006). Director of Central Intelligence publication. Washington, DC: U.S. Government Printing Office.

NIST Special Publication SP800-53 Recommended Security Controls for Federal Information Systems, Revision 1, December 2006

UL 437, Standard for Key Locks. (2003). Underwriters Laboratories. Northbrook IL.

UL 291, Standard for Automated Teller Systems. (2003). Underwriters Laboratories. Northbrook IL.

# Chapter 15: Security Documentation

## 15.1 Introduction/Scope

Voting system documentation is divided into the following two groups: Technical Data Package (TDP) and User Documentation (UD). The TDP includes detailed information necessary for test labs to fully test the voting system. This includes technical documentation such as system design and algorithms. The UD includes information necessary for the end user to configure and implement the voting system. This includes user manual information such as descriptions of features and capabilities of the voting system as well as suggested policies and procedures.

Both groups of documentation are essential for efficient and effective security evaluations. The purpose of the documentation is for testing experts to gain an understanding of the voting system device under test (DUT). In addition to understandability, documentation also aids maintainability of the voting system.

Most documentation will be supplied directly by the vendor, however some may be supplied indirectly by reference, e.g. if a vendor is using a standard operating system and there exists adequate documentation of the security properties and mechanisms of that operating system.

## 15.2 Security documentation requirements

This subsection defines the documentation requirements for voting systems. These recommendations apply to the full scope of voting system functionality, including functionality for defining the ballot and other pre-voting functions, as well as functions for casting and storing votes, vote reporting, system logging, and maintenance of the voting system. User documentation includes all public information that is provided to the end users. The Technical Data Package (TDP) includes the user documentation along with other private information that is viewed only by the test labs.

### 15.2.1 General security documentation requirements

General requirements address the high level documentation for a voting system. These are the fundamental documentation requirements upon which other requirements in this section are based.

→ **15.2.1-A** Overall security documentation requirement

Vendors ***SHALL*** document in the TDP all aspects of system design, development, and proper usage that are relevant to system security. This includes, but is not limited to the following:

- System security objectives
- All hardware and software security mechanisms
- Development procedures employed to ensure absence of malicious code
- Initialization, usage, and maintenance procedures necessary to secure operation
- All attacks the system is designed to resist or detect
- Any security vulnerabilities known to the vendor.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of Documentation)*

DISCUSSION

*Source:* *VVSG 2005 Volume I, Section 8.7*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 8.7 by specifying the security related topics needing to be addressed in the TDP.*

→ **15.2.1-B** High level security documentation requirement

Vendors ***SHALL*** provide at a minimum the high level documents listed in Table 1 as part of the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of Documentation)*

DISCUSSION

*Source:* *VVSG 2005 Volume I, Section 8.7*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 8.7 by specifying specific security related documents to be included with the TDP; and what information the documents must contain.*

| DOCUMENT | DESCRIPTION |
|---|---|
| Security Threats Controls | This document shall identify the threats the voting system protects against and the implemented security controls on voting system and system components. |

| DOCUMENT | DESCRIPTION |
|---|---|
| Security Architecture | This document shall provide an architecture level description of how the security requirements are met, to include the various authentication, access control, audit, confidentiality, integrity, and availability requirements. |
| Interface Specification | This document shall describe external interfaces (programmatic, human, and network) provided by each of the computer components of the voting system (examples of components are DRE, Central Tabulator, Independent Audit machine). |
| Design Specification | This document shall provide a high-level design of each voting system component. |
| Development Environment Specification | This document shall provide descriptions of the physical, personnel, procedural, and technical security of the development environment including configuration management, tools used, coding standards used, software engineering model used, and description of developer and independent testing. |
| Security Testing and Vulnerability Analysis Documentation | These documents shall describe security tests performed to identify vulnerabilities and the results of the testing. This also includes testing performed as part of software development, such as unit, module, and subsystem testing. |

Table 15-8 High Level Voting System Documentation

## 15.2.2 Access control documentation requirements

Documentation requirements address the minimum access control information necessary for testing and implementation of the voting system. This includes both public and private information.

NOTE: These requirements have been moved from the documentation section of the Access Control section.

→ **15.2.2-A** General user and TDP documentation requirement

Vendors ***SHALL*** provide user and TDP documentation of access control capabilities of the voting system.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring user and TDP documentation for voting system access control capabilities.*

➞ **15.2.2-B** Access control implementation, configuration, and management user documentation requirement

Vendors ***SHALL*** provide user documentation containing guidelines and usage instructions on implementing, configuring, and managing access control capabilities.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by providing examples of user documentation components.*

➞ **15.2.2-C** Access control policy template user documentation requirement

Vendors ***SHALL*** provide, within the user documentation, an access control policy template or instructions to facilitate the implementation of the access control policy and associated access controls on the voting system.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Access control policy requirements include the minimum baseline policy definitions necessary for testing and implementation of the voting system. The policies may be pre-defined within the voting system or provided as guidelines in the documentation.

*Source:* *VVSG 2005 Volume I, Section 7.2.1*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.2.1 by requiring an access control policy template.*

→ **15.2.2-D** Model access control policy user documentation requirement

Vendors ***SHALL*** provide, within the user documentation, a model access control policy under which the voting system was designed to operate and a description of the hazards of deviating from this policy.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

The model access control policy includes the assumptions that were made when the system was designed, the justification for the policy, and the hazards of deviating from the policy.

*Source:* *VVSG 2005 Volume I, Section 7.2.1*

*Impact:* *This requirement updates VVSG 2005 Volume I, Section 7.2.1 by requiring a model access control policy.*

→ **15.2.2-E** General access control technical specification TDP documentation requirement

Vendors ***SHALL*** provide descriptions and specifications of all access control mechanisms of the voting system including management capabilities of authentication, authorization, and passwords in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

DISCUSSION

Access control mechanisms include those that are designed to permit authorized access to the voting system and prevent unauthorized access to the voting system. Specific examples of access control measures include but are not limited to: Use of data and user authorization, security kernels, computer-generated password keys, and special protocols.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by providing examples of TDP documentation components.*

→ **15.2.2-F** Unauthorized access technical specification TDP documentation requirement

Vendors ***SHALL*** provide descriptions and specifications of methods to prevent unauthorized access to the access control mechanisms of the voting system in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring the TDP to include information on methods to restrict access to the access control mechanisms.*

→ **15.2.2-G** Access control dependant voting system mechanisms TDP documentation requirement

Vendors ***SHALL*** provide descriptions and specifications of all other voting system mechanisms that are dependent upon, support, and interface with access controls in the TDP.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring the TDP to include information on any other voting system mechanisms that interoperate with voting system access control.*

→ **15.2.2-H** Privileged account user documentation requirement

The vendor ***SHALL*** disclose and document information on all privileged accounts included on the voting system.

*Applies to:* *Voting System*

*Test Reference:* *Volume V, Section 4.1 (Review of documentation)*

D I S C U S S I O N

Information on privileged accounts include the name of the account, purpose, capabilities and permissions, and how to disable the account in the user documentation.

*Source:* *VVSG 2005 Volume I, Section 7.2.1.2*

*Impact:* *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by requiring the disclosure of privileged accounts and related information.*

### 15.2.3 XYZ documentation requirements

NOTE: Documentation requirements currently found in other security related sections will be given an appropriate section heading and moved into this chapter; this will consolidate all security related documentation requirements in this chapter.

# Chapter 16: General Requirements

## 16.1 General Design Requirements

Note: The ballot counter requirements from [2] have been converted into functional requirements (Dangling ref: PleaseAddReference_STS_Auditability_MustHaveBallotCounter and Dangling ref: PleaseAddReference_STS_Auditability_BallotCounterAvailability).

➞ **16.1-A** No cheating

Voting systems ***SHALL*** contain no logic or functionality for the purpose of producing fraudulent election results.

*Applies to:* *Voting system*

*Test Reference:* *Verification of Design Requirements, SecurityDiscussion*

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

➞ **16.1-B** Verifiably correct vote recording and tabulation

The vote recording and tabulation logic in a voting system ***SHALL*** be verifiably correct.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.7*

D I S C U S S I O N

The key word in this requirement is "verifiably." If a voting system is designed in such a way that it cannot be shown to count votes correctly despite full access to its designs, source code, etc., then it does not satisfy this requirement.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

→ **16.1-C** Voting system, minimum devices included

Voting systems ***SHALL*** contain at least one EMS and at least one vote-capture device.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.2*

D I S C U S S I O N

All voting systems must be capable of election definition, vote collection, counting and reporting. To accomplish this requires at least one EMS and at least one vote-capture device.

*Source:* *Clarification of [2].*

*Impact:* *Click here to add the Impact*

→ **16.1-D** Paper ballots, separate data from metadata

Paper ballots used by paper-based voting devices ***SHALL*** meet the following standards:

1. Marks that identify the unique ballot style **SHALL** be outside the area in which votes are recorded, so as to minimize the likelihood that these marks will be mistaken for vote responses and the likelihood that recorded votes will obliterate these marks;
2. If alignment marks are used to locate the vote response fields on the ballot, these marks **SHALL** be outside the area in which votes are recorded, so as to minimize the likelihood that these marks will be mistaken for vote responses and the likelihood that recorded votes will obliterate these marks.

*Applies to:* *Paper-based device*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

See also Requirement IV.3.5.4.2-B.

*Source:* *[2] I.3.2.4.2.1.*

*Impact:* *Click here to add the Impact*

→ **16.1-E** Card holder

A frame or fixture for printed ballot cards is optional. However, if such a device is provided, it ***SHALL***:

1. Position the card properly; and

2. Hold the ballot card securely in its proper location and orientation for voting.

*Applies to:* *MMPB*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.4.2.5.*

*Impact:* *Deleted vacuous requirement to "Be of any size and shape consistent with its intended use" and redundant requirement to comply with design, construction, and maintainability requirements.*

➞ **16.1-F** Ballot boxes

Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, ***SHALL***:

1. Incorporate locks and/or seals;
2. Provide specific points where ballots are inserted, with all other points on the box constructed in a manner that prevents ballot insertion; and
3. If needed, contain separate compartments for the segregation of ballots that may require special handling or processing.

*Applies to:* *Paper-based device*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

Requirement III.5.1-F.c should be understood in the context of Requirement III.6.6.3-A.18, Requirement III.6.8.3-A and Requirement III.6.8.3-B. The differing options in how to handle separable ballots mean that separate compartments might not be required. See also Dangling ref: PleaseAddReference_STS_SpecifyLocks.

*Source:* *[2] I.3.2.4.2.6.*

*Impact:* *Deleted vacuous requirement to "Be of any size, shape, and weight commensurate with their intended use."*

➞ **16.1-G** Vote-capture device activity indicator

Programmed vote-capture devices ***SHALL*** include an audible and/or visible activity indicator providing the status of each voting device. This indicator ***SHALL***:

1. Indicate whether the device is in polls-opened or polls-closed state; and
2. Indicate whether a voting session is in progress.

*Applies to:* *Vote-capture device ∧ Programmed device*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

Polls-closed could be broken down into pre-voting and post-voting states as in Volume III Section 7.2 or further divided into separate states for not-yet-tested, testing, ready/not ready (broken), and reporting.

*Source:* *Clarified from [2] I.2.5.1.c and I.3.2.4.3.1.*

*Impact:* *Click here to add the Impact*

→ **16.1-H** Precinct devices operation

Precinct tabulators and vote-capture devices ***SHALL*** be designed for operation in any enclosed facility ordinarily used as a polling place.

*Applies to:* *Precinct tabulator, Vote-capture device*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.2.1 / [6] I.4.1.2.1*

*Impact:* *Click here to add the Impact*

## 16.2 Voting Variations

The purpose of these formulaic requirements is to clarify that support for a given voting variation cannot be asserted at the system level unless device-level support is present. It is not necessarily the case that every device in the system would support every voting variation claimed at the system level; e.g., vote-capture devices used for in-person voting may have nothing in common with the vote-capture devices (typically MMPB) used for absentee voting. However, sufficient devices must be present to enable satisfaction of the system-level claim.

→ **16.2-A** In-person voting, system composition

Systems of the *In-person voting* class ***SHALL*** gather votes using vote-capture devices of the *In-person voting device* class, count votes using tabulators of the *In-person voting device* class, and perform election management tasks using an EMS of the *In-person voting device* class.

*Applies to:* *In-person voting*

*Test Reference:* *Volume V Section 4.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

→ **16.2-B** Absentee voting, system composition

Systems of the *Absentee voting* class ***SHALL*** gather votes using vote-capture devices of the *Absentee voting device* class, count votes using tabulators of the *Absentee voting device* class, and perform election management tasks using an EMS of the *Absentee voting device* class.

*Applies to:* *Absentee voting*

*Test Reference:* *Volume V Section 4.2*

D I S C U S S I O N

If the voting system requires that absentee ballots be counted manually, then it does not conform to the Absentee voting class. However, it may conform to the Review-required ballots class.

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

→ **16.2-C** Review-required ballots, system composition

Systems of the *Review-required ballots* class ***SHALL*** gather votes using vote-capture devices of the *Review-required ballots device* class, count votes using tabulators of the *Review-required ballots device* class, and perform election management tasks using an EMS of the *Review-required ballots device* class.

*Applies to:* *Review-required ballots*

*Test Reference:* *Volume V Section 4.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

→ **16.2-D** Write-ins, system composition

Systems of the *Write-ins* class ***SHALL*** gather votes using vote-capture devices of the *Write-ins device* class, count votes using tabulators of the *Write-ins* device class, and perform election management tasks using an EMS of the *Write-ins device* class.

*Applies to:* *Write-ins*

*Test Reference:* *Volume V Section 4.2*

DISCUSSION

If the voting system requires that write-in votes be counted manually, then it does not conform to the Write-ins class. However, it may conform to the *Review-required ballots* class.

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

→ **16.2-E** Split precincts, system composition

Systems of the *Split precincts class* ***SHALL*** gather votes using vote-capture devices of the *Split precincts device* class, count votes using tabulators of the *Split precincts device* class, and perform election management tasks using an EMS of the *Split precincts device* class.

*Applies to:* *Split precincts*

*Test Reference:* *Volume V Section 4.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

→ **16.2-F** Straight party voting, system composition

Systems of the *Straight party voting* class ***SHALL*** gather votes using vote-capture devices of the *Straight party voting device* class, count votes using tabulators of the *Straight party voting device* class, and perform election management tasks using an EMS of the *Straight party voting device* class.

*Applies to:* *Straight party voting*

*Test Reference:* *Volume V Section 4.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

↳ **16.2-F.1** Cross-party endorsement, system composition

Systems of the *Cross-party endorsement* class ***SHALL*** gather votes using vote-capture devices of the *Cross-party endorsement device* class, count votes using tabulators of the *Cross-party endorsement device* class, and perform election management tasks using an EMS of the *Cross-party endorsement device* class.

*Applies to:* *Cross-party endorsement*

*Test Reference:* *Volume V Section 4.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

→ **16.2-G** Ballot rotation, system composition

Systems of the *Ballot rotation* class ***SHALL*** gather votes using vote-capture devices of the *Ballot rotation device* class, count votes using tabulators of the *Ballot rotation device* class, and perform election management tasks using an EMS of the *Ballot rotation device* class.

*Applies to:* *Ballot rotation*

*Test Reference:* *Volume V Section 4.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

→ **16.2-H** Primary elections, system composition

Systems of the *Primary elections* class ***SHALL*** gather votes using vote-capture devices of the *Primary elections device* class, count votes using tabulators of the *Primary elections device* class, and perform election management tasks using an EMS of the *Primary elections device* class.

*Applies to:* *Primary elections*

*Test Reference:* *Volume V Section 4.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

↳ **16.2-H.1** Closed primaries, system composition

Systems of the *Closed primaries* class ***SHALL*** gather votes using vote-capture devices of the *Closed primaries device* class, count votes using tabulators of the *Closed primaries device* class, and perform election management tasks using an EMS of the *Closed primaries device* class.

*Applies to:* *Closed primaries*

*Test Reference:* *Volume V Section 4.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

↳ **16.2-H.2** Open primaries, system composition

Systems of the *Open primaries* class ***SHALL*** gather votes using vote-capture devices of the *Open primaries device* class, count votes using tabulators of the *Open primaries device* class, and perform election management tasks using an EMS of the *Open primaries device* class.

*Applies to:* *Open primaries*

*Test Reference:* *Volume V Section 4.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

→ **16.2-I** Provisional / challenged ballots, system composition

Systems of the *Provisional / challenged ballots* class ***SHALL*** gather votes using vote-capture devices of the *Provisional / challenged ballots device* class, count votes using tabulators of the *Provisional / challenged ballots device* class, and perform election management tasks using an EMS of the *Provisional / challenged ballots device* class.

*Applies to:* *Provisional / challenged ballots*

*Test Reference:* *Volume V Section 4.2*

DISCUSSION

If the voting system requires that provisional/challenged ballots be counted manually, then it does not conform to the *Provisional / challenged ballots* class. However, it may conform to the *Review-required ballots* class.

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

→ **16.2-J** Cumulative voting, system composition

Systems of the *Cumulative voting* class ***SHALL*** gather votes using vote-capture devices of the *Cumulative voting device* class, count votes using tabulators of the *Cumulative voting device* class, and perform election management tasks using an EMS of the *Cumulative voting device* class.

*Applies to:* *Cumulative voting*

*Test Reference:* *Volume V Section 4.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

→ **16.2-K** N of M voting, system composition

Systems of the *N of M voting* class ***SHALL*** gather votes using vote-capture devices of the *N of M voting device* class, count votes using tabulators of the *N of M voting device* class, and perform election management tasks using an EMS of the *N of M voting device* class.

*Applies to:* *N of M voting*

*Test Reference:* *Volume V Section 4.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

→ **16.2-L** Ranked order voting, system composition

Systems of the *Ranked order voting* class ***SHALL*** gather votes using vote-capture devices of the *Ranked order voting device* class, count votes using tabulators of the *Ranked order voting device* class, and perform election management tasks using an EMS of the *Ranked order voting device* class.

*Applies to:* *Ranked order voting*

*Test Reference:* *Volume V Section 4.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Conformance ramifications of system/device relationship.*

*Impact:* *Click here to add the Impact*

# 16.3 Hardware and Software Performance, General Requirements

This section contains requirements for hardware and software performance:

4. Reliability;
5. Accuracy/error rate; and
6. Electrical/RF.

## 16.3.1 Reliability

Following subsections provide the background and rationale for the reliability benchmarks appearing in Volume III Section 5.3.1.5. Given that there is no "typical" volume or "typical" configuration of voting system with such diversity among the many jurisdictions, it is nevertheless necessary to base the benchmarks on some rough estimates in order that they may be in the correct order of magnitude, albeit not optimal for every case.

### 16.3.1.1 Classes of equipment

Because different classes of voting devices are used in different ways in elections, the kinds of volume against which their reliability is measured and the specific reliability that is required of them are different. The classes of voting devices for which estimates are provided are listed below. Please refer to the definitions of the parenthesized terms in Volume II.

- Central count optical scanner (CCOS)
- Election Management System (EMS)
- Precinct count optical scanner (PCOS)
- Direct Recording Electronic (DRE)
- Electronically-assisted Ballot Marker (EBM)
- Ballot activator (activation device)
- Audit device (audit device)

### 16.3.1.2 Estimated volume per election

The "typical" volumes described below are the volumes that medium-sized jurisdictions in western states need their equipment to handle in a high turn-out election, as of 2006. 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 2000 voters which equals 60 polling places in a mid-sized county.

Central count optical scanner: Medium-sized jurisdictions in western states need their central count equipment to scan 120 000 ballots in an election. Depending upon the actual throughput speeds of the scanners, they use 2 to 8 machines to handle the volume. "Typical" volume for a single scanner is the maximum tabulation rate that the vendor declares for the equipment times 8 hours.

Election Management System: The volume equals the total number of interactions with the vote gathering equipment required by the design configuration of the voting system to collect the election results from all the vote-capture devices.

The typical constant across the systems is that the Election Management System will interact once with each polling place for each class of equipment. Assuming our "typical" county with 60 polling places, one or more DREs in each polling place, and one or more optical scan devices, that totals 2×60=120 transactions per election.

The primary differences in the central count EMS environment are whether the optical scan devices are networked with the EMS or function independently.

In the networked environment, the device will interact with the EMS once per batch (typically around 250 ballots). So 120 000/250=480 interactions.

In the independent environment, the results are handled similar to the polling place uploads. Results are copied off to media and uploaded to the EMS. Since central counting typically occurs over several days—especially in a vote-by-mail environment—the test should include several uploads from each scanner. 2 scanners × 4 days = 8 uploads.

To simplify these different cases to a single benchmark, we use the highest of the volumes (480 transactions), which leads to the lowest failure rate benchmark.

Precinct count optical scanner: Polling place equipment has a maximum number of paper ballots that can be handled before the outtake bins fill up. Usually around 2500.

Direct Recording Electronic: Typical ballot takes 3–5 minutes to vote, so the most a single DRE should be expected to handle are 150–200 voters in a 12 hour election day.

Electronically-assisted Ballot Marker: Typically takes longer to vote than with a DRE. An individual unit should not be expected to handle more than 70 voters on election day.

Ballot activator: The volume use of these devices match the volumes for the polling place, which in our assumed county is 2000/polling place. Our assumed county would have 10–14 DREs/polling place with around 20 tokens. Each token would be used about 100 times.

Audit device: No information available.

The estimated volumes are summarized in Table 4. The estimates for PCOS and CCOS have been generalized to cover precinct tabulator and central tabulator respectively, and a default volume based on the higher of the available estimates has been supplied for other vote-capture devices that may appear in the future. Audit devices are assumed to be comparable to activation devices in the numbers that are deployed.

| 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 |
| precinct tabulator | 2000 ballots | 120 000 ballots |
| DRE | 200 voting sessions | 120 000 voting sessions |

| DEVICE CLASS | ESTIMATED VOLUME PER DEVICE PER ELECTION | ESTIMATED VOLUME PER ELECTION |
|---|---|---|
| EBM | 70 voting sessions | 120 000 voting sessions |
| Other vote-capture device | 200 voting sessions | 120 000 voting sessions |
| activation device | 2000 ballot activations | 120 000 ballot activations |
| audit device | 2000 ballots | 120 000 ballots |

Table 4 Estimated volumes per election by device class

### 16.3.1.3 Manageable failures per election

The term failure is defined in Volume II. 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. Misfeeds of ballots into optical scanners are handled by a separate benchmark (Requirement III.6.8.4-C), so these are not included as failures for the general reliability benchmark.

The following estimates express what failures would be manageable for a mid-sized county in a high-turnout election. Medium-sized counties send out troubleshooters to polling places to replace or resolve problems with machines.

Any failure that results in even one ballot becoming unrecoverable (disenfranchisement) is unacceptable.

Central count optical scanner: No more than one machine breakdown per jurisdiction requiring repairs done by the vendor or highly trained personnel. Medium sized jurisdictions plan on having one backup machine for each election.

Election Management System: This is a critical system that must perform in an extremely time sensitive environment for a mid-sized county over a 3 to 4 hour period election night. Any failure during the test that a requires the vendor or highly trained personnel to recover should disqualify the system. Otherwise, as long as the vendor's documentation provides useable 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 disqualifies the system.

Precinct count optical scanner: 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 vendor or highly trained personnel to repair (e.g., won't boot). No more than 5 % 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 and Electronically-assisted Ballot Marker: No more than 1 % of the machines in an election experience failures that would require the vendor or highly trained personnel to repair (e.g., won't boot) and no more than 3 % of the machines in an election experience failures that require the attention of a troubleshooter (e.g., printer jams, recalibration, etc.).

Ballot activator: The media/token shouldn't fail more than 3 % 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).

Audit device: No information available. If comparable to ballot activators, there should be at least 1 spare.

The manageable failure estimates are summarized in Table 5. A "user-serviceable" failure is one that can be remedied by a troubleshooter and/or election official; a "non-user-serviceable" failure is one that requires the vendor or highly trained personnel to repair.

Please note that the failures are relative to the collection of all devices of a given class, so the value 1 in the row for central tabulator means 1 failure among the 2 to 8 central tabulators that are required to count 120 000 ballots in 8 hours, not 1 failure per device.

| DEVICE CLASS | FAILURE TYPE | MANAGEABLE FAILURES PER ELECTION |
|---|---|---|
| voting device (all) | Disenfranchisement | 0 |
| central tabulator | All[2] | 1 |
| EMS | Non-user-serviceable | 0 |
| EMS | User-serviceable (10 minutes) | 2 |
| precinct tabulator | Non-user-serviceable | 1 |
| precinct tabulator | User-serviceable | 5 % of devices = 3 |
| DRE | Non-user-serviceable | 1 % of devices = 6 |
| DRE | User-serviceable | 3 % of devices = 18 |
| EBM | Non-user-serviceable | 1 % of devices = 17 |
| EBM | User-serviceable | 3 % of devices = 51 |
| Other vote-capture device | Non-user-serviceable | 1 % of devices = 6 |
| Other vote-capture device | User-serviceable | 3 % of devices = 18 |

[2] Apart from misfeeds, which are handled by a separate benchmark, TGDC experience is that central tabulator failures are never user-serviceable.

| DEVICE CLASS | FAILURE TYPE | MANAGEABLE FAILURES PER ELECTION |
|---|---|---|
| activation device | Media/token | 3 % of tokens = 36 |
| activation device | Main unit | 1 |
| audit device | All | 1 |

Table 5 Estimated manageable failures per election by device class

### 16.3.1.4 Derivation of benchmarks

We focus on one class of device and one type of failure at a time, and we assume that each failure is followed by repair or replacement of the affected device. This means that we consider two failures of the same device to be equivalent to one failure of two different devices of the same class. The sense of "*X* % of the machines fail" is thus approximated by a simple failure count, which is *X*/100 times the number of devices. This then must be related to the total volume processed by the entire group of devices over the course of an election.

To reduce the likelihood of an unmanageable situation to an acceptably low level, a benchmark is needed such that the probability of *observing* the number of failures discussed in the previous paragraph for the total volume estimated is "acceptably low." That "acceptably low level" is here defined to be a probability of no more than 1 %, except in the case of disenfranchisement, where the only acceptable probability is 0.

Under the simplifying assumption that failures occur randomly and in a Poisson distribution, the probability of observing *n* or less failures for volume *v* and failure rate *r* is the value of the Poisson cumulative distribution function,

$$P(n, rv) = \sum_{x=0}^{n} \frac{e^{-rv}(rv)^x}{x!}$$

Consequently, given *n* (the maximum manageable number of failures) and *v* (the estimated total volume), the desired benchmark is found by solving P(*n*,*rv*) = 0.99 for *r*. This sets the benchmark such that there remains a 1 % risk that a greater number of failures would occur. In the case of disenfranchisement, that risk is unacceptable; hence the benchmark is simply set to zero.

### 16.3.1.5 Requirements

→ **16.3.1-A** General reliability

Voting systems ***SHALL*** be designed and constructed so that the frequency of equipment malfunctions is reduced to the lowest level consistent with cost constraints.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.3*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.3.4.1.a / [6] I.4.3.1.a*

*Impact:* *Click here to add the Impact*

→ **16.3.1-B** Failure rate benchmark

All devices ***SHALL*** achieve failure rates not exceeding those indicated in Table 6.

*Applies to:* *Voting device*

*Test Reference:* *Volume V Section 5.3.2*

*Source:* *Revised from [2] I.3.4.3 / [6] I.4.3.3*

*Impact:* *Click here to add the Impact*

| DEVICE CLASS | FAILURE TYPE | UNIT OF VOLUME | BENCHMARK |
|---|---|---|---|
| voting device (all) | Disenfranchisement | | 0 |
| central tabulator | All | ballot | $1.237\times10^{-6}$ |
| EMS | Non-user-serviceable | transaction | $2.093\times10^{-5}$ |
| EMS | User-serviceable (10 minutes) | transaction | $9.084\times10^{-4}$ |
| precinct tabulator | Non-user-serviceable | ballot | $1.237\times10^{-6}$ |
| precinct tabulator | User-serviceable | ballot | $6.860\times10^{-6}$ |
| DRE | Non-user-serviceable | voting session | $1.941\times10^{-5}$ |
| DRE | User-serviceable | voting session | $8.621\times10^{-5}$ |
| EBM | Non-user-serviceable | voting session | $8.013\times10^{-5}$ |
| EBM | User-serviceable | voting session | $3.058\times10^{-4}$ |
| Other vote-capture device | Non-user-serviceable | voting session | $1.941\times10^{-5}$ |
| Other vote-capture device | User-serviceable | voting session | $8.621\times10^{-5}$ |

| DEVICE CLASS | FAILURE TYPE | UNIT OF VOLUME | BENCHMARK |
|---|---|---|---|
| activation device | Media/token | ballot activation | $2.027\times10^{-4}$ |
| activation device | Main unit | ballot activation | $1.237\times10^{-6}$ |
| audit device | All | ballot | $1.237\times10^{-6}$ |

Table 16-9 Failure rate benchmarks

→ **16.3.1-C** No single point of failure

All systems ***SHALL*** protect against a single point of failure that would prevent further voting at the polling place.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.2.4.1.a / [6] I.2.1.4.a*

*Impact:* *Click here to add the Impact*

→ **16.3.1-D** Protect against failure of input and storage devices

All systems ***SHALL*** protect against the failure of any data input or storage device.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

AG action item: Needs more testable language.

*Source:* *[2] I.2.2.4.1.e / [6] I.2.1.4.e*

*Impact:* *Click here to add the Impact*

## 16.3.2 Accuracy/error rate

Since accuracy is measured at the system level, it is not necessary to define different benchmarks for different classes of devices.

→ **16.3.2-A** Satisfy integrity constraints

All systems ***SHALL*** satisfy the constraints in Volume III Section 7.3.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.7*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Formalization of general requirements.*

*Impact:* *Click here to add the Impact*

→ **16.3.2-B** End-to-end accuracy benchmark

All systems ***SHALL*** achieve a report total error rate of no more than $8\times10^{-6}$ (1 / 125 000).

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 5.3.3*

D I S C U S S I O N

For the definition of report total error rate, see Requirement V.5.3.3-B.

This benchmark is derived from the "maximum acceptable error rate" used as the lower test benchmark in [6]. That benchmark was defined as a *ballot position* error rate of $2\times10^{-6}$ (1 / 500 000).

Given that there is no "typical" ratio of votes to ballot positions with such diversity among the many jurisdictions, it is nevertheless necessary to base the benchmark on some rough estimates in order that it may be in the correct order of magnitude, albeit not optimal for every case. The rough estimates are as follows. In a presidential election, there will be approximately 20 contests with a vote for 1 on each ballot with an average of 4 candidates, including the write-in position, per contest. (Some states will have fewer contests and some more. A few contests, like President, would have 8–13 candidates; most have 3 candidates including the write-in, and a few have 2 candidates.) The estimated ratio of votes to ballot positions is thus ¼.

For paper-based tabulators, this general requirement is elaborated in Volume III Section 6.8.5.

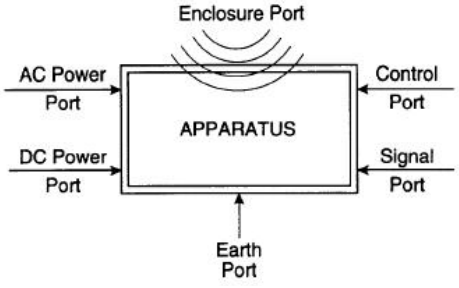
*Source:* *Generalized and clarified from [2] I.3.2.1 / [6] I.4.1.1*

*Impact:* *Click here to add the Impact*

Other accuracy-related requirements include Requirement III.5.4.1.7-D, Requirement III.6.1-E, Requirement III.6.1-F, Requirement III.6.6.4-A, and Requirement III.6.9.3.1-B.

## 16.3.3 Electromagnetic Compatibility (EMC) Immunity

The International Electrotechnical Commission (IEC) Technical Committee 77 on Electromagnetic Compatibility has defined [EMC 16] the concept of "ports" as the interface of an electronic device ("apparatus") with its electrical and electromagnetic environment, as illustrated below. In the sketch, the arrows point toward the apparatus but in a complete assessment of the compatibility, one should also consider the other direction, that is, what disturbances ("emissions") can the apparatus inject into its environment.




Five of these ports involve conducted disturbances carried by metallic conductors, and the sixth, the "enclosure" allows radiated disturbances to impinge on the apparatus. In this context, the term "enclosure" should not be understood as limited to a physical entity (metallic, non metallic, totally enclosed or with openings) but rather be understood as simply the route whereby electromagnetic radiations couple with the circuitry and components of the apparatus.

In previous voting systems guidelines, possible interactions and immunity concerns have been described but perhaps not in explicit terms relating them to the concept of ports. In this updated version of the VVSG, the recitation of compatibility requirements is structured by considering the ports one at a time, plus some consideration of a possible interaction between ports:

7. **Power port** – also described as "power supply" – via ordinary receptacles of the polling place
8. **Earth port** – implied in the NEC stipulations for dealing with the power supply of the polling place
9. **Signal port** – connection to the landline telephone of the polling place to the central tabulator
10. **Control port** – inter-system connections such as voting station to precinct tabulator
11. **Enclosure port** – considerations on immunity to radiated disturbances and electrostatic discharge
12. Interaction between signal port and power port during surge events

### 16.3.3.1 Steady-state Conditions

Adequate operation of an eventual surge-protective device and, more important, safety considerations demand that the power supply receptacles be of the three-prong type (Line, Neutral, and Equipment Grounding Conductor). The use of a "cheater" adapter for older type receptacles with only two-blade capacity and no dependable grounding conductor should be prohibited. Details on the safety considerations are addressed in Volume III, Section 12.2.8.3.

The requirement of using a dedicated landline telephone service should also be satisfied for polling places.

Steady state conditions of a polling place are generally out of the control of the local jurisdiction.

However, for a polling place to ensure reliable voting, the power supply and telephone service need to be suitable for the purpose. Compliance with the National Electrical Code [EMC 26] is assumed to be required.

→ **16.3.3.1-A** Power Supply – Energy Service Provider

To obtain maximum flexibility of application, the voting system ***SHALL*** be powered by a 120 Vrms, single phase power supply, as available in polling places, derived from typical energy service providers.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 3.1, Inspection*

D I S C U S S I O N

It is assumed that the AC power necessary to operate the voting system will be derived from the existing power distribution system of the facility housing the polling place. This single-phase power may be a leg of a 120/240 V single phase system, or a leg of a 120/208 V three-phase system, at a frequency of 60 Hz, according to the limits defined in [EMC 4], and premises wiring compliant with the [EMC 26], in particular its grounding requirements.

*Source:* *[EMC 26]*

*Impact:* *Click here to add the Impact*

→ **16.3.3.1-B** Telecommunications Services Provider

To avoid compromising voting integrity (accidentally or intentionally), the telephone connection of a voting system ***SHALL*** use a dedicated line (no extensions on the same telephone number) and be compatible with the requirements of the telephone service provider.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 3.1, Inspection*

DISCUSSION

Communications (upon closing of the poll) between the polling place and the central tabulator is expected to be provided exclusively by the landline network of the telephone service provider connected to the facility housing the polling place. The use of cell phone communications is specifically prohibited.

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

### 16.3.3.2 Conducted Disturbances Immunity

As described in the introductory paragraphs of Volume III. Section 16.3.3, several ports of the voting system are gateways to possible electromagnetic disturbances, both inbound and outbound. This subsection dealing with conducted disturbances immunity addresses concerns about the Power Port and the communications ports (a combination of the in-house communications and communications to remote tabulating facilities.

Limitations of outbound conducted disturbances ("emissions" in EMC language) that might inject objectionable interference into the facility power distribution system or the telephone service connection are addressed in Volume III, Section 16.3.4.

→ **16.3.3.2-A** Power Port Disturbances

All electronic voting systems ***SHALL*** withstand conducted electrical disturbances that affect the power ports of the system.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.1.2-A*

DISCUSSION

The power distribution system of the polling place can be expected to be affected by several types of disturbances, ranging from very brief surges (microseconds) to longer durations (milliseconds) and ultimately the possibility of a long-term outage. These are addressed in the following requirements: A.1, A.2, A.3, and A.4.

**NOTE:** *There are several scenarios of accidental conditions that can produce voltages far in excess of the deviations implied by [EMC 4] or [EMC 23], such as loss of a neutral conductor, commingling of distribution systems with low-voltage conductors (knocked down poles, falling tree limbs). Such an event will produce in the building massive failures of equipment other than voting systems, and be obvious to the officials conducting the polling. Hardware failure of the voting system can be expected. Fortunately, the occurrence of such events is quite rare, albeit not impossible, so that such a extreme stress should not be included in the*

*EMC requirements nor in the regimen of national certification testing – provided that the failure mode would not result in a safety hazard.*

*Source:* *[EMC 4], [EMC 10], [EMC 23]*

*Impact:* *Click here to add the Impact*

↳ **16.3.3.2-A.1** Combination Wave

All electronic voting systems ***SHALL*** be able to withstand, without disruption of normal operation or loss of data, a "Combination Wave" surge of 1.2/50 µs for open-circuit voltage and 8/20 µs for short-circuit current.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.1.2-A.1*

D I S C U S S I O N

The so-called "Combination Wave" has been accepted by industry as representative of surges that might occur in low-voltage AC power systems and be imposed on connected loads.

*Source:* *[EMC 10]*

*Impact:* *Click here to add the Impact*

↳ **16.3.3.2-A.2** Ring Waves

All electronic voting systems ***SHALL*** be able to withstand, without disruption of normal operation or loss of data, a "Ring Wave" surge with a 0.5 µs rise time and a decaying oscillation at 100 kHz.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.1.2-A.2*

D I S C U S S I O N

This test waveform, proposed by IEEE since 1980 [14] as a "Standard Waveform," and more recently adopted by the IEC [EMC 21] represents common disturbances on AC power lines but it was not included in previous versions of the VVSG. It originates during disturbances of power flow within the building, an occurrence more frequent than lightning surges. It is less likely than the Combination Wave to produce hardware destruction, but high levels still can produce hardware failure.

The "Power Quality" literature [EMC 24] and some standards [EMC 8] also cite "Decaying Ring Waves" or "Damped Oscillatory Waves" with lower frequencies but lesser amplitudes typically associated with the switching of power-factor correction capacitors. These can be significant for surge-protective device survival and possibly disruption of the operation of switched-mode power supplies. However,

inclusion of the Combination Wave, the Ring Wave, and the Swells in these immunity criteria should be sufficient to ensure immunity against these lower frequency and lower amplitude decaying ring waves.

*Source:* *[EMC 10]*

*Impact:* *Click here to add the Impact*

↳ **16.3.3.2-A.3** Electrical Fast Transient Burst

All electronic voting systems ***SHALL*** be able to withstand, without disruption of normal operation or loss of data, a burst of repetitive fast transients with a waveform of 5/50 ns, each burst lasting 15 ms.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.1.2-A.3*

D I S C U S S I O N

While the fast transients involved in this immunity requirement do not propagate very far and are not expected to travel from the energy supply provider, they can be induced within a facility if cable runs are exposed to switching disturbances in other load circuits. Unlike the preceding two disturbances that are deemed to represent possibly destructive surges, the Electrical Fast Transient (EFT) Burst has been developed to demonstrate equipment immunity to these non-destructive but disruptive transients. Their repetitive profile increases the probability that a disruption might occur when the logic circuits go through a transition. It is important to recognize that this test, which does not represent the actual environment, is one of interference immunity, not a test of withstanding energy stress.

*Source:* *[EMC 10]*

*Impact:* *Click here to add the Impact*

↳ **16.3.3.2-A.4** Outages, Sags and Swells

All electronic voting systems ***SHALL*** be able to withstand, without disruption of normal operation or loss of data, a complete loss of power lasting two hours and also a temporary overvoltage of up to 120 % of nominal system voltage lasting up to 0.5 second, and a permanent overvoltage of up to 110 % of nominal system voltage.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.1.2-A.4*

DISCUSSION

Because the VVSG stipulates a two-hour back up, generally implemented by a floating battery pack, sag immunity is inherently ensured. However, the floating battery, unless buffered by a switch-mode power supply with inherent cut-off in case of a large swell, might not ensure inherent immunity against swells (short duration system overvoltages). The Information Technology industry has adopted a recommendation that IT equipment should be capable to operate correctly for swells reaching 120 % of the nominal system voltage with duration ranging from 3 ms to 0.5 s and permanent overvoltages up to 110 % of nominal system voltage.

*Source:* *[EMC 23]*

*Impact:* *Click here to add the Impact*

→ **16.3.3.2-B** Communications (Telephone) Port Disturbances

All electronic voting systems ***SHALL*** withstand conducted electrical disturbances that affect the telephone ports of the system.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.1.2-B*

DISCUSSION

Voting equipment, by being connected to the outside service provider via premises wiring, can be exposed to a variety of electromagnetic disturbances. These have been classified as lightning-induced, power-fault induced, power contact, Electrical Fast Transient (EFT), and presence of steady-state induced voltage. Within a complex voting system installed in a polling place, there is also a possibility that the various pieces of equipment can be exposed to emissions from other piece of connected equipment. In the context of the VVSG compatibility, not only must the voting system equipment be immune to these disturbances, but also the public switched telephone network must be protected against harm originating from customer premises equipment, in this context the voting system equipment. Protection of the network is discussed in the Volume III, Section 16.3.4. Immunity to disturbances impinging on the voting system telephone port is addressed in the following requirements: B.1, B.2, B.3, B.4, B.5, and B.6.

*Source:* *[EMC 27]*

*Impact:* *Click here to add the Impact*

↳ **16.3.3.2-B.1** Emissions from Other Connected Equipment

All elements of an electronic voting system ***SHALL*** be able to withstand the conducted emissions generated by other elements of the voting system.

*Applies to:* *Electronic device*

*Test Reference:* *Volume 5, Section 5.1.1.2-B.1*

D I S C U S S I O N

This requirement is an issue of inherent compatibility among the diverse elements of a voting system, not compatibility with the polling place environment or subscriber equipment other than those making up the voting system. It is understood and implemented that security requirements dictate that the voting system outgoing communications be provided by a dedicated landline telephone service excluding other subscriber terminal equipment otherwise used by entities occupying the facility when telephone communication with central tabulators is established.

*Source:* *[EMC 27], [EMC 5]*

*Impact:* *Click here to add the Impact*

↳ **16.3.3.2-B.2** Lightning-induced Disturbances

All electronic voting systems ***SHALL*** be able to withstand, without disruption of normal operation or loss of data, the stresses induced into the network by lightning events.

*Applies to:* *Electronic device*

*Test Reference:* *Volume 5, Section 5.1.1.2-B.2*

D I S C U S S I O N

Lightning events (direct flashes to the network or voltages induced in the network by nearby flashes to earth) can be at the origin of voltage surges or current surges impinging upon the interface of the premises with the landline network. The provision of surge protection in the Network Interface Device (primary protection NID) is not universally provided, especially in dense urban locations.

*Source:* *[EMC 27]*

*Impact:* *Click here to add the Impact*

↳ **16.3.3.2-B.3** Power Fault-induced Disturbances

All electronic voting systems ***SHALL*** be able to withstand, without disruption of normal operation or loss of data, the stresses induced into the network by power faults occurring in adjacent power distribution systems.

*Applies to:* *Electronic device*

*Test Reference:* *Volume 5, Section 5.1.1.2-B.3*

D I S C U S S I O N

For overhead telephone landline cables that share the pole with power distribution cables (medium-voltage as well as low-voltage), as well as direct burial of adjacent telephone and power cables, large power system faults can induce significant voltages and the resulting currents in the telephone network.

*Source:* *[EMC 27]*

*Impact:* *Click here to add the Impact*

↳ **16.3.3.2-B.4** Power Contact Disturbances

All electronic voting systems ***SHALL*** be able to withstand, without disruption of normal operation or loss of data, the stresses appearing at the telephone port as a result from an accidental contact between the telephone network cables and nearby power distribution cables.

*Applies to:* *Electronic device*

*Test Reference:* *Volume 5, Section 5.1.1.2-B.4*

D I S C U S S I O N

Outside of the polling place building, accidental contact between the telephone network cables and power distribution cables (sharing poles for overhead, or sharing trenches for underground) can inject substantial 60 Hz current and voltages into the telephone network. Within the polling place facility, while not at high probability, instances have been noted whereby contractors working in a facility can provoke a similar injection of 60 Hz current or voltage into the premises telephone wiring.

*Source:* *[EMC 27]*

*Impact:* *Click here to add the Impact*

↳ **16.3.3.2-B.5** Electrical Fast Transient (EFT)

All electronic voting systems ***SHALL*** be able to withstand, without disruption of normal operation or loss of data, the disturbances associated with EFT burst.

*Applies to:* *Electronic device*

*Test Reference:* *Volume 5, Section 5.1.2-B.5*

D I S C U S S I O N

Electrical Fast Transient bursts emulate the interference associated with electromagnetic coupling between the premises wiring of the telephone service and the premises wiring of the power distribution system in which switching surges can occur. Because these switching surges are random events, the occurrence of

interference varies with the timing of their occurrence with respect to the transitions of the circuits. It is important to recognize that this requirement deals with interference immunity, not with withstanding energy stress. Immunity against such high-frequency coupling has been added to the requirements listed by [EMC 27], effective January 1, 2008.

*Source:* *[EMC 27], [EMC 19]*

*Impact:* *Click here to add the Impact*

↳ **16.3.3.2-B.6** Steady-state Induced Voltage

All electronic voting systems ***SHALL*** be able to withstand, without disruption of normal operation or loss of data, the disturbances associated with steady-state induced voltages and currents.

*Applies to:* *Electronic device*

*Test Reference:* *Volume 5, Section 5.1.1.2-B.6*

D I S C U S S I O N

Voting systems interfacing with the telephone service provider plant can be subject to the interfering effects of steady-state voltages induced from nearby power lines. Through electromagnetic coupling, normal operating currents on these power lines can induce common-mode (longitudinal) voltages and currents in the outside cable plant. The 60 Hz and 180 Hz components of the induced voltage spectrum can interfere with signaling and supervisory functions for data transmission from a polling place toward a central tabulator. Higher frequencies can produce audible noise in voice-band transmission.

*Source:* *[EMC 27]*

*Impact:* *Click here to add the Impact*

➞ **16.3.3.2-C** Interaction between Power Port and Telephone Port

All electronic voting systems connected to both a power supply and a landline telephone system ***SHALL*** withstand the potential difference caused by the flow of surge current in the facility grounding network.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.1.2-C*

D I S C U S S I O N

A voting system that is powered via its power port to the power distribution system of the facility and to the telephone service provider via its telephone port can experience a potentially damaging stress between the two ports during the

expected operation of the telephone network interface device in the event of a surge occurring in the telephone system.

*Source:* *[EMC 9], [EMC 15]*

*Impact:* *Click here to add the Impact*

### 16.3.3.3 Radiated Disturbances Immunity

This section discusses radiated disturbances impacting the enclosure port of the voting system, including electromagnetic fields originating from adjacent or distant sources, as well as a particular radiation associated with electrostatic discharge.

Emissions limits requirements of radiated (and conducted) disturbances are addressed in Volume III, Section 16.3.4.2.

→ **16.3.3.3-A** Electromagnetic Field Immunity (80 MHz to 6.0 GHz)

All electronic voting systems ***SHALL*** withstand, without disruption of normal operation or loss of data, exposure to radiated electromagnetic fields over the entire frequency range of 80 MHz to 6.0 GHz.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.1.3-A*

DISCUSSION

The proliferation of portable transmitters (cellular telephones and personal communications systems) used by the general population and the common communications transmitters used by security, public safety, amateur radio, and other services increases the likelihood that the voting equipment covered in the VVSG will be exposed to the radiated electromagnetic fields from these devices. Also, other wireless devices (wireless local area networks, etc), communications and broadcast transmitters may be operating in the vicinity and need to be considered. Since it may be impractical to eliminate nearby radio-frequency sources, voting systems must demonstrate immunity to these signals in order to operate to a high standard of reliability. This requirement is intended to ensure intrinsic immunity to the electromagnetic environment.

*Source:* *[EMC 7], [EMC 18], [EMC 22]*

*Impact:* *Click here to add the Impact*

→ **16.3.3.3-B** Electromagnetic Field Immunity (150 kHz to 80 MHz)

All electronic voting systems ***SHALL*** withstand, without disruption of normal operation or loss of data exposure to radio-frequency energy induced on cables in the frequency range of 150 kHz to 80 MHz.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.1.3-B*

D I S C U S S I O N

The dominant coupling mechanism of radiated electromagnetic fields to equipment electronics at frequencies below 80 MHz is considered to be through currents induced on interconnecting cables. At these frequencies, the wavelengths are such that typical circuit components are electrically very small and thus inefficient in coupling energy directly from the radiated electromagnetic fields. The interconnecting cables, on the other hand, tend to be on the order of the signal wavelengths and may act as efficient and possibly resonant antennas. Thus, the radiated electromagnetic fields will efficiently induce currents on these cables which are connected directly to the equipment electronics.

*Source:* *[EMC 7], [EMC 20]*

*Impact:* *Click here to add the Impact*

→ **16.3.3.3-C** Electrostatic Discharge Immunity

All electronic voting systems ***SHALL*** withstand, without disruption of normal operation or loss of data, electrostatic discharges associated with human contact and contact with mobile equipment (service carts, wheelchairs, etc.).

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.1.3-C*

D I S C U S S I O N

Electrostatic discharge events can originate from direct contact between an "intruder" (person or object) charged at a potential different from that of the units of the voting system, or from an approaching person about to touch the equipment – an "air discharge." The resulting discharge current can induce disturbances in the circuits of the equipment.

**Note:** *The immunity addressed in this subsection is concerned with normal operations and procedures at the polling place. It does not include immunity to electrostatic discharges that might occur when service personnel open the enclosure and handle internal components.*

*Source:* *[EMC 3], [EMC 17]*

*Impact:* *Click here to add the Impact*

## 16.3.4 Electromagnetic Compatibility (EMC) Emission Limits

"Emission limits" are the companion of "Immunity Requirements" – both are necessary to achieve electromagnetic compatibility. In contrast with immunity requirements that are expressed as withstand levels for the equipment, emission limits requirements are expressed as compliance with consensus-derived limits on the parameters of the disturbances injected in the electromagnetic environment by the operation of the voting system.

### 16.3.4.1 Conducted Emissions

Electronic voting systems, by their nature, can generate currents or voltages that will exit via their connecting cables to the power supply or to the telephone service provider of the voting facility. To ensure compatibility, industry standards or mandatory regulations have been developed to define maximum levels of such emissions.

→ **16.3.4.1-A** Power Port Connection to the Facility Power Supply

All electronic voting systems installed in a polling place ***SHALL*** comply with emission limits affecting the power supply connection to the energy service provider. according to Federal Regulations [EMC 1].

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.2.1*

D I S C U S S I O N

The normal operation of an electronic system can produce disturbances that will travel upstream an affect the power supply system of the polling place, creating a potential deviation from the expected electromagnetic compatibility of the system. The issue is whether these actual disturbances (after possible mitigation means incorporated in the equipment) reach a significant level to exceed stipulated limits, which include the following categories:

- Harmonic emissions associated with the load current drawn by the voting system. However, given the low values of the current drawn by the voting system, these emissions do not represent a significant issue, as explained in [EMC 13]. They are only mentioned here for the sake of completeness in reciting the range of disturbances and therefore do not require testing.
- High-frequency conducted emissions (distinct from the harmonic spectrum) into the power cord by coupling from high-frequency switching or data transmission inherent to the system operation. These are addressed in the mandatory certification requirements of [EMC 1], Class B.

*Source:* *[EMC 13], [EMC 1]*

*Impact:* *Click here to add the Impact*

→ **16.3.4.1-B** Telephone Port Connection to the Public Network

All electronic voting systems installed in a polling place ***SHALL*** comply with emission limits stipulated by the industry-recognized organizations of telephone service providers Telcordia [EMC 27] and TIA [EMC 5].

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.2.1-A*

D I S C U S S I O N

Regulatory emission limits requirements for protecting the network (public switched telephone network) from harm via customer premises equipment are contained in the source documents [EMC 27], [EMC 5], [EMC 2] and compliance to these documents is considered mandatory for offering the equipment on the market.

*Source:* *[EMC 27], [EMC 5], [EMC 2]*

*Impact:* *Click here to add the Impact*

→ **16.3.4.1-C** Leakage via Grounding Port

All electronic voting systems installed in a polling place ***SHALL*** comply with limits of leakage currents effectively established by the trip threshold of all listed Ground Fault Current Interrupters (GFCI), if any, installed in the branch circuit supplying the voting system.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.3.2-A*

D I S C U S S I O N

Excessive leakage current is objectionable for two reasons:

- For a branch circuit or wall receptacle that could be provided with a GFCI (depending upon the wiring practice applied at the particular polling place), leakage current above the GFCI built-in trip point would cause the GFCI to trip and therefore disable the operation of the system.
- Should the power cord lose the connection to the equipment grounding conductor of the receptacle, a personnel hazard would occur. (Note the prohibition of “cheater” adapters in the discussion of general requirements for the polling place).

This requirement is related to safety considerations as discussed in Volume III, Section 12.2.8.3 “Safety” – in particular the requirement to have the voting system comply with [EMC 29].

**Note:** *According to[26], a bond between the equipment grounding conductor and the neutral conductor is prohibited downstream from the entrance service panel. GFCIs are designed to trip if such a prohibited bond is detected by the GFCI.*

*Source:* *[EMC 28], [EMC 26]*

*Impact:* *Click here to add the Impact*

### 16.3.4.2 Radiated Emissions

→ **16.3.4.2-A** Radiated Radio Frequency Emissions

All electronic voting systems installed in a polling place ***SHALL*** comply with emission limits according to the Rules and Regulations of the Federal Communications Commission, Part 15, Class B [EMC 1] for radiated radio-frequency emissions.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.2.2-A*

D I S C U S S I O N

Electronic equipment in general and modern high-speed digital electronic circuits in particular have the potential to produce unintentional radiated and conducted radio-frequency emissions over wide frequency ranges. These unintentional signals can interfere with the normal operation of other equipment, especially radio receivers, in close proximity. The requirements of [EMC 1] and [EMC 6] are intended to minimize this possible interference and control the level of unwanted radio-frequency signals in the environment.

*Source:* *[EMC 1]*

*Impact:* *Click here to add the Impact*

## 16.3.5 Other Requirements

In addition to the requirements associated with EMC discussed in the preceding sections, there are other requirements, including dielectric withstand, personnel safety considerations (addressed in Volume III, Section 12.2.8.3) and hardware failure modes (which can also be a safety issue) [EMC 29].

### 16.3.5.1 Dielectric Withstand

→ **16.3.5.1-A** Dielectric Stresses

All electronic voting systems ***SHALL*** be able to withstand the dielectric test stresses associated with connection to the network, characterized by limits of the admissible leakage current.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V, Section 5.1.3.1-A*

D I S C U S S I O N

Dielectric withstand requirements stipulated by industry-consensus telephone requirements as a condition for connecting equipment to their network involve the insulation and leakage current limits between elements of the voting system hardware, including the following:

- Network and device or accessible circuitry which might in turn connect to the user
- Network and hazardous power system
- Power equipment

*Source:* *[EMC 27]*

*Impact:* *Click here to add the Impact*

## 16.4 Workmanship

This section contains requirements for voting system materials, and for good design and construction workmanship for software and hardware:

13. Software engineering practices;
14. Quality assurance and configuration management;
15. General build quality;
16. Durability;
17. Security and audit architectural requirements;
18. Maintainability;
19. Temperature and humidity; and
20. Equipment transportation and storage.

## 16.4.1 Software engineering practices

This section describes essential design and performance characteristics of the logic used in voting systems. The requirements of this section are intended to ensure that voting system logic is reliable, robust, testable, and maintainable.

The general requirements of this section apply to logic used to support the entire range of voting system activities. Although this section emphasizes software, the standards described also influence hardware design considerations.

While there is no best way to design logic, the use of outdated and ad hoc practices is a risk factor for unreliability, unmaintainability, etc. Consequently, these guidelines require the use of modern programming practices. The use of widely recognized and proven logic design methods will facilitate the analysis and testing of voting system logic.

### 16.4.1.1 Scope

The design requirements of this section apply to all application logic, regardless of the ownership of the logic or the ownership and location of the hardware on which the logic is installed or operates. Although it would be desirable for COTS software to conform to the design requirements on workmanship, its conformity to those requirements could not be assessed without access to the source code; hence, the design requirements are scoped to exclude COTS software. However, where there are functional requirements, the behaviors of COTS software and hardware are constrained. (N.B., the definition of COTS precludes any application logic from receiving a COTS designation.)

Third-party logic, border logic, and configuration data are not required to conform to the design requirements on workmanship, but vendors are required to supply that source code and data to the test lab to enable a complete review of the application logic (Requirement IV.2.4.7.2-E, Requirement IV.2.10-D).

All software used in any manner to support any voting-related activities must meet the requirements for security described in Volume III Chapter 3.

### 16.4.1.2 Selection of programming languages

→ **16.4.1.2-A** Acceptable programming languages

Application logic ***SHALL*** be produced in a high-level programming language that has all of the following control constructs:

1. Sequence;
2. Loop with exit condition (e.g., for, while, and/or do-loops);
3. If/Then/Else conditional;
4. Case conditional; and
5. Block-structured exception handling (e.g., try/throw/catch).

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

The intent of this requirement is clarified in Volume III Section 1.4.5.2 with discussion and examples of specific programming languages.

By excluding border logic, this requirement allows the use of assembly language for hardware-related segments, such as device controllers and handler programs. It also allows the use of an externally-imposed language for interacting with an Application Program Interface (API) or database query engine. However, the special code should be insulated from the bulk of the code, e.g. by wrapping it in callable units expressed in the prevailing language, to minimize the number of places that special code appears. C.f. [51] Rule 2.1: "Assembly language **SHALL** be encapsulated and isolated."

Acceptable programming languages are also constrained by Requirement III.5.4.1.7-A.4 and Requirement III.5.4.1.7-A.5, which effectively prohibit the invention of new languages.

*Source:* *[6] I.5.2.1, I.5.2.4 and II.5.4.1.*

*Impact:* *Click here to add the Impact*

↳ **16.4.1.2-A.1** COTS language extensions are acceptable

Requirement III.5.4.1.2-A may be satisfied by using COTS extension packages to add missing control constructs to languages that could not otherwise conform.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

For example, C99 [31] does not support block-structured exception handling, but the construct can be retrofitted using (e.g.) [49] or another COTS package.

The use of non-COTS extension packages or vendor-specific code for this purpose is not acceptable, as it would place an unreasonable burden on the test lab to verify the soundness of an unproven extension (effectively a new programming language). The package must have a proven track record of performance supporting the assertion that it would be stable and suitable for use in voting systems, just as the compiler or interpreter for the base programming language must.

*Source:* *Tightening of [6] I.5.2.4 and II.5.4.1.*

*Impact:* *Click here to add the Impact*

### 16.4.1.3 Selection of general coding conventions

**16.4.1.3-A** Acceptable coding conventions

Application logic ***SHALL*** adhere to a published, credible set of coding rules, conventions or standards (herein simply called "coding conventions") that enhance the workmanship, security, integrity, testability, and maintainability of applications.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Coding conventions that are excessively specialized or simply inadequate may be rejected on the grounds that they do not enhance one or more of workmanship, security, integrity, testability, and maintainability.

See the discussion for Requirement III.5.4.1.2-A regarding border logic.

*Source:* *Rewrite of [2] I.4.2.6.*

*Impact:* *Click here to add the Impact*

**16.4.1.3-A.1** Published

Coding conventions ***SHALL*** be considered published if and only if they appear in a publicly available book, magazine, journal, or new media with analogous circulation and availability, or if they are publicly available on the Internet.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

This requirement attempts to clarify the "published, reviewed, and industry-accepted" language appearing in previous iterations of the Guidelines, but the intent of the requirement is unchanged.

Following are examples of published coding conventions (links valid as of 2007-02). These are only examples and are not necessarily the best available for the purpose.

- Ada: Christine Ausnit-Hood, Kent A. Johnson, Robert G. Pettit, IV, and Steven B. Opdahl, Eds., Ada 95 Quality and Style, Lecture Notes in Computer Science #1344, Springer-Verlag, 1995-06. Content available at http://www.iste.uni-stuttgart.de/ps/ada-doc/style_guide/cover.html and elsewhere.

- C++: Mats Henricson and Erik Nyquist, Industrial Strength C++, Prentice-Hall, 1997. Content available at http://hem.passagen.se/erinyq/industrial/.
- C#: "Design Guidelines for Class Library Developers," Microsoft. http://www.msdn.microsoft.com/library/default.asp?url=/library/en-us/cpgenref/html/cpconnetframeworkdesignguidelines.asp.
- Java: "Code Conventions for the Java™ Programming Language," Sun Microsystems. http://java.sun.com/docs/codeconv/.

*Source:* *Clarification of [2] I.4.2.6.*

*Impact:* *Click here to add the Impact*

↳ **16.4.1.3-A.2** Credible

Coding conventions ***SHALL*** be considered credible if and only if at least two different organizations with no ties to the creator of the rules or to the vendor seeking certification, and which are not themselves voting equipment vendors, independently decided to adopt them and made active use of them at some time within the three years before certification was first sought.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

DISCUSSION

This requirement attempts to clarify the "published, reviewed, and industry-accepted" language appearing in previous iterations of the Guidelines, but the intent of the requirement is unchanged.

Coding conventions evolve, and it is desirable for voting systems to be aligned with modern practices. If the "three year rule" was satisfied at the time that a system was first submitted for certification, it is considered satisfied for the purpose of subsequent recertifications of that system. However, new systems must meet the three year rule as of the time that they are first submitted for certification, even if they reuse parts of older systems.

*Source:* *Clarification of [2] I.4.2.6.*

*Impact:* *Click here to add the Impact*

### 16.4.1.4 Software modularity and programming

→ **16.4.1.4-A** Modularity

Application logic ***SHALL*** be designed in a modular fashion.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

See module. The modularity rules described here apply to the component submodules of a library.

*Source:* *Extracted and revised from [2] I.4.2.3.*

*Impact:* *Removed untestable requirement on COTS.*

↳ **16.4.1.4-A.1** Module testability

Each module ***SHALL*** have a specific function that can be tested and verified independently of the remainder of the code.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

In practice, some additional modules (such as library modules) may be needed to compile the module under test, but the modular construction allows the supporting modules to be replaced by special test versions that support test objectives.

*Source:* *Extracted and revised from [2] I.4.2.3.a.*

*Impact:* *Click here to add the Impact*

→ **16.4.1.4-B** Module size and grouping

Modules ***SHALL*** be small, easily identifiable, and constructed to be grouped according to functionality.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Revision of [2] II.5.4.2.i, as revised by Section 6.6.4.2, Paragraph i of [3].*[5]

*Impact:* *Click here to add the Impact*

↳ **16.4.1.4-B.1** Callable unit length limit

No more than 50 % of all callable units (functions, methods, operations, subroutines, procedures, etc.) should exceed 25 lines of code in length, excluding comments, blank lines, and initializers for read-only lookup tables; no more than 5 % of all callable units should exceed 60 lines in length; and no callable units should exceed 180 lines in length.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

"Lines," in this context, are defined as executable statements or flow control statements with suitable formatting.

*Source:* *Revision of [2] II.5.4.2.i, as revised by Section 6.6.4.2, Paragraph i of [3].*[5]

*Impact:* *Clarified and updated with module replaced by callable unit. Added exclusion for blank lines and initializers to resolve unintended consequence.*

↳ **16.4.1.4-B.2** Lookup tables in separate files

Read-only lookup tables longer than 25 lines should be placed in separate files from other source code if the programming language permits it.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

### 16.4.1.5 Structured programming

→ **16.4.1.5-A** Block-structured exception handling

Application logic ***SHALL*** handle exceptions using block-structured exception handling constructs.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

See Volume III Section 1.4.5.2.

*Source:* *Extension of [6] requirements for structured programming.*

*Impact:* *Click here to add the Impact*

↳ **16.4.1.5-A.1** Legacy library units must be wrapped

If application logic makes use of any COTS or third-party logic callable units that do not throw exceptions when exceptional conditions occur, those callable units ***SHALL*** be wrapped in callable units that check for the relevant error conditions and translate them into exceptions, and the remainder of application logic ***SHALL*** use only the wrapped version.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

For example, if an application written in C99 [31] + cexcept [49] used the malloc function of libc, which returns a null pointer in case of failure instead of throwing an exception, the malloc function would need to be wrapped. Here is one possible implementation:

```
void *checkedMalloc (size_t size) {
     void *ptr = malloc (size);
     if (!ptr)
          Throw bad_alloc;
     return ptr;
}
#define malloc checkedMalloc
```

Wrapping legacy functions avoids the need to check for errors after every invocation, which both obfuscates the application logic and creates a high likelihood that some or many possible errors will not be checked for.

In C++, it would be preferable to use one of the newer mechanisms that already throw exceptions on failure and avoid use of legacy functions altogether.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

➞ **16.4.1.5-B** Unstructured control flow is prohibited

Application logic ***SHALL*** contain no unstructured control constructs.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

See the discussion for Requirement III.5.4.1.2-A regarding border logic.

*Source:* *Generalization and summary of [6] I.5.2.4 and II.5.4.1.*

*Impact:* *Click here to add the Impact*

↳ **16.4.1.5-B.1** Goto

Arbitrary branches (a.k.a. gotos) are prohibited.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Generalization and summary of [6] I.5.2.4 and II.5.4.1.*

*Impact:* *Click here to add the Impact*

↳ **16.4.1.5-B.2** Intentional exceptions

Exceptions ***SHALL*** only be used for error conditions. Exceptions ***SHALL*** not be used to redirect the flow of control in normal ("non-exceptional") conditions.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

"Intentional exceptions" cannot be used as a substitute for arbitrary branch. Normal, expected events, such as reaching the end of a file that is being read from beginning to end, are not exceptional conditions and should not be implemented using exception handlers.

*Source:* *[2] I.4.2.4.d, II.5.4.1.c / [6] I.5.2.4.a.iii, II.5.4.1*

*Impact:* *Click here to add the Impact*

↳ **16.4.1.5-B.3** Unstructured exception handling

Unstructured exception handling (e.g., On Error GoTo, setjmp/longjmp, or explicit tests for error conditions after every executable statement) is prohibited.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

The internal use of such constructs by a COTS extension package that adds block-structured exception handling to a programming language that otherwise would not have it, as described in Requirement III.5.4.1.2-A.1, is allowed. Analogously, it is not a problem that source code written in a high-level programming language is compiled into low-level machine code that contains arbitrary branches. It is only the direct use of low-level constructs in application logic that presents a problem.

*Source:* *Extension of [6] requirements for structured programming.*

*Impact:* *Click here to add the Impact*

→ **16.4.1.5-C** Separation of code and data

Application logic ***SHALL*** not compile or interpret configuration data as a programming language.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

The requirement in [6] read "Operator intervention or logic that evaluates received or stored data **SHALL** not re-direct program control within a program routine." That attempt to define what it means to compile or interpret data as a programming language caused confusion.

Distinguishing what is a programming language from what is not requires some professional judgment. However, in general, sequential execution of imperative instructions is a characteristic of functional programming languages that should not be exhibited by configuration data. Configuration data must be declarative or informative in nature, not imperative.

For example: it is permissible for configuration data to contain a template that informs a report generating application as to the form and content of a report that it should generate, but it is not permissible for configuration data to contain instructions that are executed to generate a report, essentially embedding the logic of the report generator inside the configuration data.

The reasons for this requirement are (1) mingling code and data is bad design, and (2) embedding logic within configuration data is an evasion of the conformity assessment process for application logic.

See also Requirement III.5.4.1.7-A.4 and Requirement III.5.4.1.7-A.5.

*Source:* *Clarification of [2] I.4.2.4.d and II.5.4.1.c / [6] I.5.2.4.a.iii and II.5.4.1 paragraph 4.*

*Impact:* *Click here to add the Impact*

### 16.4.1.6 Comments

➞ **16.4.1.6-A** Header comments

Application logic modules should include header comments that provide at least the following information for each callable unit (function, method, operation, subroutine, procedure, etc.):

1. The purpose of the unit and how it works (if not obvious);
2. A description of input parameters, outputs and return values, exceptions thrown, and side-effects;
3. Any protocols that must be observed (e.g., unit calling sequences);
4. File references by name and method of access (read, write, modify, append, etc.);
5. Global variables used (if applicable);
6. Audit event generation;
7. Date of creation; and
8. Change log (revision record).

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Header comments and other commenting conventions should be specified by the selected coding conventions in a manner consistent with the idiom of the programming language chosen. If the coding conventions specify a coding style and commenting convention that make header comments redundant, then they may be omitted. Otherwise, in the event that the coding conventions fail to specify the content of header comments, the non-redundant portions of this generic guideline should be applied.

Change logs need not cover the nascent period, but they must go back as far as the first baseline or release that is submitted for certification, and should go back as far as the first baseline or release that is deemed reasonably coherent.

*Source:* *Revised from [2] I.4.2.7.a.*

*Impact:* *Added exceptions and audit events, revised language, other nits. The discussion on change logs responds to a known controversy regarding how far back change logs must go.*

### 16.4.1.7 Executable code and data integrity[4,5]

**16.4.1.7-A** Code coherency

Application logic ***SHALL*** conform to the following subrequirements.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

This is to scope the following subrequirements to application logic. For COTS software where source code is unobtainable, they would be unverifiable.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

**16.4.1.7-A.1** Self-modifying code

Self-modifying code is prohibited.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.4.2.2.*

*Impact:* *The VSS text continues "except under the security provisions outlined in section 6.4.e" but there is no 6.4.e.*

**16.4.1.7-A.2** Remotely loaded code

Remotely loaded code is prohibited.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[3] Section 5.6.2.2.*

*Impact:* *This IEEE-originated tightening of the restrictions in [2] I.4.2.2 makes explicit something that was implied in [2] (many requirements about what must be "resident").*

↳ **16.4.1.7-A.3** Dynamically loaded code

Dynamically loaded code other than COTS libraries or kernel modules that are dynamically loaded or linked is prohibited.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[3] Section 5.6.2.2.*

*Impact:* *This IEEE-originated loosening of the restriction in [2] I.4.2.2 is to avoid outlawing Windows, where there is no alternative to DLLs.*

↳ **16.4.1.7-A.4** Code integrity, no strange compilers

If compiled code is used, it ***SHALL*** only be compiled using a COTS compiler.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

This prohibits the use of arbitrary, nonstandard compilers and consequently the invention of new programming languages.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

↳ **16.4.1.7-A.5** Interpreted code, specific COTS interpreter

If interpreted code is used, it ***SHALL*** only be run under a specific, identified version of a COTS runtime interpreter.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

This ensures (1) that no arbitrary, nonstandard interpreted languages are used, and (2) that the software tested and approved during the certification process does not change behavior because of a change to the interpreter.

*Source:* *[3] Section 5.6.2.2.*

*Impact:* *This IEEE-originated loosening of the restriction in [2] I.4.2.2 is to clarify that interpreted Java is acceptable.*

*Popular belief is that [2] prohibits the use of interpreted code. In fact, [2] implies that interpreted code is acceptable in I.4.2.3 and I.6.2. The controversy probably stems from I.4.2.2, which says "interpreted code is prohibited, except under the security provisions outlined in section 6.4.e" (emphasis added). Section 6.4.e does not exist, so the restrictions on interpreted code are actually undefined.*

*[2] I.4.2.1 mentions Java by name; however, Java can be compiled (e.g., with gcj).*

→ **16.4.1.7-B** Prevent tampering with code

During an election, all programmed devices ***SHALL*** prevent replacement or modification of executable code (e.g., by other programs on the system, by people physically replacing the memory or medium containing the code, or by faulty code).

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

This requirement may be partially satisfied through a combination of read-only memory (ROM), the memory protection implemented by most popular COTS operating systems, error checking as described in Volume III Section 5.4.1.8, and access and integrity controls.

*Source:* *Rewording/expansion of [2] I.4.2.2.*

*Impact:* *Click here to add the Impact*

→ **16.4.1.7-C** Prevent tampering with data

All voting devices ***SHALL*** prevent access to or manipulation of vote data or audit records (e.g., by physical tampering with the medium or mechanism containing the data, by other programs on the system, or by faulty code) except where this access is necessary to conduct the voting process.

*Applies to:* *Voting device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

This requirement may be partially satisfied through a combination of the memory protection implemented by most popular COTS operating systems, error checking as described in Volume III Section 5.4.1.8, and access and integrity controls. Systems using mechanical counters to store vote data must protect the counters from tampering. If vote data are stored on paper, the paper must be protected from tampering. Modification of audit records after they are created is never necessary.

*Source:* *Rewording/expansion of [2] I.4.2.2.*

*Impact:* *Click here to add the Impact*

→ **16.4.1.7-D** Monitor I/O errors

All programmed devices ***SHALL*** provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.2.2.1.e.*

*Impact:* *Click here to add the Impact*

### 16.4.1.8 Error checking[5,6]

This section contains requirements for application logic to avoid, detect, and prevent well-known types of errors that could compromise voting integrity and security. Additional advice from the security perspective is available at [21] and related sites, esp. [22].

→ **16.4.1.8-A** Detect garbage input

All programmed devices ***SHALL*** check information inputs for accuracy, completeness, and validity.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

This general requirement applies to all programmed devices, while the specific ones following are only enforceable for application logic.

*Source:* *[25] [SI-10].*

*Impact:* *Click here to add the Impact*

↳ **16.4.1.8-A.1** Defend against garbage input

All programmed devices ***SHALL*** ensure that inaccurate, incomplete, or invalid inputs do not lead to irreversible error.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.2.5.2.2.f.*

*Impact:* *Click here to add the Impact*

➞ **16.4.1.8-B** Mandatory internal error checking

All application logic that is vulnerable to the following types of errors ***SHALL*** check for these errors at run time and respond defensively when they occur.

1. Out-of-bounds accesses of arrays or strings (includes buffers used to move data);
2. Stack overflow errors;
3. CPU-level exceptions such as address and bus errors, dividing by zero, and the like;
4. Variables that are not appropriately handled when out of expected boundaries;
5. Numeric overflows;
6. Known programming language specific vulnerabilities.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

It is acceptable, even expected, that logic verification will show that some error checks cannot logically be triggered and some exception handlers cannot logically be invoked. These checks and exception handlers are not redundant—they provide defense-in-depth against faults that escape detection during logic verification.

See also Requirement III.6.6.6-A.

*Source:* *[3] Section 5.6.2.2 expansion of [2] I.4.2.2, modified.*

*Impact:* *Did not retain the requirement for case statements to handle every case (agree with public comments that this is counterproductive).*

↳ **16.4.1.8-B.1** Array overflows

If the application logic uses arrays, vectors, or any analogous data structures and the programming language does not provide automatic run-time range checking of the indices, the indices ***SHALL*** be ranged-checked on every access.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Range checking code should not be duplicated before each access. Clean implementation approaches include:

1. Consistently using dedicated accessors (functions, methods, operations, subroutines, procedures, etc.) that range-check the indices;
2. Defining and consistently using a new data type or class that encapsulates the range-checking logic;
3. Declaring the array using a template that causes all accessors to be range-checked; or
4. Declaring the array index to be a data type whose enforced range is matched to the size of the array.

Range-enforced data types or classes may be provided by the programming environment or they may be defined in application logic.

If acceptable values of the index do not form a contiguous range, a map structure may be more appropriate than a vector.

*Source:* *Expansion of [2] I.4.2.2.*

*Impact:* *Expansion was to specify what constitutes an acceptable "control."*

↳ **16.4.1.8-B.2** Stack overflows

If stack overflow does not automatically result in an exception, the application logic ***SHALL*** explicitly check for and prevent stack overflow.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

DISCUSSION

Embedded system developers use a variety of techniques for avoiding stack overflow. Commonly, the stack is monitored and warnings and exceptions are thrown when thresholds are crossed. In non-embedded contexts, stack overflow often manifests as a CPU-level exception related to memory segmentation, in which case it can be handled pursuant to Requirement III.5.4.1.8-B.3 and Requirement III.5.4.1.9-D.2.

*Source:* *Added precision.*

*Impact:* *Click here to add the Impact*

↳ **16.4.1.8-B.3** CPU traps

The application logic ***SHALL*** implement such handlers as are needed to detect and respond to CPU-level exceptions.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

DISCUSSION

For example, under Unix a CPU-level exception would manifest as a signal, so a signal handler is needed. If the platform supports it, it is preferable to translate CPU-level exceptions into software-level exceptions so that all exceptions can be handled in a consistent fashion within the voting application; however, not all platforms support it.

*Source:* *Added precision.*

*Impact:* *Click here to add the Impact*

↳ **16.4.1.8-B.4** Garbage input parameters

All scalar or enumerated type parameters whose valid ranges as used in a callable unit (function, method, operation, subroutine, procedure, etc.) do not cover the entire ranges of their declared data types ***SHALL*** be range-checked on entry to the unit.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

DISCUSSION

This applies to parameters of numeric types, character types, temporal types, and any other types for which the concept of range is well-defined.[7] In cases where the restricted range is frequently used and/or associated with a meaningful concept within the scope of the application, the best approach is to define a new class or

data type that encapsulates the range restriction, eliminating the need for range checks on each use.

This requirement differs from Requirement III.5.4.1.8-A. Requirement III.5.4.1.8-A deals with user input, which is expected to contain errors, while this requirement deals with program internal parameters, which are expected to conform to the expectations of the designer. User input errors are a normal occurrence; the errors discussed here are grounds for throwing exceptions.

*Source:* *Elaboration on Requirement III.5.4.1.8-B.d, which is an expansion of [2] I.4.2.2.*

*Impact:* *Click here to add the Impact*

↳ **16.4.1.8-B.5** Numeric overflows

If the programming language does not provide automatic run-time detection of numeric overflow, all arithmetic operations that could potentially overflow the relevant data type ***SHALL*** be checked for overflow.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

This requirement should be approached in a manner similar to Requirement III.5.4.1.8-B.1. Overflow checking should be encapsulated as much as possible.

*Source:* *Added precision.*

*Impact:* *Click here to add the Impact*

➞ **16.4.1.8-C** Recommended internal error checking

All application logic that is vulnerable to the following types of errors should check for these errors at run time and respond defensively when they occur.

1. Pointer variable errors;
2. Dynamic memory allocation and management errors.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[3] Section 5.6.2.2 expansion of [2] I.4.2.2, modified.*

*Impact:* *Click here to add the Impact*

↳ **16.4.1.8-C.1** Pointers

If application logic uses pointers or a similar mechanism for specifying absolute memory locations, the application logic should validate pointers or addresses before they are used.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Improper overwriting should be prevented in general as required by Requirement III.5.4.1.7-B and Requirement III.5.4.1.7-C. Nevertheless, even if read-only memory would prevent the overwrite from succeeding, an attempted overwrite indicates a logic fault that must be corrected.

Pointer use that is fully encapsulated within a standard platform library is treated as COTS software.

*Source:* *Slight revision of [3] 6.6.4.2.e.*

*Impact:* *This is "should" not "**SHALL**" only because it is very difficult in the general case to validate a pointer. It is easier to design the system in such a way that pointers are not required.*

↳ **16.4.1.8-C.2** Memory mismanagement

If dynamic memory allocation is performed in application logic, the application logic should be instrumented and/or routinely analyzed with a COTS tool for detecting memory management errors.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.4*

D I S C U S S I O N

Dynamic memory allocation that is fully encapsulated within a standard platform library is treated as COTS software.

*Source:* *Added precision.*

*Impact:* *This is "should" not "**SHALL**" only because such tooling may not be available or applicable in all cases. See [23] discussion of supported platforms and the barriers to portability.*

→ **16.4.1.8-D** Nullify freed pointers

If pointers and dynamic memory allocation are used, any pointer variables that remain within scope after the memory they point to is deallocated ***SHALL*** be set to null or marked as invalid (pursuant to the idiom of the programming language used) after the memory they point to is deallocated.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

If this is not done automatically by the programming environment, a callable unit should be dedicated to the task of deallocating memory and nullifying pointers. Equivalently, "smart pointers" like the C++ std::auto_ptr can be used to avoid the problem. One should not add assignments after every deallocation in the source code.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

→ **16.4.1.8-E** React to errors detected

The detection of any of the errors enumerated in Requirement III.5.4.1.8-B and Requirement III.5.4.1.8-C ***SHALL*** be treated as a complete failure of the callable unit in which the error was detected. An appropriate exception ***SHALL*** be thrown and control ***SHALL*** pass out of the unit forthwith.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **16.4.1.8-F** Do not disable error checks

Error checks detailed in Requirement III.5.4.1.8-B and Requirement III.5.4.1.8-C ***SHALL*** remain active in certified production code.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

These errors are incompatible with voting integrity, so masking them is unacceptable.

Vendors should not implement error checks using the C/C++ assert() macro. It is often disabled, sometimes automatically, when software is compiled in production mode. Furthermore, it does not appropriately throw an exception, but instead aborts the program.

"Inevitably, the programmed validity checks of the defensive programming approach will result in run-time overheads and, where performance demands are critical, many checks are often removed from the operational software; their use is restricted to the testing phase where they can identify the misuse of components by faulty designs. In the context of producing complex systems which can never be fully tested, this tendency to remove the protection afforded by programmed validity checks is most regrettable and is not recommended here." [19]

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **16.4.1.8-G** Roles authorized to respond to errors

Exceptions resulting from failed error checks or CPU-level exceptions ***SHALL*** require intervention by an election official or administrator before voting can continue.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

These errors are incompatible with voting integrity, so masking them is unacceptable.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **16.4.1.8-H** Diagnostics

Electronic devices ***SHALL*** include a means of identifying device failure and any corrective action needed.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Generalized from [2] I.2.4.1.2.2.c and I.2.4.1.3.d.*

*Impact:* *Click here to add the Impact*

➞ **16.4.1.8-I** Equipment health monitoring

Electronic devices should proactively detect equipment failures and alert an election official or administrator when they occur.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Response to Issue #2147.*

*Impact:* *Afraid to make this a "**SHALL**" because continual self-test could be too onerous for some kinds of equipment.*

➞ **16.4.1.8-J** Election integrity monitoring

To the extent possible, electronic devices ***SHALL*** proactively detect or prevent basic violations of election integrity (e.g., stuffing of the ballot box or the accumulation of negative votes) and alert an election official or administrator if they occur.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Equipment can only verify those conditions that are within the scope of what the equipment does. However, insofar as the equipment can detect something that is blatantly wrong, it should do so and raise the alarm. This provides defense-in-depth to supplement procedural controls and auditing practices.

*Source:* *Response to Issue #2147.*

*Impact:* *Click here to add the Impact*

### 16.4.1.9 Recovery

For specific requirements regarding misfed paper ballots or hangs during the vote-casting function, see Dangling ref: PleaseAddReference_HFP DRE, review and cast ballot, Requirement III.6.8.4-A and Requirement III.6.8.4-B.

→ **16.4.1.9-A** System **SHALL** survive device failure

All systems ***SHALL*** be capable of resuming normal operation following the correction of a failure in any device.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Extrapolated from [2] I.2.2.3.*

*Impact:* *Click here to add the Impact*

→ **16.4.1.9-B** Failures **SHALL** not compromise voting or audit data

Exceptions and system recovery ***SHALL*** be handled in a manner that protects the integrity of all recorded votes and audit log information.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Extracted and generalized from [2] I.4.2.3.e.*

*Impact:* *Click here to add the Impact*

→ **16.4.1.9-C** Device **SHALL** survive component failure

All voting devices ***SHALL*** be capable of resuming normal operation following the correction of a failure in any component (e.g., memory, CPU, ballot reader, printer) provided that catastrophic electrical or mechanical damage has not occurred.

*Applies to:* *Voting device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Reworded from [2] I.2.2.3.b and c.*

*Impact:* *Click here to add the Impact*

➞ **16.4.1.9-D** Controlled recovery

Error conditions ***SHALL*** be corrected in a controlled fashion so that system status may be restored to the initial state existing before the error occurred.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

"Initial state" refers to the state existing at the start of a logical transaction or operation. Transaction boundaries must be defined in a conscientious fashion to minimize the damage. Language changed to "may" because election officials responding to the error condition might want the opportunity to select a different state (e.g., controlled shutdown with memory dump for later analysis).

*Source:* *Generalization from [2] I.2.2.5.2.2.g.*

*Impact:* *Click here to add the Impact*

↳ **16.4.1.9-D.1** Nested error conditions

Nested error conditions ***SHALL*** be corrected in a controlled sequence so that system status may be restored to the initial state existing before the first error occurred.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Slight relaxation of [2] I.2.2.5.2.2.g.*

*Impact:* *Relaxation was the "**SHALL**" to "may" change mentioned in Requirement III.5.4.1.9-D discussion.*

↳ **16.4.1.9-D.2** Reset CPU error states

CPU-level exceptions ***SHALL*** be handled in a manner that restores the CPU to a normal state and allows the system to log the event and recover as with a software-level exception.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

System developers should test to see how CPU-level exceptions are handled and make any changes necessary to ensure robust recovery. Invocation of any other error routine while the CPU is in an exception handling state is to be avoided—software error handlers often do not operate as intended when the CPU is in an exception handling state.

If the platform supports it, it is preferable to translate CPU-level exceptions into software-level exceptions so that all exceptions can be handled in a consistent fashion within the voting application; however, not all platforms support it.

*Source:* *Added precision.*

*Impact:* *Click here to add the Impact*

➞ **16.4.1.9-E** Coherent checkpoints

When recovering from non-catastrophic failure of a device or from any error or malfunction that is within the operator's ability to correct, the system ***SHALL*** restore the device to the operating condition existing immediately prior to the error or failure, without loss or corruption of voting data previously stored in the device.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.6.1*

D I S C U S S I O N

If, as discussed in Requirement III.5.4.1.9-D, the system is left in something other than the last known good state for diagnostic reasons, this requirement clarifies that it must revert to the last known good state before being placed back into service.

*Source:* *[2] I.2.2.3.a.*

*Impact:* *Click here to add the Impact*

## 16.4.2 Quality assurance and configuration management

The quality assurance and configuration management requirements discussed in this section help assure that voting systems conform with the requirements of the VVSG. Quality Assurance is a vendor function with associated practices that is initiated prior to system development and continues throughout the maintenance life cycle of the voting system. Quality Assurance focuses on building quality into a system and reducing dependence on system tests at the end of the life cycle to detect deficiencies, thus helping ensure that the system:

- Meets stated requirements and objectives;
- Adheres to established standards and conventions;
- Functions consistent with related components and meets dependencies for use within the jurisdiction; and
- Reflects all changes approved during its initial development, internal testing, qualification, and, if applicable, additional certification processes.

Configuration management is a set of activities and associated practices that ensures full knowledge and control of the components of a system, starting with its initial development progressing through its ongoing maintenance and enhancement, and including its operational life cycle.

### 16.4.2.1 Standards Based Framework for Quality Assurance and Configuration Management

The requirement in this section establishes the quality assurance and configuration standards that voting system vendors **SHALL** conform to. The requirement to develop a Quality and Configuration Management manual, and the detailed requirements on that manual, are contained in Volume IV, Chapter 2.

➔ **16.4.2.1-A** List of Standards

Voting system vendors ***SHALL*** implement a quality assurance and configuration management program that is conformant with the recognized ISO standards in these areas:

- ISO 9000:2005 [QACM1]
- ISO 9001:2000 [QACM2]
- ISO 10007:2003 [QACM3]

*Applies to:* *Voting system*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

### 16.4.2.2 Configuration Management Requirements

This section specifies the key configuration management requirements for voting system vendors. The requirements include those of equipment tags and configuration logs. Continuation of the program, in the form of usage logs, is the responsibility of State and local officials.

→ **16.4.2.2-A** Identification of Systems

Each voting system ***SHALL*** have an identification tag that is attached to the main body.

*Applies to:* *Voting system*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **16.4.2.2-A.1** Secure Tag

The tag ***SHALL*** be tamper-resistant and difficult to remove.

*Applies to:* *Voting system*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **16.4.2.2-A.2** Tag Contents

The tag ***SHALL*** contain the following information:

- The voting system model identification in the form of a model number and possibly a model name. The model identification identifies the exact variant or version of the system
- The serial number that uniquely identifies the system

- Identification of the vendor, including address and contact information for technical service, and vendor certification information
- Date of manufacture of the voting system.

*Applies to:* *Voting system*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

→ **16.4.2.2-B** The Voting System Configuration Log

For each voting system manufactured, a Voting System Configuration Log ***SHALL*** be established.

*Applies to:* *Voting system*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.2*

D I S C U S S I O N

The Log is initialized by the configuration data supplied by the vendor. From that point on, it functions like a diary of the system. Entries are made by election officials whenever any change occurs. Every exception, disruption, anomaly, and every failure is recorded. Every time the cover is opened for inspection or a repair or maintenance is performed, an entry details what was done, and what component was changed against what other component, as well as any diagnosis of failures or exceptions.

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **16.4.2.2-B.1** Contents

The Log ***SHALL*** contain the following information:

- The information on the system tag described in Requirement 16.4.2.2-A.2
- The identification of all critical parts, components, and assemblies of the system
- The complete historical record, as developed by the vendor per Volume IV, Requirement 2.1-A.12, of all critical parts, components, and assemblies included in the voting system.

*Applies to:* *Voting system*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.2*

D I S C U S S I O N

The list of critical parts, components, and assemblies should be consistent with the rules for determining which of these entities is critical, as specified in the Quality and Configuration Manual. See Volume IV, Requirement 2.1-A.6.

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **16.4.2.2-B.2** Storage

The Log ***SHALL*** be kept on a medium that allows the writing, but not the modification or deletion, of records.

*Applies to:* *Voting system*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

## 16.4.3 General build quality

→ **16.4.3-A** General build quality

All vendors of voting systems ***SHALL*** practice proper workmanship.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **16.4.3-A.1** High quality products

All vendors ***SHALL*** adopt and adhere to practices and procedures to ensure that their products are free from damage or defect that could make them unsatisfactory for their intended purpose.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.3.4.7.a / [6] I.4.3.7.a*

*Impact:* *Click here to add the Impact*

↳ **16.4.3-A.2** High quality parts

All vendors ***SHALL*** ensure that components provided by external suppliers are free from damage or defect that could make them unsatisfactory or hazardous when used for their intended purpose.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.3.4.7.b / [6] I.4.3.7.b*

*Impact:* *Click here to add the Impact*

→ **16.4.3-B** Suitability of COTS Components

Vendors ***SHALL*** ensure that all COTS components included in their voting systems are designed to be suitable for their intended use under the requirements specified by these Guidelines.

*Applies to:* *Voting system*

*Test Reference:* *Requirement V.4.1-B*

DISCUSSION

For example, if the operating and/or storage environmental conditions specified by the manufacturer of a printer do not meet or exceed the requirements of these Guidelines, a system that includes that printer is not certifiable.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

## 16.4.4 Durability

**16.4.4-A** Durability

Voting systems ***SHALL*** be designed to withstand normal use without deterioration for a period of ten years.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.4.2 / [6] I.4.3.2*

*Impact:* *Click here to add the Impact*

**16.4.4-B** Durability of paper

Paper specified for use with the voting system ***SHALL*** conform to the applicable specifications contained within the Government Paper Specification Standards, February 1999 No. 11, or the government standards that have superseded them.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

This is to ensure that paper records will be of adequate quality to survive the handling necessary for recounts, audits, etc. without problematic degradation. The Government Paper Specification Standards include different specifications for different kinds of paper. As of 2007-04-05, the Government Paper Specification Standards, February 1999 No. 11, are available at http://www.gpo.gov/acquisition/paperspecs.htm.

*Source:* *New requirement (response to issue raised by TGDC).*

*Impact:* *Click here to add the Impact*

## 16.4.5 Maintainability

Maintainability represents the ease with which maintenance actions can be performed based on the design characteristics of equipment and software and the processes the vendor and election officials have in place for preventing failures and for reacting to failures. Maintainability includes the ability of equipment and

software to self-diagnose problems and to make non-technical election workers aware of a problem. Maintainability addresses all scheduled and unscheduled events, which are performed to:

- Determine the operational status of the system or a component;
- Determine if there is a problem with the equipment and be able to take it off-line (out of service) while retaining all cast ballot data;
- Adjust, align, tune, or service components;
- Repair or replace a component having a specified operating life or replacement interval;
- Repair or replace a component that exhibits an undesirable predetermined physical condition or performance degradation;
- Repair or replace a component that has failed;
- Ensure that, by following vendor protocols provided in the TDP, all repairs or replacements of devices or components during election use preserve all stored ballot data and/or election results, as appropriate; and
- Verify the restoration of a component, or the system, to operational status.

Maintainability is determined based on the presence of specific physical attributes that aid system maintenance activities, and the ease with which the testing laboratory can perform system maintenance tasks. Although a more quantitative basis for assessing maintainability, such as the mean time to repair the system, is desirable, laboratory testing of a system is conducted before it is approved for sale and thus before a broader base of maintenance experience can be obtained.

→ **16.4.5-A** Electronic device maintainability

Electronic devices ***SHALL*** exhibit the following physical attributes:

1. Labels and the identification of test points;
2. Built-in test and diagnostic circuitry or physical indicators of condition;
3. Labels and alarms related to failures;
4. Features that allow non-technicians to perform routine maintenance tasks such as update of the system database. AG action item: Fix this.

*Applies to:* *Electronic device*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.4.4.1 / [6] I.4.3.4.1*

*Impact:* *Click here to add the Impact*

→ **16.4.5-B** System maintainability

Voting systems ***SHALL*** allow for:

1. A non-technician to easily detect that the equipment has failed;
2. A trained technician to easily diagnose problems;
3. Easy access to components for replacement;
4. Easy adjustment, alignment, and tuning of components; and
5. Low false alarm rates (i.e., indications of problems that do not exist).

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

Need input from HFP regarding performance measures and appropriate usability tests to assess "easy" and "easily".

*Source:* *[2] I.3.4.4.2 / [6] I.4.3.4.2*

*Impact:* *Click here to add the Impact*

→ **16.4.5-C** Nameplate and labels

All voting devices ***SHALL***:

1. Display a permanently affixed nameplate or label containing the name of the manufacturer or vendor, the name of the device, its part or model number, its revision identifier, its serial number, and if applicable, its power requirements;
2. Display a separate data plate containing a schedule for and list of operations required to service or to perform preventive maintenance, or a reference to where this can be found in the Voting Equipment User Documentation; and
3. Display advisory caution and warning instructions to ensure safe operation of the equipment and to avoid exposure to hazardous electrical voltages and moving parts at all locations where operation or exposure may occur.

*Applies to:* *Voting device*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.4.6.*

*Impact:* *Modified to respond to Issue #1081.*

## 16.4.6 Temperature and humidity

AG action item: Issue with humidity causing opscan ballots to expand or curl and jam the machine: should have been prevented by environmental requirements and testing. Review these requirements in light of the reported failures in Fairfield County, Ohio, 2004-12-15. Is the 5 % to 85 % range adequate? Was it a failure of requirements, a failure of test methods, a failure to test, or a combination? [2] II.4 appears to indicate humidity only as a non-operating test, which would not address the problem.

→ **16.4.6-A** Operating temperature and humidity

Voting systems ***SHALL*** be capable of operation in temperatures ranging from 5 °C to 40 °C (41 °F to 104 °F) and relative humidity from 5 % to 85 %, non-condensing.[8]

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 5.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[3] 5.4.5*[5]

*Impact:* *IEEE gave inconsistent figures for lower bound—assumed that °C is the significant value and corrected.*

AG action item: Extract requirements from [2] II.4 and/or reconcile those with the IEEE derived requirement above.

## 16.4.7 Equipment transportation and storage

Issues raised by CRT: touchscreens going out of calibration and memory packs failing after delivery from central to precinct; high rate of system failure when taken out of storage.

→ **16.4.7-A** Survive transportation

Voting devices designated for storage between elections ***SHALL*** continue to meet all applicable requirements after transit to and from the place of use.

*Applies to:* *Voting device*

*Test Reference:* *Volume V Section 5.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.2.6.a / [6] I.2.5.a, generalized.*

*Impact:* *Click here to add the Impact*

→ **16.4.7-B** Survive storage

Voting devices designated for storage between elections ***SHALL*** continue to meet all applicable requirements after storage between elections.

*Applies to:* *Voting device*

*Test Reference:* *Volume V Section 5.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.2.6.b / [6] I.2.5.b, generalized.*

*Impact:* *Click here to add the Impact*

→ **16.4.7-C** Precinct devices storage

Precinct tabulators and vote-capture devices ***SHALL*** be designed for storage in any enclosed facility ordinarily used as a warehouse, with prominent instructions as to any special storage requirements.

*Applies to:* *Precinct tabulator, Vote-capture device*

*Test Reference:* *Volume V Section 4.3*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.2.1 / [6] I.4.1.2.1*

*Impact:* *Click here to add the Impact*

↳ **16.4.7-C.1** Design for storage and transportation

Precinct tabulators and vote-capture devices ***SHALL***:

1. Provide a means to safely and easily handle, transport, and install polling place equipment, such as wheels or a handle or handles; and
2. Be capable of using, or be provided with, a protective enclosure rendering the equipment capable of withstanding (1) impact, shock

and vibration loads accompanying surface and air transportation, and (2) stacking loads accompanying storage.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.3.3 / [6] I.4.2.3*

*Impact:* *Click here to add the Impact*

➞ **16.4.7-D** Transportation and storage conditions benchmarks

Voting devices ***SHALL*** meet specific minimum performance requirements for transportation and storage.

*Applies to:* *Voting device*

*Test Reference:* *Volume V Section 5.1*

D I S C U S S I O N

The requirements simulate exposure to physical shock and vibration associated with handling and transportation by surface and air common carriers, and to temperature conditions associated with delivery and storage in an uncontrolled warehouse environment.

Action items for AG: (1) investigate the MIL-STDs in the following subrequirements; (2) check whether the MIL-STDs been superseded or withdrawn; (3) determine the right values and/or normative references.

*Source:* *[2] I.3.2.2.14, modified by [3] 5.4.6.*[5]

*Impact:* *Click here to add the Impact*

↳ **16.4.7-D.1** Storage temperature

Voting devices ***SHALL*** withstand high and low storage temperatures ranging from –20 °C to 60 °C (–4 °F to 140 °F).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.2.14.a, modified by [3] 5.4.6.a.*[5]

*Impact:* *Original text read "–4 to +140 degrees Fahrenheit, equivalent to MIL-STD-810D, Methods 501.2 and 502.2, Procedure I-Storage."*

↳ **16.4.7-D.2** Bench handling

Voting devices ***SHALL*** withstand bench handling equivalent to the procedure of MIL-STD-810D, Method 516.3, Procedure VI.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.2.14.b*

*Impact:* *Click here to add the Impact*

↳ **16.4.7-D.3** Vibration

Voting devices ***SHALL*** withstand vibration equivalent to the procedure of MIL-STD-810D, Method 514.3, Category 1—Basic Transportation, Common Carrier.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.2.14.c*

*Impact:* *Click here to add the Impact*

↳ **16.4.7-D.4** Storage humidity

Voting devices ***SHALL*** withstand uncontrolled humidity equivalent to the procedure of MIL-STD-810D, Method 507.2, Procedure I-Natural Hot-Humid.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.2.14.d*

*Impact:* *Click here to add the Impact*

# 16.5 Archival Requirements

## 16.5.1 Archivalness of media

➔ **16.5.1-A** Records last at least 22 months

All systems ***SHALL*** maintain the integrity of election management, voting and audit data, including cast vote records, during an election and for a period of at least 22 months afterward, in temperatures ranging from 5 °C to 40 °C (41 °F to 104 °F) and relative humidity from 5 % to 85 %, non-condensing.

Make sure temperature and humidity remain consistent with Requirement III.5.4.7-A.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.3*

DISCUSSION

See also Requirement III.5.5.2-A, Volume III Section 5.5.3 and Requirement IV.3.4.8-C.

*Source:* *Merged from [2] I.2.2.11 and I.3.2.3.2; temperature and humidity harmonized with Requirement III.5.4.7-A.*

*Impact:* *Click here to add the Impact*

## 16.5.2 Procedures required for correct system functioning

The requirements for voting systems are written assuming that these procedures will be followed.

(Statutory period of retention) All printed copy records produced by the election database and ballot processing systems must be labeled and archived for a period of at least 22 months after the election. ([2] I.2.2.11) See also Requirement III.5.5.1-A and Volume III Section 5.5.3.

## 16.5.3 Period of retention (informative)

This informative subsection provides extended discussion for Requirement III.5.5.1-A and Requirement III.5.5.2-A.

United States Code Title 42, Sections 1974 through 1974e, states that election administrators must preserve for 22 months "all records and paper that came into (their) possession relating to an application, registration, payment of poll tax, or other act requisite to voting." This retention requirement applies to systems that will be used at any time for voting of candidates for federal offices (e.g., Member of Congress, United States Senator, and/or Presidential Elector). Therefore, all systems must provide for maintaining the integrity of voting and audit data during an election and for a period of at least 22 months thereafter.

Because the purpose of this law is to assist the federal government in discharging its law enforcement responsibilities in connection with civil rights and elections crimes, its scope must be interpreted in keeping with that objective. The appropriate state or local authority must preserve all records that may be relevant to the detection and prosecution of federal civil rights or election crimes for the 22-month federal retention period, if the records were generated in connection with an election that was held in whole or in part to select federal candidates. It is important to note that Section 1974 does not require that election officials generate any specific type or classification of election record. However, if a record is generated, Section 1974 comes into force and the appropriate authority must retain the records for 22 months.

For 22-month document retention, the general rule is that all printed copy records produced by the election database and ballot processing systems must be so labeled and archived. Regardless of system type, all audit trail information spelled out in Dangling ref: PleaseAddReference_STS_AuditRecordReqs must be retained in its original format, whether that be real-time logs generated by the system, or manual logs maintained by election personnel. The election audit trail includes not only in-process logs of election night (and subsequent processing of absentee or provisional ballots), but also time logs of baseline ballot definition formats, and system readiness and testing results.

In many voting systems, the source of election-specific data (and ballot styles) is a database or file. In precinct count systems, this data is used to program each machine, establish ballot layout, and generate tallying files. It is not necessary to retain this information on electronic media if there is an official, authenticatable printed copy of all final database information. However, it is recommended that the state or local jurisdiction also retain electronic records of the aggregate data for each device so that reconstruction of an election is possible without data re-entry. The same requirement and recommendation applies to vote results generated by each precinct device or system.

# 16.6 Integratability

Integratability is a quality of systems that makes it easier to adapt them or their exchanged data so that they will cooperate meaningfully for some purpose. Systems that are integratable can be made compatible with some moderate amount of effort, for example, by writing "glue code." Integratability is a weaker concept than what is usually meant by interoperability, which is that the systems will cooperate meaningfully for some purpose "out of the box," without any significant integration effort.

Although assured interoperability of components of any given voting system with components of any other is a feature desired by many jurisdictions, it cannot be achieved through conformity assessment alone. A voting system or device by itself cannot be called "interoperable;" one can only test its capability to interoperate with a specific other system or device. See Volume V Section 3.5.

In and of itself, the ability to export voting data in a transparent format guarantees neither interoperability nor integratability with any particular system. However, it enables integration to occur if the two systems are in fact compatible, and it reduces the barriers to interoperability. The barriers to interoperability are further reduced if all systems support the same commonly agreed upon, industry standard format.

See also [6] I.C.3.2 (data formats for token objects) and Resolution #23-05 (Common Ballot Format Specifications).

→ **16.6-A** Integratability

All systems ***SHALL*** maximize integratability with other systems and/or devices of other systems.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 3.5, Volume V Section 4.3*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Generalized from database design requirements in [2] I.2.2.6, TGDC Resolution #23-05, and some state RFP(s).*

*Impact:* *Click here to add the Impact*

↳ **16.6-A.1** Integratability of election programming data and report data

All Election Management Systems ***SHALL*** maximize integratability with respect to election programming data and report data (the content of vote data reports, audit reports, etc.).

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 3.5, Volume V Section 4.3*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Generalized from database design requirements in [2] I.2.2.6, TGDC Resolution #23-05, and some state RFP(s).*

*Impact:* *Click here to add the Impact*

↳ **16.6-A.2** Integratability of ballot image data

All DREs ***SHALL*** maximize integratability with respect to ballot image data.

*Applies to:* *DRE*

*Test Reference:* *Volume V Section 3.5, Volume V Section 4.3*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Generalized from database design requirements in [2] I.2.2.6, TGDC Resolution #23-05, and some state RFP(s).*

*Impact:* *Click here to add the Impact*

↳ **16.6-A.3** Integratability through open export

The integratability requirement may be met by providing the capability to export data in a royalty-free, published, open format.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

To reduce the barriers to interoperability, vendors should strive to use the same commonly agreed upon, industry standard format. The OASIS EML (Election Markup Language) is gaining recognition as such a format.

*Source:* *Generalized from [2] II.6.3.b and TGDC Resolution #23-05.*

*Impact:* *Click here to add the Impact*

↳ **16.6-A.4** Integratability through open database

The integratability requirement may be met by storing data in a documented schema in a standards-conforming database in such a manner that other applications can read and interpret the data.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

"Standards-conforming" refers to support for a standard query language and standard API.

*Source:* *Drill-down from [2] I.2.2.6.*

*Impact:* *Click here to add the Impact*

# Chapter 17: Requirements by Voting Activity

## 17.1 Election Programming

Election programming is the process by which central election officials use election databases and vendor system software to logically define the voter choices associated with the contents of the ballots.

There are significant variations among the election laws of the 50 states with respect to permissible ballot contents, voting options, and the associated ballot counting logic.

➞ **17.1-A** EMS, ballot definition

The EMS ***SHALL*** provide for the logical definition of the ballot, including the definition of the number of allowable selections for each contest.

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.2.a.*

*Impact:* *Click here to add the Impact*

↳ **17.1-A.1** EMS, ballot definition details

The EMS ***SHALL*** be capable of collecting and maintaining

1. Offices and their associated labels and instructions;
2. Candidate names and their associated labels; and
3. Issues or measures and their associated text.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.1.1.1.b.*

*Impact:* *Click here to add the Impact*

→ **17.1-B** EMS, political and administrative subdivisions

The EMS ***SHALL*** provide for the logical definition of political and administrative subdivisions, where the list of candidates or contests varies between precincts.

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.2.6.a and I.2.3.2.b.*

*Impact:* *Click here to add the Impact*

→ **17.1-C** EMS, election districts

The EMS ***SHALL*** enable central election officials to define multiple election districts.

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.2.6.a.*

*Impact:* *Click here to add the Impact*

→ **17.1-D** EMS, voting variations

The EMS ***SHALL*** enable central election officials to define and identify contests, candidates, and issues using all voting variations indicated in the implementation statement.

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.2.6.b, I.2.2.8.2, I.2.3.2.d.*

*Impact:* *Click here to add the Impact*

↳ **17.1-D.1** EMS, 1-of-M

In all systems, the Election Management System ***SHALL*** allow the definition of contests where the voter is allowed to choose at most one candidate from a list of candidates.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Implicit in [2].*

*Impact:* *Click here to add the Impact*

↳ **17.1-D.2** EMS, yes/no question

In all systems, the Election Management System ***SHALL*** allow the definition of contests where the voter is allowed to vote yes or no on a question.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement / clarification of [2] intent.*

*Impact:* *Click here to add the Impact*

↳ **17.1-D.3** EMS, indicate party affiliations and endorsements

In all systems, the Election Management System ***SHALL*** allow the definition of political parties and the indication of the affiliation and/or endorsements of each candidate.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Implicit in [2].*

*Impact:* *Click here to add the Impact*

↳ **17.1-D.4** EMS, primary elections, partisan and nonpartisan contests

EMSs of the Primary elections device class ***SHALL*** support the definition of both partisan and nonpartisan contests.

*Applies to:* *EMS ∧ Primary elections device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.1-D.5** EMS, write-ins

EMSs of the Write-ins device class ***SHALL*** support the definition of contests that include ballot positions for write-in opportunities.

*Applies to:* *EMS ∧ Write-ins device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.3.1.d.*

*Impact:* *Removed untestable reference to state law.*

↳ **17.1-D.6** EMS, straight party voting

EMSs of the *Straight party voting device* class ***SHALL*** be capable of defining the necessary straight party contest and associated metadata to support the gathering and recording of votes for the slate of candidates endorsed by a given political party.

*Applies to:* *EMS ∧ Straight party voting device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.1-D.7** EMS, cross-party endorsement

EMSs of the *Cross-party endorsement device* class ***SHALL*** be capable of defining the necessary straight party contest and associated metadata to support the gathering and recording of votes for the slate of candidates endorsed by a given political party when a given candidate is endorsed by two or more different political parties.

*Applies to:* *EMS ∧ Cross-party endorsement device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Clarification or extension of existing requirements.*

*Impact:* *Click here to add the Impact*

↳ **17.1-D.8** EMS, split precincts, define precincts and election districts

EMSs of the *Split precincts device* class ***SHALL*** support the definition of election districts and precincts in such a way that a given polling place may serve two or more election districts.

*Applies to:* *EMS ∧ Split precincts device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.1-D.9** EMS, N of M voting

EMSs of the *N of M voting device* class ***SHALL*** be capable of defining contests where the voter is allowed to choose up to a specified number of candidates (N(*r*) > 1, per Volume III Section 7.3) from a list of candidates.

*Applies to:* *EMS ∧ N of M voting device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2, I.2.3.2.a and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.1-D.10** EMS, cumulative voting

EMSs of the *Cumulative voting device* class ***SHALL*** be capable of defining contests where the voter is allowed to allocate up to a specified number of votes (N(*r*) > 1, per Volume III Section 7.3) over a list of candidates however he or she chooses, possibly giving more than one vote to a given candidate.

*Applies to:* *EMS ∧ Cumulative voting device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2, I.2.3.2.a and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.1-D.11** EMS, ranked order voting

EMSs of the *Ranked order voting device* class ***SHALL*** be capable of defining contests where the voter is allowed to rank candidates in a contest in order of preference, as first choice, second choice, etc.

*Applies to:* *EMS ∧ Ranked order voting device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

→ **17.1-E** Election definition accuracy

The EMS ***SHALL*** record the election contests, candidates, issues, and political and administrative subdivisions exactly as defined by central election officials.

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.2.2.1.a / [6] I.2.1.2.a.*

*Impact:* *Added "political and administrative subdivisions."*

→ **17.1-F** Voting options accuracy

The EMS ***SHALL*** record the options for casting and recording votes exactly as defined by central election officials.

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Reworded from [2] I.2.2.2.1.b / [6] I.2.1.2.b.*

*Impact:* *Click here to add the Impact*

→ **17.1-G** EMS, confirm recording of election definition

The EMS ***SHALL*** verify (i.e., actively check and confirm) the correct recording of election definition data to the memory components or persistent storage of the device.

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 4.3*

DISCUSSION

"Memory components or persistent storage" includes on-board RAM, nonvolatile memory, hard disks, optical disks, etc.

*Source:* *[2] I.3.2.3.1.c and e ([6] I.4.1.3.1.c and e), expanded to include persistent storage.*

*Impact:* *Click here to add the Impact*

➞ **17.1-H** EMS, election definition distribution

The EMS ***SHALL*** provide for the generation of master and distributed copies of election definitions as needed to configure each voting device in the system.

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Reworded from [2] I.2.3.2.e.*

*Impact:* *Click here to add the Impact*

## 17.2 Ballot Preparation, Formatting, and Production

➞ **17.2-A** EMS, define ballot styles and select options

The EMS ***SHALL*** enable central election officials to define ballot styles and select voting options.

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.2.2.6.c.*

*Impact:* *Click here to add the Impact*

↳ **17.2-A.1** EMS, auto-format

The EMS ***SHALL*** be capable of automatically formatting ballots in accordance with the requirements for offices, candidates, and choices qualified to be placed on the ballot for each political subdivision and election district.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.1.1.1.a.*

*Impact:* *Click here to add the Impact*

↳ **17.2-A.2** EMS, include votable contests

The EMS ***SHALL*** provide for the inclusion in a given ballot style of any contest in which the voter would be entitled to vote.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Extrapolated from relevant requirements in [2].*

*Impact:* *Click here to add the Impact*

↳ **17.2-A.3** EMS, exclude nonvotable contests

The EMS ***SHALL*** provide for the exclusion from a given ballot style of any contest in which the voter would be prohibited from voting because of place of residence or other such administrative or geographical criteria.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

In systems supporting primary elections, this would include the exclusion of partisan contests that are not votable by the selected political party.

*Source:* *[2] I.2.3.2.c.*

*Impact:* *Click here to add the Impact*

↳ **17.2-A.4** EMS, nonpartisan formatting

The EMS ***SHALL*** uniformly allocate space and fonts used for each office, candidate, and contest such that the voter perceives no active voting position to be preferred to any other.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.1.2.c.*

*Impact:* *Click here to add the Impact*

↳ **17.2-A.5** EMS, jurisdiction-dependent content

The EMS ***SHALL*** enable central election officials to add jurisdiction-dependent text, line art, logos and images to ballot styles.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Reworded from [2] I.3.2.3.1.d*

*Impact:* *Click here to add the Impact*

↳ **17.2-A.6** EMS, primary elections, associate configurations with parties

EMSs of the *Primary elections device* class ***SHALL*** support the association of different ballot configurations with different political parties.

*Applies to:* *EMS ∧ Primary elections device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

In paper-based systems, open primaries have sometimes been handled by printing a single ballot style that merges the contests from all parties, instructing the voter to vote only in the contests applicable to a single party, and rejecting or discarding votes that violate this instruction. To satisfy the requirements for *Primary elections device*, the EMS must be *capable* of associating different ballot configurations with different political parties.

*Source:* *Reworded from [2] I.2.3.1.1.1.d.*

*Impact:* *Click here to add the Impact*

↳ **17.2-A.7** EMS, ballot rotation

EMSs of the *Ballot rotation device* class ***SHALL*** support the production of rotated ballots and/or the activation of ballot rotation functions in vote-capture devices through the inclusion of relevant metadata in distributed election definitions and ballot styles.

*Applies to:* *EMS ∧ Ballot rotation device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.2-A.8** EMS, split precincts, associate ballot configurations

EMSs of the *Split precincts device* class ***SHALL*** support the definition of distinct ballot configurations for voters from two or more election districts that are served by a given polling place.

*Applies to:* *EMS ∧ Split precincts device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

➞ **17.2-B** EMS, ballot style distribution

The EMS ***SHALL*** provide for the generation of master and distributed copies of ballot styles as needed to configure each voting device in the system.

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Reworded from [2] I.2.2.6.d.*

*Impact:* *Click here to add the Impact*

↳ **17.2-B.1** Ballot style **SHALL** be identifiable

The EMS ***SHALL*** generate codes or marks as needed to uniquely identify the ballot style associated with any ballot.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

In paper-based systems, identifying marks would appear on the actual ballots. DREs would make internal use of unique identifiers for ballot styles but would not necessarily present these where the voter would see them.

When different precincts share a common ballot style in a paper-based system, typically it is assumed that the ballots from the two precincts will be kept physically separate, tabulated separately, and attributed to the correct precinct at the time of reporting—even in combined precincts where this imposes procedural overhead.

*Source:* *[2] I.2.3.1.1.1.e.*

*Impact:* *Click here to add the Impact*

➞ **17.2-C** EMS, ballot style reuse

The EMS ***SHALL*** support retention and reuse of ballot styles from one election to the next.

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.1.2.e and g.*

*Impact:* *Click here to add the Impact*

➜ **17.2-D** EMS, ballot style protection

The EMS ***SHALL*** prevent unauthorized modification of any ballot styles.

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 4.6.2, Volume V Section 5.2.4, Volume V Section 5.5*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.1.2.f.*

*Impact:* *Click here to add the Impact*

### 17.2.1 Procedures required for correct system functioning

The requirements for voting systems are written assuming that these procedures will be followed.

See [8] for details.

(Paper ballot production) Central election officials must verify that paper ballots are produced in accordance with vendor specifications.

(Paper ballot production quality) Central election officials must ensure that paper ballots conform to vendor specifications for type of paper stock, weight, size, shape, size and location of field used to record votes, folding, bleed through, and ink for printing. ([2] I.2.3.1.3.1.c)

(Paper ballot field alignment) Central election officials must ensure that the vote response fields can be properly aligned with respect to any ballot marking devices used. ([2] I.2.3.1.1.2.b)

(Paper ballot timing mark alignment) Central election officials must ensure that timing marks align properly with the vote response fields. ([2] I.2.3.1.1.2.c)

## 17.3 Equipment Preparation

This section is to be provided by STS.

# 17.4 Equipment Setup for Security and Integrity

## 17.4.1 Setup for end-to-end cryptographic systems

This section is to be provided by STS.

## 17.4.2 Logic and accuracy testing

The purpose of logic and accuracy testing is to detect malfunctioning and misconfigured devices before polls are opened. It is not a defense against fraud.[9]

Election personnel conduct equipment and system readiness tests prior to the start of an election to ensure that the voting system functions properly, to confirm that system equipment has been properly integrated, and to obtain equipment status and readiness reports. The content of those reports is defined in Volume III Section 6.9.

→ **17.4.2-A** Support L&A testing

All systems ***SHALL*** provide the capabilities to:

1. Verify that all voting devices are properly prepared for an election and collect data that verify equipment readiness;
2. Verify the correct installation and interface of all system equipment;
3. Verify that hardware and software function correctly; and
4. Segregate test data from actual voting data, either procedurally or by hardware/software features.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.4.1, I.2.3.5.a2 and b2 (the second a and b, respectively), I.4.4.2.a.*

*Impact:* *[2] I.2.3.4.1.b moved to Requirement III.6.9.2-C. [2] I.2.3.4.1.e doesn't make sense / do not understand in this context (if you consolidate 10 readys and 1 not-ready, you get not-ready, right?). [2] I.2.3.4.1.a2 (the second a) moved to Requirement V.4.6.1-D. [2] I.2.3.4.1.b2 (the second b) moved to Requirement III.6.4.2-J.*

→ **17.4-B** Built-in self-test and diagnostics

All programmed devices ***SHALL*** include built-in measurement, self-test, and diagnostic software and hardware for monitoring and reporting the system's status and degree of operability.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.2.4.1.j, I.2.2.8.1.a.*

*Impact:* *Click here to add the Impact*

→ **17.4.2-C** Verify proper preparation of ballot styles

The EMS ***SHALL*** enable central election officials to test that ballot styles and programs have been properly prepared and installed.

*Applies to:* *EMS*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.2.6.f, I.4.4.2.c.*

*Impact:* *Click here to add the Impact*

→ **17.4.2-D** Verify proper installation of ballot styles

Programmed devices ***SHALL*** include a capability to automatically verify that the software and ballot styles have been properly selected and installed in the equipment and immediately notify an election official of any errors.

*Applies to:* *Programmed device*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.3.b, I.4.4.2.c.*

*Impact:* *Click here to add the Impact*

→ **17.4.2-E** Verify compatibility between software and ballot styles

Programmed devices ***SHALL*** include a capability to automatically verify that software correctly matches the ballot styles that it is intended to process and immediately notify an election official of any errors.

*Applies to:* *Programmed device*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.3.c, I.4.4.2.c.*

*Impact:* *Click here to add the Impact*

→ **17.4.2-F** Test ballots

Programmed tabulators ***SHALL*** provide the capability for central election officials or election judges to submit test ballots for use in verifying the integrity of the system.

*Applies to:* *Programmed device ∧ Tabulator*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.3.3.s, generalized from DREs; I.4.4.2.d and f.*

*Impact:* *Click here to add the Impact*

→ **17.4.2-G** Conversion testing

Paper-based tabulators ***SHALL*** support conversion testing that uses all potential ballot positions as active positions.

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.4.2.a, I.4.4.2.f.*

*Impact:* *Click here to add the Impact*

➞ **17.4.2-H** Paper-based tabulators, testing calibration

Paper-based tabulators ***SHALL*** support the use of test ballots to test the calibration of the paper-to-digital conversion (i.e. the calibration of optical sensors, the density threshold, and/or the logical reduction of scanned images to binary values, as applicable)

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Interpretation of [2] I.2.3.4.2.b.*

*Impact:* *Original language: Paper-based tabulators **SHALL** support conversion testing of ballots with active position density for systems without pre-designated ballot positions.*

➞ **17.4.2-I** Ballot marker readiness

Paper-based vote-capture devices ***SHALL*** include a means of verifying that the ballot marking mechanism is properly prepared and ready to use.

*Applies to:* *Vote-capture device ∧ Paper-based device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

In the case of manually marked paper ballots this requirement is mostly moot. (Sharpen the pencils.)

*Source:* *[2] I.2.4.1.2.1.a.*

*Impact:* *Click here to add the Impact*

➞ **17.4.2-J** L&A testing, no side-effects

Logic and accuracy testing functions ***SHALL*** introduce no residual side-effects other than audit log entries and status changes to note that the tests have been run with a successful or failed result.

*Applies to:* *Voting device*

*Test Reference:* *Volume V Section 4.3, Volume V Section 5.2*

DISCUSSION

Status changes required to satisfy Requirement III.6.5-A and Requirement III.6.5-B.

*Source:* *[2] I.2.3.4.1.b2 (the second b), significantly revised.*

*Impact:* *As written the original requirement was unsatisfiable.*

↳ **17.4.2-J.1** Isolate test ballots

Programmed tabulators ***SHALL*** ensure that all test data have been expunged before the logic and accuracy test is logged as successful. If the test data have not been expunged the logic and accuracy test ***SHALL*** log as failed.

*Applies to:* *Programmed device ∧ Tabulator*

*Test Reference:* *Volume V Section 4.3, Volume V Section 5.2*

DISCUSSION

Test data must never be reflected in official vote counts for specific candidates or choices.

*Source:* *[2] I.2.4.3.3.t / [6] I.2.3.3.3.v, generalized from DREs; I.4.4.2.e / [6] I.5.4.2.e.*

*Impact:* *Click here to add the Impact*

### 17.4.3 Setup validation

This section is to be provided by STS.

### 17.4.4 Procedures required for correct system functioning

See [8] and [9].

## 17.5 Opening Polls

→ **17.5-A** Programmed device, verify L&A performed

Programmed devices ***SHALL*** provide an internal test or diagnostic capability to verify that all of the tests specified in Volume III Section 6.4 have been successfully completed.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.1.1.a.*

*Impact:* *Click here to add the Impact*

➞ **17.5-B** Programmed device, disable untested devices

Programmed devices ***SHALL*** provide for automatic disabling of an untested device until it has been tested.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.1.1.b.*

*Impact:* *Click here to add the Impact*

➞ **17.5-C** Paper-based tabulator activation

Paper-based tabulators ***SHALL*** include a means of activating the ballot counting device.

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.1.2.2.a.*

*Impact:* *Click here to add the Impact*

➞ **17.5-D** Paper-based tabulator, verify activation

Paper-based tabulators ***SHALL*** include a means of verifying that the ballot counting device has been correctly activated and is functioning properly.

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.1.2.2.b.*

*Impact:* *Click here to add the Impact*

→ **17.5-E** Programmed vote-capture device, open poll function

Programmed vote-capture devices ***SHALL*** provide designated functions for opening the poll.

*Applies to:* *Vote-capture device ∧ Programmed device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.1.3, generalized.*

*Impact:* *Click here to add the Impact*

↳ **17.5-E.1** Programmed vote-capture device, protect open poll function

Programmed vote-capture devices ***SHALL*** include a security seal, a password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the poll-opening function.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.1.3.a.*

*Impact:* *Click here to add the Impact*

↳ **17.5-E.2** Programmed vote-capture device, enforce correct poll opening process

Programmed vote-capture devices ***SHALL*** include a means of enforcing the execution of poll-opening steps in the proper sequence if more than one step is required.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.1.3.b.*

*Impact:* *Click here to add the Impact*

↳ **17.5-E.3** Programmed vote-capture device, verify activation

Programmed vote-capture devices ***SHALL*** include a means of verifying that the system has been correctly activated.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.1.3.c.*

*Impact:* *Click here to add the Impact*

## 17.6 Casting

These functional capabilities include all operations conducted at the polling place by voters and officials while polls are open.

### 17.6.1 Ballot activation

→ **17.6.1-A** DRE and EBP, ballot activation

DREs and EBPs ***SHALL*** support ballot activation.

*Applies to:* *DRE, EBP*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.*

*Impact:* *Click here to add the Impact*

↳ **17.6.1-A.1** DRE and EBP, at most one cast ballot per session

DREs and EBPs ***SHALL*** enable poll workers either to initiate, or to provide the voter with the credentials necessary to initiate, a voting session in which the voter may cast at most one ballot.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

See also Requirement III.6.6.7-B.

*Source:* *[2] I.2.4.2.d, rewritten to respect the limits of what the system can do.*

*Impact:* *Click here to add the Impact*

➞ **17.6.1-B** DRE and EBP, control ballot style

DREs and EBPs ***SHALL*** enable poll workers to control the ballot style(s) made available to the voter, whether presented in printed form or electronic display, such that each voter is permitted to record votes only in contests in which that voter is authorized to vote.

*Applies to:* *DRE, EBP*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

See also Requirement III.6.2-A.2, Requirement III.6.2-A.3, and Requirement III.6.6.7-C. More than one ballot style may be available in the case of open primaries (Requirement III.6.6.1-B.4).

*Source:* *[2] I.2.4.2.a.*

*Impact:* *Click here to add the Impact*

↳ **17.6.1-B.1** DRE and EBP, enable all applicable contests

DREs and EBPs ***SHALL*** activate all portions of the ballot upon which the voter is entitled to vote.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.2.g.*

*Impact:* *Click here to add the Impact*

↳ **17.6.1-B.2** DRE and EBP, disable all non-applicable contests

DREs and EBPs ***SHALL*** disable all portions of the ballot upon which the voter is not entitled to vote.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.2.h.*

*Impact:* *Click here to add the Impact*

↳ **17.6.1-B.3** DRE and EBP, select ballot style for party in primary elections

DREs and EBPs of the Primary elections device class ***SHALL*** enable the selection of the ballot style that is appropriate to the party affiliation declared by the voter in a primary election.

*Applies to:* *DRE ∧ Primary elections device, EBP ∧ Primary elections device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

In paper-based systems, open primaries have sometimes been handled by printing a single ballot style that merges the contests from all parties, instructing the voter to vote only in the contests applicable to a single party, and rejecting or discarding votes that violate this instruction. To use that approach on a DRE or EBP would violate Requirement III.6.6.1-B.2.

*Source:* *[2] I.2.4.2.f.*

*Impact:* *Click here to add the Impact*

↳ **17.6.1-B.4** DRE and EBP, open primaries, party selection should be private

In an open primary on a DRE or EBP, the voter should be allowed to choose a party affiliation at the start of the voting session and vote the appropriate ballot style in privacy (i.e., the choice of affiliation should be private as well as the selection of votes on the ballot).

*Applies to:* *DRE ∧ Open primaries device, EBP ∧ Open primaries device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

→ **17.6.1-C** Activation devices

An activation device ***SHALL*** create a credential sufficient to activate the ballot style selected by the poll worker, and only that ballot style.

*Applies to:* *Activation device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement (response to issue raised by TGDC).*

*Impact:* *Click here to add the Impact*

## 17.6.2 General voting functionality

→ **17.6.2-A** No advertising

The ballot presented to the voter ***SHALL*** not display or link to any advertising or commercial logos of any kind, whether public service, commercial, or political, unless added by central election officials using the functionality described in Requirement III.6.2-A.5.

*Applies to:* *Vote-capture device*

*Test Reference:* *Volume V Section 4.3, Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Clarification of [2] I.2.3.1.3.1.b.*

*Impact:* *Click here to add the Impact*

→ **17.6.2-B** Capture votes

All vote-capture devices ***SHALL*** record the selection and non-selection of individual candidates or choices for each contest.

*Applies to:* *Vote-capture device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.3.1.c.*

*Impact:* *Click here to add the Impact*

## 17.6.3 Voting variations

→ **17.6.3-A** Vote-capture device, voting variations

All vote-capture devices ***SHALL*** support the gathering of votes using all voting variations indicated for them in the implementation statement.

*Applies to:* *Vote-capture device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Extrapolated from [2] I.2.2.8.2 and I.2.4.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.1** Vote-capture device, 1-of-M

All vote-capture devices ***SHALL*** be capable of gathering and recording votes in contests where the voter is allowed to choose at most one candidate from a list of candidates.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4. Extended [2] I.2.4.2.e to all systems.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.2** Vote-capture device, yes/no question

All vote-capture devices ***SHALL*** be capable of gathering and recording votes in contests where the voter is allowed to vote yes or no on a question.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement / clarification of [2] intent.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.3** Vote-capture device, indicate party affiliations and endorsements

All vote-capture devices ***SHALL*** be capable of indicating the affiliation and/or endorsements of each candidate.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.4** Vote-capture device, closed primaries

Vote-capture devices of the *Closed primaries device* class ***SHALL*** be capable of gathering and recording votes within a voting process that assigns

different ballot styles depending on the registered political party affiliation of the voter and supports both partisan and nonpartisan contests.

*Applies to:* *Vote-capture device ∧ Closed primaries device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.5** Vote-capture device, open primaries

Vote-capture devices of the *Open primaries device* class ***SHALL*** be capable of gathering and recording votes within a voting process that assigns different ballot styles depending on the political party chosen by the voter at the time of voting and supports both partisan and nonpartisan contests.

*Applies to:* *Vote-capture device ∧ Open primaries device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

In paper-based systems, open primaries have sometimes been handled by printing a single ballot style that merges the contests from all parties, instructing the voter to vote only in the contests applicable to a single party, and rejecting or discarding votes that violate this instruction. To satisfy the requirements for *Open primaries device*, the vote-capture device must be capable of handling the case where different ballot configurations are associated with different political parties.

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.6** Vote-capture device, write-ins

Vote-capture devices of the *Write-ins device* class ***SHALL*** record the voter's selection of candidates whose names do not appear on the ballot and record as many write-in votes as the voter is allowed, per the definition of N(*r*) in Volume III Section 7.3.

*Applies to:* *Vote-capture device ∧ Write-ins device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.3.1.d.*

*Impact:* *Removed untestable reference to state law.*

↳ **17.6.3-A.7** Vote-capture device, support write-in reconciliation

Vote-capture devices of the *Write-ins device* class ***SHALL*** be capable of gathering and recording votes within a voting process that allows for reconciliation of aliases and double votes.

*Applies to:* *Vote-capture device ∧ Write-ins device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Reconciliation of aliases means allowing central election officials to declare two different spellings of a candidate's name to be equivalent (or not). Reconciliation of double votes means handling the case where, in an N-of-M contest, a voter has attempted to cast multiple votes for the same candidate using the write-in mechanism. See Volume III Section 1.5.4 for details.

*Source:* *Added precision based on clarification of write-in reconciliation process.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.8** Vote-capture device, ballot rotation

Vote-capture devices of the Ballot rotation device class ***SHALL*** be capable of gathering and recording votes when the ordering of candidates in ballot positions within each contest is variable.

*Applies to:* *Vote-capture device ∧ Ballot rotation device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.9** Ballot rotation, equal time for each candidate

Programmed vote-capture devices that enable ballot rotation in a given contest ***SHALL*** alter the ordering of candidates or choices in such a manner that no candidate or choice ***SHALL*** ever have appeared in any particular ballot position two or more times more often than any other.

*Applies to:* *Vote-capture device ∧ Programmed device ∧ Ballot rotation device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

This is less restrictive than requiring sequential rotation. For a contest of *M* candidates, the order may be shuffled randomly after each batch of *M* ballots and rotated sequentially within each batch.

*Source:* *Clarification or extension of existing requirements.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.10** Vote-capture device, straight party voting

Vote-capture devices of the *Straight party voting device* class ***SHALL*** be capable of gathering and recording votes for a special contest in which the selection of a political party implies votes for the candidates endorsed by that party in all straight-party-votable contests on the ballot.

*Applies to:* *Vote-capture device ∧ Straight party voting device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.11** Vote-capture device, cross-party endorsement

Vote-capture devices of the *Cross-party endorsement device* class ***SHALL*** be capable of gathering and recording straight-party votes when a given candidate is endorsed by two or more different political parties.

*Applies to:* *Vote-capture device ∧ Cross-party endorsement device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Clarification or extension of existing requirements.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.12** Vote-capture device, split precincts

Vote-capture devices of the *Split precincts device* class ***SHALL*** be capable of gathering and recording votes in a precinct where there are distinct ballot styles for voters from two or more election districts.

*Applies to:* *Vote-capture device ∧ Split precincts device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.13** Vote-capture device, N of M voting

Vote-capture devices of the *N of M voting device* class ***SHALL*** be capable of gathering and recording votes in contests where the voter is allowed to choose up to a specified number of candidates (N(*r*) > 1, per Volume III Section 7.3) from a list of candidates.

*Applies to:* *Vote-capture device ∧ N of M voting device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.14** Vote-capture device, cumulative voting

Vote-capture devices of the *Cumulative voting device* class ***SHALL*** be capable of gathering and recording votes in contests where the voter is allowed to allocate up to a specified number of votes (N(*r*) > 1, per Volume III Section

7.3) over a list of candidates however he or she chooses, possibly giving more than one vote to a given candidate.

*Applies to:* *Vote-capture device ∧ Cumulative voting device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.15** Vote-capture device, ranked order voting

Vote-capture devices of the *Ranked order voting device* class ***SHALL*** be capable of gathering and recording votes in contests where the voter is allowed to rank candidates in a contest in order of preference, as first choice, second choice, etc.

*Applies to:* *Vote-capture device ∧ Ranked order voting device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.16** Vote-capture device, provisional / challenged ballots

Vote-capture devices of *the Provisional / challenged ballots device* class ***SHALL*** be capable of gathering and recording votes within a voting process that allows the decision whether to count a particular ballot to be deferred until after election day.

*Applies to:* *Vote-capture device ∧ Provisional / challenged ballots device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Unique identification of each provisional/challenged ballot is required. See Requirement III.6.8.2-A.5.

*Source:* *Added precision, based on [2] I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.17** DRE, categorize provisional ballots

DREs of the *Provisional / challenged ballots device* class ***SHALL*** provide the capability to categorize each provisional/challenged ballot.

*Applies to:* *DRE ∧ Provisional / challenged ballots device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Categories (e.g., "regular provisional," "extended hours provisional," "regular extended hours") would be jurisdiction-dependent.

*Source:* *[3] 5.6.5.2.s.2.*[5]

*Impact:* *Click here to add the Impact*

↳ **17.6.3-A.18** Vote-capture device, review-required ballots

Vote-capture devices of the *Review-required ballots device* class ***SHALL*** be capable of gathering and recording votes within a voting process that requires certain ballots to be flagged or separated for review.

*Applies to:* *Vote-capture device ∧ Review-required ballots device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

In some systems and jurisdictions, all ballots containing write-in votes require flagging or separation for review. Support for the class indicates that the system can flag or separate ballots in this manner and include the results of the review in the reported totals (see Volume III Section 2.6.3.1). Other reasons for which ballots are flagged or separated are jurisdiction-dependent. It is assumed that ballot presentation is unchanged for review-required ballots.

*Source:* *Extrapolated from [2] I.2.5.2.*

*Impact:* *Click here to add the Impact*

## 17.6.4 Recording votes

→ **17.6.4-A** Record votes as voted

Vote-capture devices ***SHALL*** record each vote precisely as indicated by the voter.

*Applies to:* *Vote-capture device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.2.2.1.c / [6] I.2.1.2.c.*

*Impact:* *Click here to add the Impact*

↳ **17.6.4-A.1** Records consistent with feedback to voter

All cast vote records and logs ***SHALL*** be consistent with the feedback given to the voter.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision / response to issue raised by TGDC.*

*Impact:* *Click here to add the Impact*

→ **17.6.4-B** DRE, confirm votes recorded

DREs ***SHALL*** verify (i.e., actively check and confirm) the correct addition of voter selections to the memory components or persistent storage of the device.

*Applies to:* *DRE*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

"Memory components or persistent storage" includes on-board RAM, nonvolatile memory, hard disks, optical disks, etc.

*Source:* *[2] I.3.2.4.3.3.c, expanded to include persistent storage.*

*Impact:* *Click here to add the Impact*

→ **17.6.4-C** Casting

All systems ***SHALL*** support the casting of a ballot.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

This does not entail retaining a ballot image. DREs are required to retain ballot images (see Dangling ref: PleaseAddReference_STS_Auditability_HumanReadableCVRs) but other devices might not.

*Source:* *[2] I.2.4. Extended [2] I.2.4.2.e to all systems.*

*Impact:* *Click here to add the Impact*

↳ **17.6.4-C.1** Equipment allows each eligible voter to vote

All systems ***SHALL*** make it possible for each eligible voter to cast a ballot, provided that the limits declared in the implementation statement for each device are not exceeded.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

See also Requirement III.6.6.7-A, Requirement III.6.6.7-B and Requirement III.6.6.7-C.

*Source:* *[2] I.2.4.2.b, generalized to all systems.*

*Impact:* *Click here to add the Impact*

↳ **17.6.4-C.2** Paper-based, must have secure ballot boxes

Systems that include paper-based vote-capture devices ***SHALL*** include secure receptacles for holding voted ballots.

*Applies to:* *Paper-based device ∧ Vote-capture device*

*Test Reference:* *Volume V Section 4.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.4.1.2.1.c.*

*Impact:* *Click here to add the Impact*

→ **17.6.4-D** DRE, cast is committed

DREs ***SHALL*** prevent modification of the voter's vote after the ballot is cast.

*Applies to:* *DRE*

*Test Reference:* *Volume V Section 4.6.2, Volume V Section 5.2.4, Volume V Section 5.5*

D I S C U S S I O N

See also Requirement III.6.6.7-D, cast ballot.

*Source:* *[2] I.2.4.3.3.n.*

*Impact:* *Click here to add the Impact*

## 17.6.5 Redundant records

This section contains design requirements to enhance the recoverability of DRE devices. This is a separate concern from auditability, which is addressed in Dangling ref: PleaseAddReference_STS_Auditability. However, in some systems, the same records might satisfy both these requirements and auditability requirements.

→ **17.6.5-A** DRE, at least two separate copies of CVR

DREs ***SHALL*** record and retain at least two machine-countable copies of each cast vote record.

*Applies to:* *DRE*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

Besides data stored in electronic memory, a paper record with barcodes or EBM-style markings would qualify as machine-countable.

*Source:* *[2] I.2.2.2.2, I.2.2.4.2 and I.3.2.4.3.2.c.*

*Impact:* *Click here to add the Impact*

↳ **17.6.5-A.1** DRE, redundant CVRs on physically separate media

These redundant records ***SHALL*** be written to media that are physically separate from one another (e.g., two separate memory cards or one electronic record and one paper record).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

For improved auditability, it is preferable for the processes and paths used to record separate records to themselves to be as separate as possible, so that the opportunities for a single error to corrupt multiple records in the same way are minimized.

*Source:* *[2] I.2.2.4.2 and I.3.2.4.3.2.c.*

*Impact:* *Converted untestable portions of [6] I.4.1.4.3.b.iii and iv into discussion; removed counterproductive requirement to designate one path as primary. See also Volume III Section 1.4.8.*

## 17.6.6 Respecting limits

➞ **17.6.6-A** Tabulator, prevent counter overflow

When a tabulator can no longer accept another ballot without the potential of overflowing a vote counter or otherwise compromising the integrity of the counts, it ***SHALL*** notify the user or operator and cease to accept new ballots.

*Applies to:* *Tabulator*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Assuming that the counter size is large enough such that the value will never be reached is not adequate. Systems are required to detect and prevent an impending overflow condition.

*Source:* *Clarification of [2] II.5.4.2.g.*

*Impact:* *Click here to add the Impact*

↳ **17.6.6-A.1** DRE, stop when full

When a DRE can no longer accept another ballot without the potential of overflowing a vote counter or otherwise compromising the integrity of the counts, it ***SHALL*** emit appropriate warnings and audit events and cease to activate new ballots.

*Applies to:* *DRE*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

A DRE must not initiate a voting session if there is the possibility that the next ballot could not be properly cast and recorded. If there exists a way of voting the ballot that would exceed one of the limits, then the ballot must not be activated.

*Source:* *Clarification of [2] II.5.4.2.g.*

*Impact:* *Click here to add the Impact*

## 17.6.7 Procedures required for correct system functioning

The requirements for voting systems are written assuming that these procedures will be followed.

(Process allows each eligible voter to vote) The voting process must allow each eligible voter to cast a ballot. ([2] I.2.4.2.b, generalized from DRE systems to the voting process.) See also Requirement III.6.6.4-C.1.

(At most one cast ballot per voter) The voting process must prevent a voter from casting more than one ballot in the same election. ([2] I.2.4.2.d, generalized from DRE systems to the voting process.) See also Requirement III.6.6.1-A.1.

(Process ensures correct ballot style) The voting process must prevent a voter from voting a ballot style to which he or she is not entitled. ([2] I.2.4.2.c, generalized from DRE systems to the voting process.) See also Requirement III.6.2-A.2, Requirement III.6.2-A.3 and Requirement III.6.6.1-B.

(Process prevents vote tampering) The voting process must prevent modification of the voter's vote after the ballot is cast. ([2] I.2.4.3.3.n, generalized.) See also Requirement III.6.6.4-D, cast ballot.

(Early voting, ballot accounting) In the presence of a witness, election judges must record the value of the ballot counter from each tabulator at the end of each active period. (Issue #1366, Issue #2143) See Volume III Section 7.2. This procedure might be facilitated by designated functions of the voting equipment (i.e., printing of special early-voting end-of-day reports that include the timestamp, the value of the ballot counter, and little else).

(Early voting, resumption practices) Election judges returning equipment to the ready state after it has been placed in the suspended state must perform this operation in the presence of a witness, confirm that the equipment recorded no activity, and confirm that the ballot counter is unchanged from the value that was recorded when voting was suspended. See Volume III Section 7.2. This procedure might be facilitated by designated functions of the voting equipment (i.e., printing of special early-voting resumption reports that include the timestamp, the value of the ballot counter, confirmation that nothing happened overnight, and little else).

# 17.7 Closing Polls

➞ **17.7-A** DRE, no CVRs before close of polls

DREs ***SHALL*** prevent access to cast vote records until after the close of polls.

*Applies to:* *DRE*

*Test Reference:* *Volume V Section 4.6.2, Volume V Section 5.2.4, Volume V Section 5.5*

D I S C U S S I O N

This does not apply to paper-based devices because the ballot is subject to handling beyond their control; however, a locked ballot box (per Requirement III.6.6.4-C.2 and Requirement III.5.1-F) serves the same purpose. See also Requirement III.6.7.1-A.

*Source:* *[2] I.2.4.3.3.r.*

*Impact:* *Click here to add the Impact*

➞ **17.7-B** Programmed vote-capture devices, poll-closing function

Programmed vote-capture devices ***SHALL*** provide designated functions for closing the polls.

*Applies to:* *Vote-capture device ∧ Programmed device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Reworded from [2] I.2.5.*

*Impact:* *Click here to add the Impact*

↳ **17.7-B.1** Programmed vote-capture devices, no voting when polls are closed

Programmed vote-capture devices ***SHALL*** prevent the further enabling, activation or marking of ballots by those devices once the polls have closed.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.2, Volume V Section 5.2.4, Volume V Section 5.5*

DISCUSSION

An EBM cannot prevent a voter from marking a paper ballot with a writing utensil after polls have closed. This must be prevented through procedures.

*Source:* *Reworded from [2] I.2.5.1.a.*

*Impact:* *Click here to add the Impact*

↳ **17.7-B.2** DRE, no ballot casting when polls are closed

DREs ***SHALL*** prevent the further casting of ballots once the polls have closed.

*Applies to:* *DRE*

*Test Reference:* *Volume V Section 4.6.2, Volume V Section 5.2.4, Volume V Section 5.5*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Reworded from [2] I.2.5.1.a.*

*Impact:* *Click here to add the Impact*

↳ **17.7-B.3** Programmed vote-capture devices, poll closing integrity check

Programmed vote-capture devices ***SHALL*** provide an internal test that verifies that the prescribed closing procedure has been followed and that the device status is normal.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Reworded from [2] I.2.5.1.b.*

*Impact:* *Click here to add the Impact*

↳ **17.7-B.4** Programmed vote-capture devices, report on poll closing process

Programmed vote-capture devices ***SHALL*** provide a means to produce a diagnostic test record that verifies the sequence of events and indicates that the poll closing process has been activated.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Reworded from [2] I.2.5.1.d.*

*Impact:* *Click here to add the Impact*

↳ **17.7-B.5** Programmed vote-capture devices, prevent reopening polls

Programmed vote-capture devices ***SHALL*** prevent reopening of the polls once the poll closing has been completed for that election.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.6.2, Volume V Section 5.2.4, Volume V Section 5.5*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Revised from [2] I.2.5.1.e; made consistent with [1] 2.2.3.1.*

*Impact:* *Changed from "preclude the unauthorized reopening of polls" in response to feedback saying that it is never authorized and never OK. [1] read: "The device **SHALL** preclude the re-opening once the poll closing has been completed for that election."*

➞ **17.7-C** Precinct EMS, post-election reports

Precinct EMSs ***SHALL*** provide designated functions for generating precinct post-election reports.

*Applies to:* *Precinct tabulator ∧ EMS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Reworded from [2] I.2.5.*

*Impact:* *Click here to add the Impact*

### 17.7.1 Procedures required for correct system functioning

The requirements for voting systems are written assuming that these procedures will be followed.

(Process, no early reporting) The voting process must prevent access to voted ballots until after the close of polls. ([2] I.2.4.3.3.r, generalized.) See also Requirement III.6.7-A.

## 17.8 Counting

### 17.8.1 Integrity

➞ **17.8.1-A** Detect and prevent ballot style mismatches

All voting systems ***SHALL*** detect and prevent ballot style mismatches.

*Applies to:* *Voting system*

*Test Reference:* *Requirement V.5.2.3-F.1*

D I S C U S S I O N

For example, if the ballot styles loaded on a tabulator disagree with the ballot styles that were used by vote-capture devices, the system must raise an alarm and prevent the incorrect ballot styles from being used during tabulation. Otherwise, votes could be ascribed to the wrong candidates.

Such a mismatch should have been detected and prevented in L&A testing (see Requirement III.6.4.2-C, Requirement III.6.4.2-D and Requirement III.6.4.2-E), but if it was not, it must be detected and prevented before tabulation commences.

*Source:* *Amplification of existing requirements.*

*Impact:* *Click here to add the Impact*

➞ **17.8.1-B** Detect and reject ballots that are oriented incorrectly

Paper-based tabulators ***SHALL*** either

1. Correctly count ballots regardless of whether they are fed upside down, right side up, forward, or reversed; or
2. Detect and reject ballots that are oriented incorrectly.

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Requirement V.5.2.3-F.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

## 17.8.2 Voting variations

→ **17.8.2-A** Tabulator, voting variations

All tabulators ***SHALL*** support all voting variations indicated in the implementation statement.

*Applies to:* *Tabulator*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.2.2.8.1 plus I.2.2.8.2.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.1** Tabulator, 1-of-M

All tabulators ***SHALL*** be capable of tabulating votes, overvotes, and undervotes in contests where the voter is allowed to choose at most one candidate from a list of candidates.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Implicit in [2].*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.2** Tabulator, yes/no question

All tabulators ***SHALL*** be capable of tabulating votes, overvotes, and undervotes in contests where the voter is allowed to vote yes or no on a question.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement / clarification of [2] intent.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.3** Tabulator, absentee voting

Tabulators of the Absentee voting device class ***SHALL*** be capable of tabulating votes, overvotes, and undervotes from absentee ballots.

*Applies to:* *Tabulator ∧ Absentee voting device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.1, I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.4** Tabulator, provisional / challenged ballots

Tabulators of the *Provisional / challenged ballots device* class ***SHALL*** be capable of tabulating votes, overvotes, and undervotes in contests where the decision whether to count a particular ballot is deferred until after election day.

*Applies to:* *Tabulator ∧ Provisional / challenged ballots device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.1, I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.5** Tabulator, accept or reject provisional / challenged ballots individually

Tabulators of the *Provisional / challenged ballots device* class ***SHALL*** support the independent acceptance and rejection of individual provisional/challenged ballots.

*Applies to:* *Tabulator ∧ Provisional / challenged ballots device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

This is meant to rule out the mode of failure in which the IDs assigned to provisional ballots fail to be unique, rendering the system incapable of accepting one without also accepting the others with the same ID.

*Source:* *Added precision, based on [2] I.2.2.8.1, I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.6** Tabulator, accept or reject provisional / challenged ballots by category

Tabulators of the *Provisional / challenged ballots device* class ***SHALL*** support the acceptance and rejection of provisional/challenged ballots by category.

*Applies to:* *Tabulator ∧ Provisional / challenged ballots device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

For "category," see Requirement III.6.6.3-A.17. The behavior when an individual acceptance/rejection conflicts with a categorical acceptance/rejection is system-dependent and should be documented by the vendor.

*Source:* *[3] 5.6.5.2.s.3.*[5]

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.7** Tabulator, primary elections

Tabulators of the *Primary elections device* class ***SHALL*** be capable of keeping separate totals for each political party for the number of ballots read and counted.

*Applies to:* *Tabulator ∧ Primary elections device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

In paper-based systems, open primaries have sometimes been handled by printing a single ballot style that merges the contests from all parties and instructing the voter to vote only in the contests applicable to a single party. This approach requires additional logic in the tabulator to support the rejection or discarding of votes that violate these special instructions, while the approach of assigning different ballot configurations to different parties does not. Support for the merged ballot approach is not required for a tabulator to satisfy the requirements for *Primary elections device*. See Volume III Section 1.5.1.

This requirement to separate by party applies only to the number of read ballots and counted ballots. It does not apply to candidate and choice vote totals.

*Source:* *Added precision, based on [2] reporting requirements.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.8** Tabulator, write-ins

Tabulators of the *Write-ins device* class ***SHALL*** be capable of tabulating votes for write-in candidates, with separate totals for each candidate.

*Applies to:* *Tabulator ∧ Write-ins device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.1, I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.9** Tabulator, support write-in reconciliation

Tabulators of the *Write-ins device* class ***SHALL*** be capable of gathering and recording votes within a voting process that allows for reconciliation of aliases and double votes.

*Applies to:* *Tabulator ∧ Write-ins device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Reconciliation of aliases means allowing central election officials to declare two different spellings of a candidate's name to be equivalent (or not). Reconciliation of

double votes means handling the case where, in an N-of-M contest, a voter has attempted to cast multiple votes for the same candidate using the write-in mechanism. See Volume III Section 1.5.4 for details.

*Source:* *Added precision based on clarification of write-in reconciliation process.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.10** Tabulator, ballot rotation

Tabulators of the *Ballot rotation device* class ***SHALL*** be capable of tabulating votes when the ordering of candidates in ballot positions within each contest is variable.

*Applies to:* *Tabulator ∧ Ballot rotation device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

This just means that ballot rotation must not impact the correctness of the count. A mode of failure would be getting confused about the mapping from ballot positions to candidates.

*Source:* *Added precision, based on [2] I.2.2.8.1, I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.11** Tabulator, straight party voting

Tabulators of the *Straight party voting device* class ***SHALL*** be capable of tabulating straight party votes.

*Applies to:* *Tabulator ∧ Straight party voting device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.1, I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.12** Tabulating straight party votes

A straight party vote ***SHALL*** be counted as a vote in favor of all candidates endorsed by the chosen party in each straight-party-votable contest in which the voter does not cast an explicit vote.

*Applies to:* *Tabulator ∧ Straight party voting device*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

This requirement intentionally says nothing about what happens when there is both a straight party endorsed candidate and an explicit vote in a given contest (a scratch vote). See Volume III Section 1.5.3.

*Source:* *Added precision, based on [2] I.2.2.8.1, I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.13** Tabulator, cross-party endorsement

Tabulators of the *Cross-party endorsement device* class ***SHALL*** be capable of tabulating straight-party votes when a given candidate is endorsed by two or more different political parties.

*Applies to:* *Tabulator ∧ Cross-party endorsement device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.1, I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.14** Tabulator, split precincts

Tabulators of the *Split precincts device* class ***SHALL*** be capable of tabulating votes for two or more election districts within the same precinct.

*Applies to:* *Tabulator ∧ Split precincts device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.1, I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.15** Tabulator, N of M voting

Tabulators of the *N of M voting device* class ***SHALL*** be capable of tabulating votes, overvotes, and undervotes in contests where the voter is allowed to choose up to a specified number of candidates (N(*r*) > 1, per Volume III Section 7.3) from a list of candidates.

*Applies to:* *Tabulator ∧ N of M voting device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.1, I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.16** Tabulator, cumulative voting

Tabulators of the *Cumulative voting device* class ***SHALL*** be capable of tabulating votes, overvotes, and undervotes in contests where the voter is allowed to allocate up to a specified number of votes (N(r) > 1, per Volume III Section 7.3) over a list of candidates however he or she chooses, possibly giving more than one vote to a given candidate.

*Applies to:* *Tabulator ∧ Cumulative voting device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Added precision, based on [2] I.2.2.8.1, I.2.2.8.2 and glossary.*

*Impact:* *Click here to add the Impact*

↳ **17.8.2-A.17** Tabulator, ranked order voting

Tabulators of the *Ranked order voting device* class ***SHALL*** be capable of determining the results of a ranked order contest for each round of voting.

*Applies to:* *Tabulator ∧ Ranked order voting device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

This requirement is minimal. Since ranked order voting is not currently in wide use, it is not clear what, other than the final result, must be computed. See Volume III Section 1.5.5.

*Source:* *[2] I.2.2.8.1 plus I.2.2.8.2.*

*Impact:* *Click here to add the Impact*

## 17.8.3 Ballot separation

See also Dangling ref: PleaseAddReference_HFP_Rejection and Requirement III.6.8.4-C.

➞ **17.8.3-A** Central paper tabulator, ballot separation

In response to designated conditions, paper-based central tabulators ***SHALL*** (a) outstack the ballot, (b) stop the ballot reader and display a message prompting the election official or designee to remove the ballot, or (c) mark the ballot with an identifying mark to facilitate its later identification.

*Applies to:* *Central tabulator ∧ Paper-based device*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.5.1.2.*

*Impact:* *Click here to add the Impact*

↳ **17.8.3-A.1** Central paper tabulator, unreadable ballots

All paper-based central tabulators ***SHALL*** perform this action in response to an unreadable ballot.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.5.1.2.*

*Impact:* *Click here to add the Impact*

↳ **17.8.3-A.2** Central paper tabulator, write-ins

Paper-based central tabulators of the *Review-required ballots device* class ***SHALL*** be able to perform this action in response to a ballot containing write-in votes.

*Applies to:* *Central tabulator ∧ Paper-based device ∧ Review-required ballots device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

The requirement to separate ballots containing write-in votes is not applicable in systems in which an EBM encodes write-in votes in machine-readable form and an optical scanner generates individual tallies for all written-in candidates automatically. Separation of ballots containing write-in votes is only necessary in systems that require write-in votes to be counted manually. Such systems do not conform to the *Write-ins* class. See Volume III Section 2.6.3.1.

*Source:* *[2] I.3.2.5.1.2.*

*Impact:* *Click here to add the Impact*

↳ **17.8.3-A.3** Central paper tabulator, overvotes, undervotes, blank ballots

All paper-based central tabulators ***SHALL*** provide a capability that can be activated by central election officials to perform this action in response to ballots containing overvotes, blank ballots, and ballots containing undervotes in a designated race.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.5.1.2.*

*Impact:* *Click here to add the Impact*

→ **17.8.3-B** Precinct paper tabulator, write-ins

Paper-based precinct tabulators of the *Review-required ballots device* class ***SHALL*** have the capability, when presented with a ballot containing a write-in

vote, to segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification.

*Applies to:* *Precinct tabulator ∧ Paper-based device ∧ Review-required ballots device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

The requirement to separate ballots containing write-in votes is not applicable in systems in which an EBM encodes write-in votes in machine-readable form and an optical scanner generates individual tallies for all written-in candidates automatically. Separation of ballots containing write-in votes is only necessary in systems that require write-in votes to be counted manually. Such systems do not conform to the *Write-ins* class. See Volume III Section 2.6.3.1.

*Source:* *[2] I.3.2.5.1.3.b.*

*Impact:* *Click here to add the Impact*

→ **17.8.3-C** ECOS, react to marginal marks and overvotes

ECOS should provide a capability to alert an election official when a ballot that is scanned appears to contain marginal marks or overvotes.

*Applies to:* *ECOS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

If an EMPB appears to contain marginal marks or overvotes, either the EBM is broken or the scanner is broken. Either way, an election official should be notified immediately. (Possibly the voter has simply disregarded instructions and marked the ballot manually.)

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

## 17.8.4 Misfed ballots

→ **17.8.4-A** Paper-based tabulator, ability to clear misfeed

If multiple feed or misfeed (jamming) occurs, a paper-based tabulator ***SHALL*** halt in a manner that permits the operator to remove the ballot(s) causing the error and reinsert them in the input hopper (if unread) or insert them in the ballot box (if read).

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Volume V Section 4.3, Volume V Section 5.2*

DISCUSSION

See also Requirement III.6.8.4-B and Requirement III.6.8.7-A.

*Source:* *[2] I.3.2.5.1.4.a, expanded to include jamming and ballots that were read.*

*Impact:* *Tightened language from "if multiple feed is detected" to "if multiple feed occurs." Failure to detect is still a failure. Changed "card" to "ballot."*

→ **17.8.4-B** Paper-based tabulator, indicate status of misfed ballot

If multiple feed or misfeed (jamming) occurs, a paper-based tabulator ***SHALL*** clearly indicate whether or not the ballot(s) causing the error have been read.

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Volume V Section 4.3, Volume V Section 5.2*

DISCUSSION

A similar issue arises with DREs that hang just as the voter presses the "cast ballot" button. See Dangling ref: PleaseAddReference_HFP DRE, review and cast ballot. See also Requirement III.6.8.4-A and Requirement III.6.8.7-A.

*Source:* *[45] 14.2.5.3 (page 46).*

*Impact:* *Click here to add the Impact*

→ **17.8.4-C** Paper-based tabulators, misfeed rate benchmark

The misfeed rate ***SHALL*** not exceed 0.002 (1 / 500).

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Volume V Section 5.3.4*

DISCUSSION

Multiple feeds, misfeeds (jams), and rejections of ballots that meet all vendor specifications are all treated collectively as "misfeeds" for benchmarking purposes; i.e., only a single count is maintained.

*Source:* *Merge of [2] I.3.2.5.1.4.b and I.3.2.5.2.c, reset benchmark per TGDC advice.*

*Impact:* *Original requirement in I.3.2.5.2.c: Paper-based tabulators **SHALL** reject ballots that meet all vendor specifications at a rate not to exceed 2 %.*

## 17.8.5 Accuracy

Requirement III.5.3.2-B applies to all voting systems and need not be repeated here. The following requirements elaborate the general requirement with respect to issues that are unique to paper-based systems.

➞ **17.8.5-A** Optical scanner, ignore unmarked voting targets

Optical scanners ***SHALL*** ignore (not record as votes) unmarked voting targets to the satisfaction of Requirement III.5.3.2-B.

*Applies to:* *Optical scanner*

*Test Reference:* *Volume V Section 5.3.3*

D I S C U S S I O N

"Unmarked" in this requirement means containing no marks of any kind other than those designed to be present as part of the ballot style. This includes extraneous perforations, smudges, folds, and blemishes in the ballot stock. See Requirement III.6.8.5-E, Requirement III.6.8.5-F and Requirement III.6.8.5-G.

*Source:* *[2] I.3.2.5.2, "Recognize vote punches or marks, or the absence thereof"*

*Impact:* *Click here to add the Impact*

➞ **17.8.5-B** ECOS, accurately detect marks

ECOS ***SHALL*** detect EBM-generated vote indications to the satisfaction of Requirement III.5.3.2-B.

*Applies to:* *ECOS*

*Test Reference:* *Volume V Section 5.3.3*

D I S C U S S I O N

Reading of marginal marks should be a non-issue if EBMs are used.

*Source:* *Narrowed from [2] I.3.2.5.2.a and I.3.2.6.1.1.*

*Impact:* *Click here to add the Impact*

→ **17.8.5-C** MCOS, accurately detect perfect marks

MCOS ***SHALL*** detect marks that conform to vendor specifications to the satisfaction of Requirement III.5.3.2-B.

*Applies to:* *MCOS*

*Test Reference:* *Volume V Section 5.3.3*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.5.2.a and I.3.2.6.1.1.*

*Impact:* *Click here to add the Impact*

→ **17.8.5-D** MCOS, accurately detect imperfect marks

MCOS ***SHALL*** detect a 1 mm thick line that is made with a #2 pencil, that crosses the entirety of the voting target on its long axis, that is centered on the voting target, and that is as dark as can practically be made with a #2 pencil, to the satisfaction of Requirement III.5.3.2-B.

*Applies to:* *MCOS*

*Test Reference:* *Volume V Section 5.3.3*

D I S C U S S I O N

Different optical scanning technologies will register imperfect marks in different ways. Variables include the size, shape, orientation, and darkness of the mark, the location of the mark within the voting target, the wavelength of light used by the scanner, the size and shape of the scanner's aperture, the color of the ink, the sensed background-white and maximum-dark levels, and of course the calibration of the scanner. The mark specified in this requirement is intended to be less than 100 % perfect, but reliably detectable, i.e., not so marginal as to bring the uncontrolled variables to the forefront. In plain language: scanning technologies may vary, but as a minimum requirement, all of them should be capable of reliably reading *this* mark.

*Source:* *Many issues and public comments. Specification of mark originated with recommendation in Issue #1322, changed to reduce ambiguity.*

*Impact:* *Click here to add the Impact*

→ **17.8.5-E** Paper-based tabulators, ignore extraneous outside voting targets

Paper-based tabulators ***SHALL*** not record as votes any marks, perforations, smudges, or folds appearing outside the boundaries of voting targets.

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

In previous iterations of these Guidelines it was unclear whether "extraneous perforations, smudges, and folds" included perforations, smudges and folds appearing within voting targets. Those appearing within voting targets are now discussed in Requirement III.6.8.5-F and Requirement III.6.8.5-G. Those other requirements are "should" not "**SHALL**"—technology in wide use as of 2006 cannot reliably distinguish extraneous marks within voting targets from deliberate marks.

Marks that conflict with timing marks may cause a tabulator to reject a ballot. This is conforming behavior as it does not result in the recording of bogus votes.

*Source:* *Clarified from [2] I.3.2.5.2.b.*

*Impact:* *Click here to add the Impact*

→ **17.8.5-F** Optical scanner, ignore extraneous inside voting targets

Optical scanners should not record as votes imperfections in the ballot stock and similar insignificant marks appearing inside voting targets.

*Applies to:* *Optical scanner*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

With technology that is in wide use as of 2006, insignificant marks appearing inside voting targets can be detected as votes. This problem should be minimized.

*Source:* *Clarified from [2] I.3.2.5.2.b.*

*Impact:* *Click here to add the Impact*

→ **17.8.5-G** MCOS, ignore hesitation marks

MCOS should not record as votes hesitation marks and similar insignificant marks.

*Applies to:* *MCOS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

With technology that is in wide use as of 2006, it may be possible to reliably detect reasonable marks and reliably ignore hesitation marks if the scanner is calibrated to a specific marking utensil. Unfortunately, in practice, optical scanners are required to tolerate the variations caused by the use of unapproved marking utensils. Thus, lighter marks of a significant size are detected at the cost of possibly detecting especially dark hesitation marks. Emerging technologies for context-sensitive ballot scanning may solve this problem. It is also solvable through procedures that ensure that all voters use only the approved marking utensil.

*Source:* *Clarified from [2] I.3.2.5.2.b.*

*Impact:* *Click here to add the Impact*

→ **17.8.5-H** MCOS, marginal marks, no bias

The detection of marginal marks from manually-marked paper ballots ***SHALL*** not show a bias.

*Applies to:* *MCOS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Bias errors are not permissible in any system ([1] 7.3.3.3). An example of bias would be if marginal marks in the first ballot position were detected differently than marginal marks in the second ballot position.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

→ **17.8.5-I** MCOS, marginal marks, repeatability

The detection of marginal marks from manually-marked paper ballots should be repeatable.

*Applies to:* *MCOS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

It is difficult to have confidence in the equipment if consecutive readings of the same ballots on the same equipment yield dramatically different results. However, it is technically impossible to achieve repeatable reading of ballots containing marks that fall precisely on the sensing threshold. See Volume III Section 1.4.4.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

## 17.8.6 Consolidation

→ **17.8.6-A** Precinct EMS consolidation

Precinct EMSs ***SHALL*** consolidate the data contained in each unit into a single report for the polling place when more than one vote-capture device or precinct tabulator is used.

*Applies to:* *Precinct tabulator ∧ EMS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

For requirements on report content see Volume III Section 6.9.

*Source:* *Reworded from [2] I.2.5.3.2.*

*Impact:* *Click here to add the Impact*

↳ **17.8.6-A.1** DRE, consolidate in 5 minutes

DREs ***SHALL***, if the consolidation of polling place data is done locally, perform this consolidation in a time not to exceed 5 minutes per DRE.

*Applies to:* *Precinct tabulator ∧ EMS ∧ DRE*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

This requirement assumes that the precinct is operating using DREs exclusively and that one of those DREs fills the role of EMS.

*Source:* *Reworded from [2] I.3.2.6.2.1.*

*Impact:* *Click here to add the Impact*

## 17.8.7 Procedures required for correct system functioning

The requirements for voting systems are written assuming that these procedures will be followed.

(Paper-based tabulator, clearing misfeeds when ballot was read) If it is necessary to clear a misfed ballot that was read by a paper-based tabulator but became stuck

on its way to the ballot box, election judges or central election officials must perform this task in the presence of a witness. If an audit found that the contents of the ballot box and the records from the tabulator did not match, one would want to be able to rule out the possibility that something made its way into the ballot box while the tabulator was disconnected.

## 17.9 Reporting

Although reporting is typically an EMS function, most of the requirements in this section are scoped to the entire system because any given EMS might not generate all of the specified information. For example, the precinct- and jurisdiction-level reports might be generated by different EMSs located in the precinct and central location, respectively. The precinct EMSs need not have the capability to generate jurisdiction-level reports and vice-versa.

### 17.9.1 General reporting functionality

➞ **17.9.1-A** Reports are timestamped

All reports ***SHALL*** include the date and time of the report's generation, including hours, minutes, and seconds.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Even if the clock's accuracy leaves something to be desired, second precision is useful to have if two reports are generated in quick succession.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

➞ **17.9.1-B** Timestamps should be ISO 8601 compliant

Timestamps in reports should comply with ISO 8601 [36], provide all four digits of the year and include the time zone.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

➞ **17.9.1-C** Reporting is non-destructive

All programmed devices ***SHALL*** prevent data, including data in transportable memory, from being altered or destroyed by report generation.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 4.3*

D I S C U S S I O N

The appending of an audit record reflecting the fact that a report has been generated is not considered an alteration.

*Source:* *From [2] I.2.2.6.h, I.2.5.3.1.g, and I.2.5.3.2.d.*

*Impact:* *Click here to add the Impact*

## 17.9.2 Audit, status, and readiness reports

➞ **17.9.2-A** Audit reports

All systems ***SHALL*** be capable of producing reports of the event logs defined in Dangling ref: PleaseAddReference_STS_AuditRecordReqs.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.2.6.i and I.2.5.3.1.f.*

*Impact:* *Click here to add the Impact*

➞ **17.9.2-B** Pre-election reports

The EMS ***SHALL*** provide the capability to obtain a report that includes

1. The allowable number of selections in each contest;
2. The combinations of voting patterns permitted or required by the jurisdiction;
3. The inclusion or exclusion of contests as the result of multiple districting within a polling place;

4. Any other characteristics that may be peculiar to the jurisdiction, the election or the precincts;
5. Manual data maintained by election personnel;
6. Samples of all final ballot styles; and
7. Ballot preparation edit listings.

*Applies to:* *EMS*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

For the logging of auditable events during election programming see Dangling ref: PleaseAddReference_STS_AuditRecordReqs.

*Source:* *[2] I.4.4.1 / [6] I.5.4.1*

*Impact:* *Click here to add the Impact*

➞ **17.9.2-C** Status reports

All programmed devices ***SHALL*** provide the capabilities to obtain status and equipment readiness reports.

*Applies to:* *Programmed device*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

These reports typically are generated during pre-voting logic and accuracy testing; see Volume III Section 6.4.2.

*Source:* *Reworded from [2] I.2.3.4.1.b.*

*Impact:* *Click here to add the Impact*

➞ **17.9.2-D** Readiness reports, per polling place

Readiness reports ***SHALL*** include at least the following information for each polling place:

1. The election's identification data;
2. The identification of the precinct and polling place;
3. The identification of all voting devices deployed in the precinct;
4. The identification of all ballot styles used in that precinct;
5. Confirmation that no hardware or software failures were detected during setup and testing, or a record of those that occurred; and
6. Confirmation that all vote-capture devices are ready for the opening of polls, or identification of those that are not.

*Applies to:* *In-person voting*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

In jurisdictions where there are no programmed devices in the precincts, confirmation of equipment readiness could occur through a manual check and signoff by election judges. These readiness reports could take the form of checklists, fill-in forms and signature sheets supplied to the precincts by a central authority.

*Source:* *[2] I.2.3.5, separated generic precinct vs. precinct tabulator reqs, modified to deal with failures.*

*Impact:* *Click here to add the Impact*

→ **17.9.2-E** Readiness reports, precinct tabulator

Readiness reports ***SHALL*** include the following information for each precinct tabulator:

1. The election's identification data;
2. The identification of the precinct and polling place;
3. The identification of the tabulator;
4. The contents of each active candidate register by office and of each active ballot choice register at all storage locations;
5. Confirmation that no hardware or software failures were detected during setup and testing, or a record of those that occurred; and
6. Any other information needed to confirm the readiness of the equipment and to accommodate administrative reporting requirements.

*Applies to:* *Precinct tabulator*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.5, separated generic precinct vs. precinct tabulator reqs, harmonized with Requirement III.6.9.2-F, modified to deal with failures, deleted "special voting options."*

*Impact:* *Click here to add the Impact*

→ **17.9.2-F** Readiness reports, central tabulator

Readiness reports ***SHALL*** include the following information for each central tabulator:

1. The election's identification data;
2. The identification of the tabulator;
3. The identification of all ballot styles used in the jurisdiction;
4. The contents of each active candidate register by office and of each active ballot choice register at all storage locations;

5. Confirmation that no hardware or software failures were detected during setup and testing, or a record of those that occurred; and
6. Any other information needed to confirm the readiness of the equipment and to accommodate administrative reporting requirements.

*Applies to:* *Central tabulator*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.6, harmonized with Requirement III.6.9.2-E, modified to deal with failures, deleted "special voting options."*

*Impact:* *Click here to add the Impact*

➜ **17.9.2-G** Readiness reports, public network test ballots

Systems that send ballots over a public network ***SHALL*** provide a report of test ballots that includes

1. The number of test ballots sent;
2. When each test ballot was sent;
3. The identity of the machine from which each test ballot was sent; and
4. The specific votes or selections contained in the test ballots.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.4.4.2.g / [6] I.5.4.2.g*

*Impact:* *Click here to add the Impact*

## 17.9.3 Vote data reports

The requirements in this section specify a minimum set of information that a voting system must report. They do not prohibit any voting system from reporting additional information that may be required by jurisdictions or merely found to be useful.

Similarly, the identification of four "standard" reporting contexts (tabulator, precinct, election district, and jurisdiction) requires voting systems to support these at a minimum, but does not prohibit any voting system from supporting additional reporting contexts or from offering a generalized facility through which central election officials may define arbitrary reporting contexts.

### 17.9.3.1 General functionality

→ **17.9.3.1-A** Reporting, ability to produce text

All devices used to produce reports of the vote count ***SHALL*** be capable of producing:

1. Alphanumeric headers;
2. Election, office and issue labels; and
3. Alphanumeric entries generated as part of the audit record.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.7.2 / [6] I.4.1.7.2*

*Impact:* *Original requirement was scoped to printers. Generalized to allow for paperless reporting.*

→ **17.9.3.1-B** Report all votes cast

All systems ***SHALL*** be able to produce an accurate, human-readable report of all votes cast.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Binary document formats and text containing markup tags are not considered human-readable. The system may generate such documents, but it must also provide the functionality to render those documents in human-readable form (e.g., by including the necessary reader application).

*Source:* *[2] I.2.2.2.1.c as expanded by [3] 5.2.1.1.c.*[5]

*Impact:* *Click here to add the Impact*

→ **17.9.3.1-C** Account for all cast ballots and all valid votes

All systems ***SHALL*** produce vote data reports that account for all cast ballots and all valid votes.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **17.9.3.1-D** Vote data reports, discrepancies can't happen

Vote data reports ***SHALL*** be completely consistent, with no discrepancy among reports of voting device data at any level.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Reworded from [2] I.3.2.6.2.2, extended to all systems.*

*Impact:* *Removed "error-free" language, which has caused confusion with respect to apparent conflict with Requirement III.5.3.2-B. [2] I.3.2.6.2.2 is restricted to DREs and talks about consolidation and reporting. In Issue #2349, EAC interpretation was "3.2.1 refers to ballot position accuracy and 3.2.6.2.2 refers to accuracy of tabulation." Error-freeness is still the standard in logic verification.*

↳ **17.9.3.1-D.1** Discrepancies that happen anyway must be flagged

Any discrepancy that is detectable by the system ***SHALL*** be flagged by the system by an annotation or error message in the affected report(s) and/or a separate discrepancy report.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

If this requirement is applicable, then the system has failed to satisfy Requirement III.6.9.3.1-D and is therefore non-conforming. Nevertheless, in practice it is essential that discrepancies be flagged by the system as much as possible so that they are not overlooked by election judges. The system cannot detect discrepancies if no single voting device is ever in possession of a sufficient set of data.

*Source:* *New requirement in response to Issue #1366.*

*Impact:* *Click here to add the Impact*

↳ **17.9.3.1-D.2** Discrepancies that happen anyway must be explainable

Any discrepancy in reports, regardless of source, ***SHALL*** be resolvable to a specific cause.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

If this requirement is applicable, then the system has failed to satisfy Requirement III.6.9.3.1-D and is therefore non-conforming. Nevertheless, in practice it is essential that a specific cause be determinable.

*Source:* *Reworded and generalized from [2] I.3.2.6.2.2.*

*Impact:* *Click here to add the Impact*

→ **17.9.3.1-E** Reporting, combined precincts

All systems should be capable of generating reports that consolidate vote data from selected precincts.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Jurisdictions in which more than one precinct may vote at the same location on either the same ballot style or a different ballot style may desire reports that consolidate the voting location.

*Source:* *Derived from [43] 5.04.05.g, [44] Requirement 23 and [45] 14.3.2.3.*

*Impact:* *Click here to add the Impact*

→ **17.9.3.1-F** Precinct tabulators, no tallies before close of polls

Precinct tabulators ***SHALL*** prevent the printing of vote data reports and the extraction of vote tally data prior to the official close of polls.

*Applies to:* *Precinct tabulator*

*Test Reference:* *Volume V Section 4.6.2, Volume V Section 5.2.4, Volume V Section 5.5*

DISCUSSION

Providing ballot counts does not violate this requirement. The prohibition is against providing vote totals. Ballot counts are required for ballot accounting, but early extraction of vote totals is an enabler of election fraud.

*Source:* *Revised from [2] I.2.5.3.2.*

*Impact:* *Changed from "prevent the printing of reports and the unauthorized extraction of data."*

### 17.9.3.2 Ballot counts

Source for Requirement III.6.9.3.2-A through Requirement III.6.9.3.3-I: These requirements were distilled, refactored, and clarified from overlapping, subtly differing requirements appearing several places in Chapters 2 and 4 of [2], including: I.2.2.2.1.c (produce an accurate report of all votes cast), I.2.2.6.h (printed report of everything in I.2.5), I.2.2.9 (ballot counter), I.2.5.2 (means to consolidate vote data), I.2.5.3.1.a (geographic reporting), I.2.5.3.1.b (printed report of number of ballots counted by each tabulator), I.2.5.3.1.c (contest results, overvotes, and undervotes for each tabulator), I.2.5.3.1.d (consolidated reports including other data sources), I.4.4.4.a (number of ballots cast, using each ballot configuration, by tabulator, precinct, and political subdivision), I.4.4.4.b (candidate and measure totals for each contest, by tabulator), I.4.4.4.c (number of ballots read within each precinct and for additional jurisdictional levels, by configuration, including separate totals for each party in primary elections), I.4.4.4.d (separate accumulation of overvotes and undervotes for each contest, by tabulator, precinct, and additional jurisdictional levels), and I.4.4.4.e (for paper-based systems, the total number of ballots both processed and unprocessable, and the total number of cards read).

→ **17.9.3.2-A** Report cast ballots

All systems ***SHALL*** report the number of cast ballots in the precinct, election district, and jurisdiction reporting contexts, both in total and broken down by ballot configuration.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

In the case of 100 % DRE systems, it would suffice to provide a single total that is noted to represent both the number of cast ballots and the number of read ballots, since these are necessarily equal. Only when there is a tangible (paper) ballot is it possible to cast a ballot that is never read. There is no sub-requirement for separate reporting of provisional cast ballots because the system is unlikely to know whether a ballot is provisional until it is successfully read.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **17.9.3.2-B** Report read ballots

All systems ***SHALL*** report the number of read ballots in each reporting context (tabulator, precinct, election district, and jurisdiction), both in total and broken down by ballot configuration.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **17.9.3.2-B.1** Report read ballots, multi-page

Systems that include paper-based devices ***SHALL***, if there are multiple card/page ballots, report the number of cards/pages read in each reporting context (tabulator, precinct, election district, and jurisdiction), both in total and broken down by ballot configuration.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **17.9.3.2-B.2** Report read ballots by party

Systems conforming to the *Primary elections* class ***SHALL*** report separate totals for each party in primary elections.

*Applies to:* *Primary elections*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

This requirement to report by party applies only to the number of read ballots. It does not apply to candidate and ballot choice vote totals.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **17.9.3.2-B.3** Report read provisional ballots

Systems conforming to the *Provisional / challenged ballots* class ***SHALL*** report the number of provisional/challenged read ballots in each reporting context (tabulator, precinct, election district, and jurisdiction), both in total and broken down by ballot configuration.

*Applies to:* *Provisional / challenged ballots*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **17.9.3.2-C** Report counted ballots

All systems ***SHALL*** report the number of counted ballots in each reporting context (tabulator, precinct, election district, and jurisdiction), both in total and broken down by ballot configuration.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

See also Requirement III.6.9.3.2-D, which breaks down counted ballots by contest.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **17.9.3.2-C.1** Report counted ballots by party

Systems conforming to the Primary elections class ***SHALL*** report separate ballot counts for each party in primary elections.

*Applies to:* *Primary elections*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

This requirement to report by party applies only to the number of counted ballots. It does not apply to candidate and ballot choice vote totals.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **17.9.3.2-C.2** Report counted provisional ballots

Systems conforming to the *Provisional / challenged ballots* class ***SHALL*** report the number of provisional/challenged counted ballots in each reporting context (tabulator, precinct, election district, and jurisdiction), both in total and broken down by ballot configuration.

*Applies to:* *Provisional / challenged ballots*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **17.9.3.2-C.3** Report blank ballots

All systems should report the number of blank ballots (ballots containing no votes) that were counted in each reporting context (tabulator, precinct, election district, and jurisdiction), both in total and broken down by ballot configuration.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

DISCUSSION

Some jurisdictions find this information to be useful. Blank ballots sometimes represent a protest vote.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **17.9.3.2-D** Report counted ballots by contest

All systems ***SHALL*** report the number of counted ballots for each relevant N-of-M or cumulative voting contest, in each reporting context (tabulator, precinct, election district, and jurisdiction), per the definition of $K(j,r,t_E)$ in Table 4.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

See definition of relevant contest in Volume II.

This is by contest, while Requirement III.6.9.3.2-C is the overall count. The count by contest could be inferred from the other counts that are broken down by ballot configuration, but providing this figure explicitly will make it easier to account for every vote per Volume III Section 7.3.3.

N-of-M in this requirement includes the most common type of contest, 1-of-M.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

## 17.9.3.3 Vote totals

For the source of these requirements, please see the note in Volume III Section 6.9.3.2.

➞ **17.9.3.3-A** Report votes for each candidate or choice

All systems ***SHALL*** report the vote totals for each candidate or choice in each relevant N-of-M or cumulative voting contest, in each reporting context (tabulator, precinct, election district, and jurisdiction), per the definition of $T(c,j,r,t_E)$ in Table 4 and Volume III Section 7.3.3.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

See definition of relevant contest in Volume II.

N-of-M in this requirement includes the most common type of contest, 1-of-M.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **17.9.3.3-B** Report overvotes for each contest

All systems ***SHALL*** report the number of overvotes for each relevant N-of-M or cumulative voting contest, in each reporting context (tabulator, precinct, election district, and jurisdiction), per the definition of $O(j,r,t_E)$ in Table 4 and Volume III Section 7.3.3.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

See definition of relevant contest in Volume II.

N-of-M in this requirement includes the most common type of contest, 1-of-M.

[2] required the reporting of overvotes even on 100 % DRE systems where overvoting is prevented (Dangling ref: PleaseAddReference_HFP VEBD, prevent overvoting); that requirement is retained here, though it may be redundant.

Overvotes are defined in Volume III Section 7.3. Consistent with the definition of undervotes (see Requirement III.6.9.3.3-C), the count is of votes lost to overvoting, not of ballots containing overvotes. This means that a ballot that overvotes an N-of-M contest would contribute N to the count of overvotes for that contest.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **17.9.3.3-B.1** Reporting overvotes, ad hoc queries

All systems ***SHALL*** be capable of producing a consolidated report of the combination of overvotes for any contest that is selected by an authorized official (e.g.; the number of overvotes in a given contest combining candidate A and candidate B, combining candidate A and candidate C, etc.).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *From [2] I.2.2.6.h and I.2.5.3.1.e.*

*Impact:* *Click here to add the Impact*

→ **17.9.3.3-C** Report undervotes for each contest

All systems ***SHALL*** report the number of undervotes for each relevant N-of-M or cumulative voting contest, in each reporting context (tabulator, precinct, election district, and jurisdiction), per the definition of $U(j,r,t_E)$ in Table 4 and Volume III Section 7.3.3.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

See definition of relevant contest in Volume II.

N-of-M in this requirement includes the most common type of contest, 1-of-M.

Undervotes are defined in Volume III Section 7.3 as needed to enable accounting for every vote. Counting ballots containing undervotes instead of votes lost to undervoting is insufficient.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **17.9.3.3-D** Ranked order voting, report results

Systems conforming to the *Ranked order voting* class ***SHALL*** report the candidate or choice vote totals for each ranked order contest for each round of voting/counting at the jurisdiction level.

*Applies to:* *Ranked order voting*

*Test Reference:* *Volume V Section 5.2*

D I S C U S S I O N

This requirement is minimal. Since ranked order voting is not currently in wide use, it is not clear what must be reported, how bogus orderings are reported, or how it would be done in multiple reporting contexts. See Volume III Section 1.5.5.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **17.9.3.3-E** Include in-person votes

Systems conforming to the *In-person voting* class ***SHALL*** include votes collected from in-person voting in the consolidated reports.

*Applies to:* *In-person voting*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

"Include" simply means that the final totals must reflect them. It does not entail separate totals for the different kinds of votes.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **17.9.3.3-F** Include absentee votes

Systems conforming to the *Absentee voting* class ***SHALL*** include votes from absentee ballots in the consolidated reports.

*Applies to:* *Absentee voting*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

"Include" simply means that the final totals must reflect them. It does not entail separate totals for the different kinds of votes.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **17.9.3.3-G** Include write-in votes

Systems conforming to the *Write-ins* class ***SHALL*** include write-in votes in the consolidated reports.

*Applies to:* *Write-ins*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

"Include" simply means that the final totals must reflect them. It does not entail separate totals for the different kinds of votes.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **17.9.3.3-H** Include accepted provisional / challenged votes

Systems conforming to the *Provisional / challenged ballots* class ***SHALL*** include votes from accepted provisional/challenged ballots in the consolidated reports.

*Applies to:* *Provisional / challenged ballots*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

"Include" simply means that the final totals must reflect them. It does not entail separate totals for the different kinds of votes. See also Requirement III.6.8.2-A.4, Requirement III.6.9.3.2-B.3 and Requirement III.6.9.3.2-C.2.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **17.9.3.3-I** Include accepted reviewed votes

Systems conforming to the *Review-required ballots* class ***SHALL*** include votes from accepted reviewed ballots in the consolidated reports.

*Applies to:* *Review-required ballots*

*Test Reference:* *Volume V Section 4.7, Volume V Section 5.2*

D I S C U S S I O N

"Include" simply means that the final totals must reflect them. It does not entail separate totals for the different kinds of votes.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

## 17.9.4 Procedures required for correct system functioning

The requirements for voting systems are written assuming that these procedures will be followed.

(Ballot accounting) All precincts must account for all ballots pursuant to the current best practices for ballot accounting.

(Label unofficial reports) Any unofficial reports must be clearly labelled as unofficial. ([2] I.2.5.4.c, converted to procedural requirement.) See Volume III Section 1.4.8.

# Chapter 18: Reference Models

## 18.1 Process Model (informative)

### 18.1.1 Introduction

This section contains 16 diagrams describing the elections and voting process. The diagrams are expressed in Unified Modeling Language (UML) version 2.0 [11].

To simplify the diagrams, the following shortcuts have been taken.

- The expansion regions around activities that are performed for every precinct or every voter are not shown.
- When a particular object may or may not exist depending on system and jurisdiction-specific factors (e.g., paper-based vs. DRE), that object is modelled as an optional parameter to an activity. This does not capture the constraint that subsequent activities must wait on this object in those jurisdictions where it applies (i.e., in some jurisdictions it is mandatory).
- Objects that flow downstream in an obvious manner through many activities are not shown as inputs/outputs of all of those activities.
- The propagation of the registration database from one election cycle to the next is not shown. The database appears as an input to the Register voters activity with no indication of its origin.
- Many activities produce reports and other objects that eventually flow into the Archive activity. These flows into the archive are not shown.

### 18.1.2 Diagrams

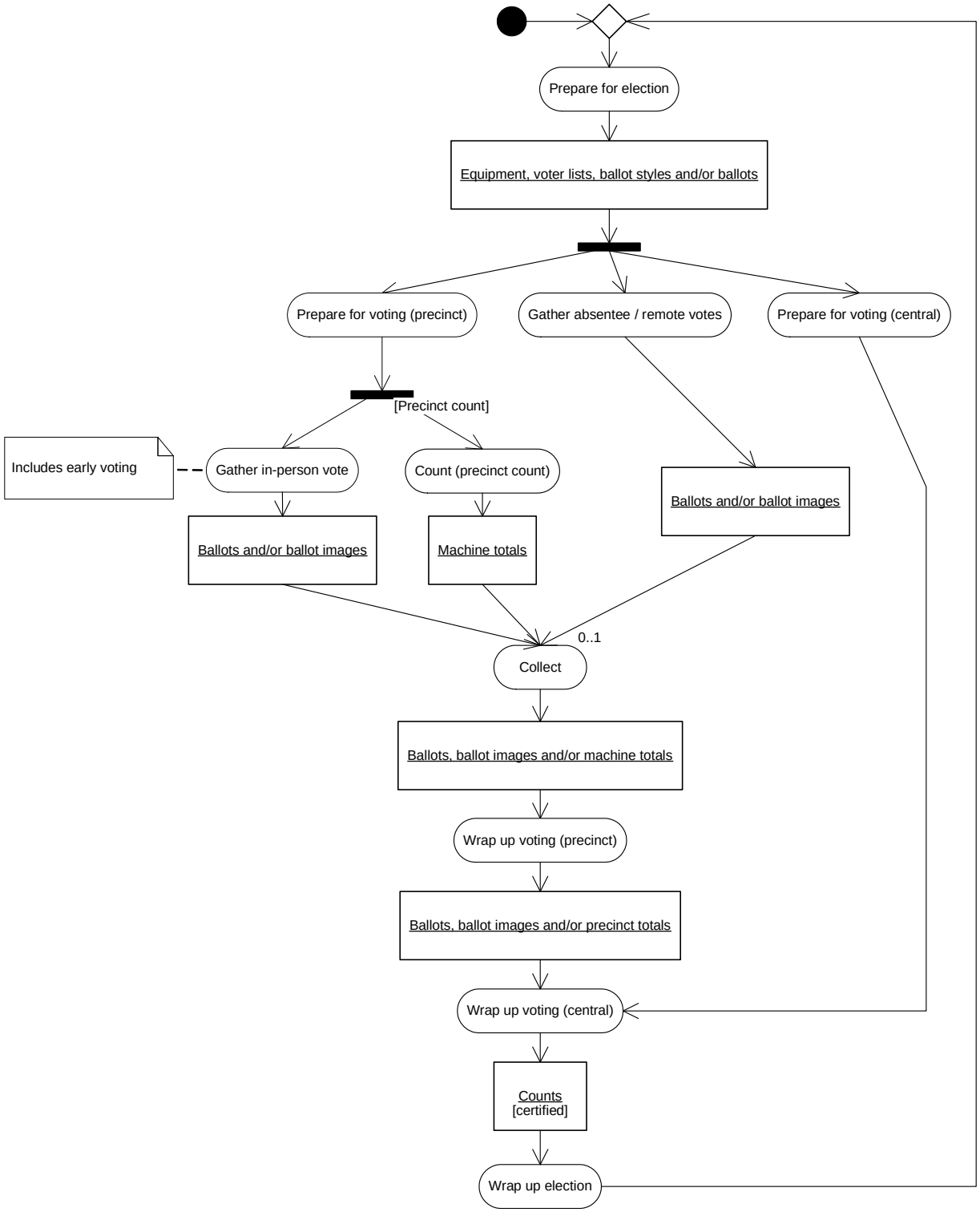



Figure 18-4 Administer elections

## 18.1 Process Model (informative)

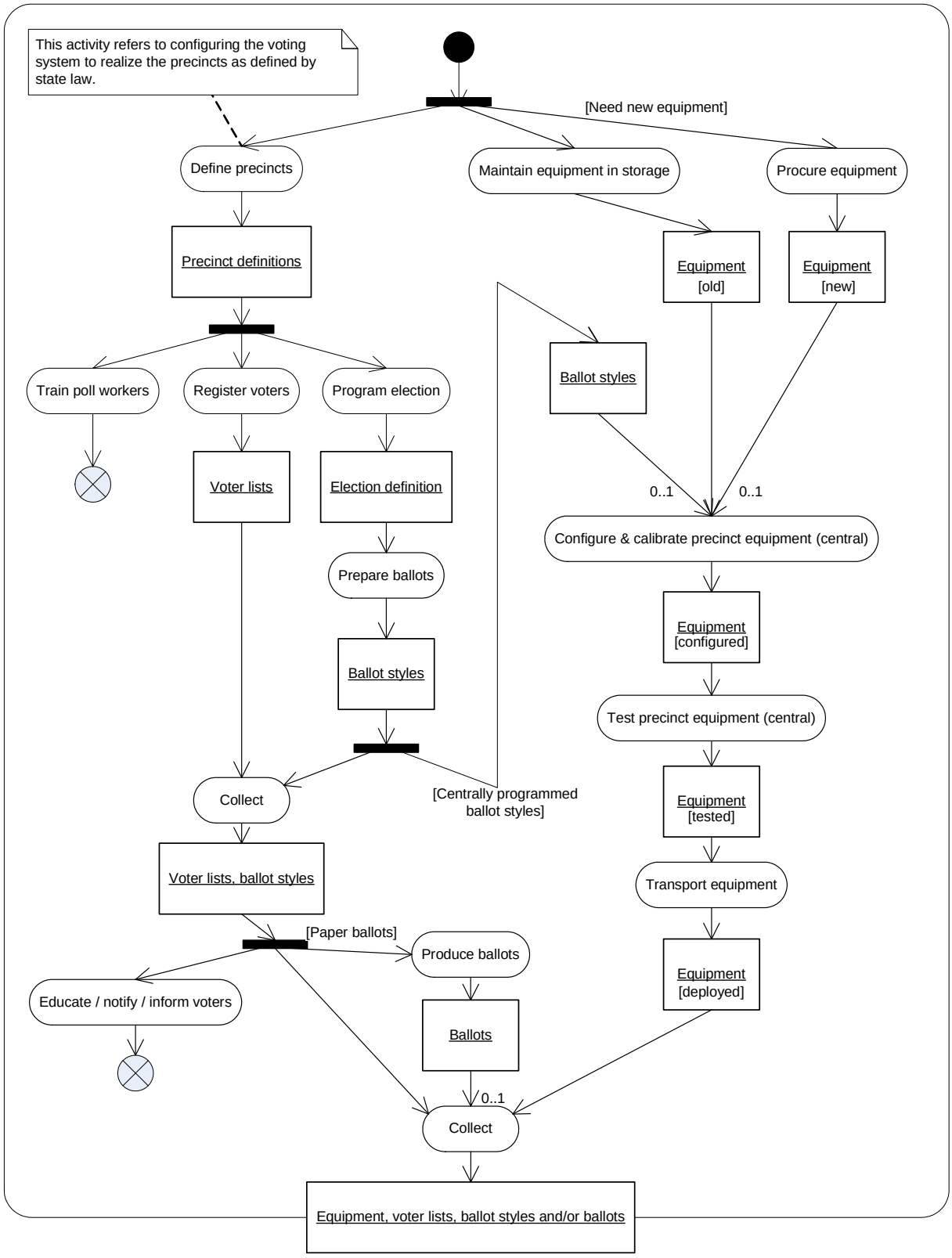



Figure 18-5 Prepare for election

## 18.1 Process Model (informative)

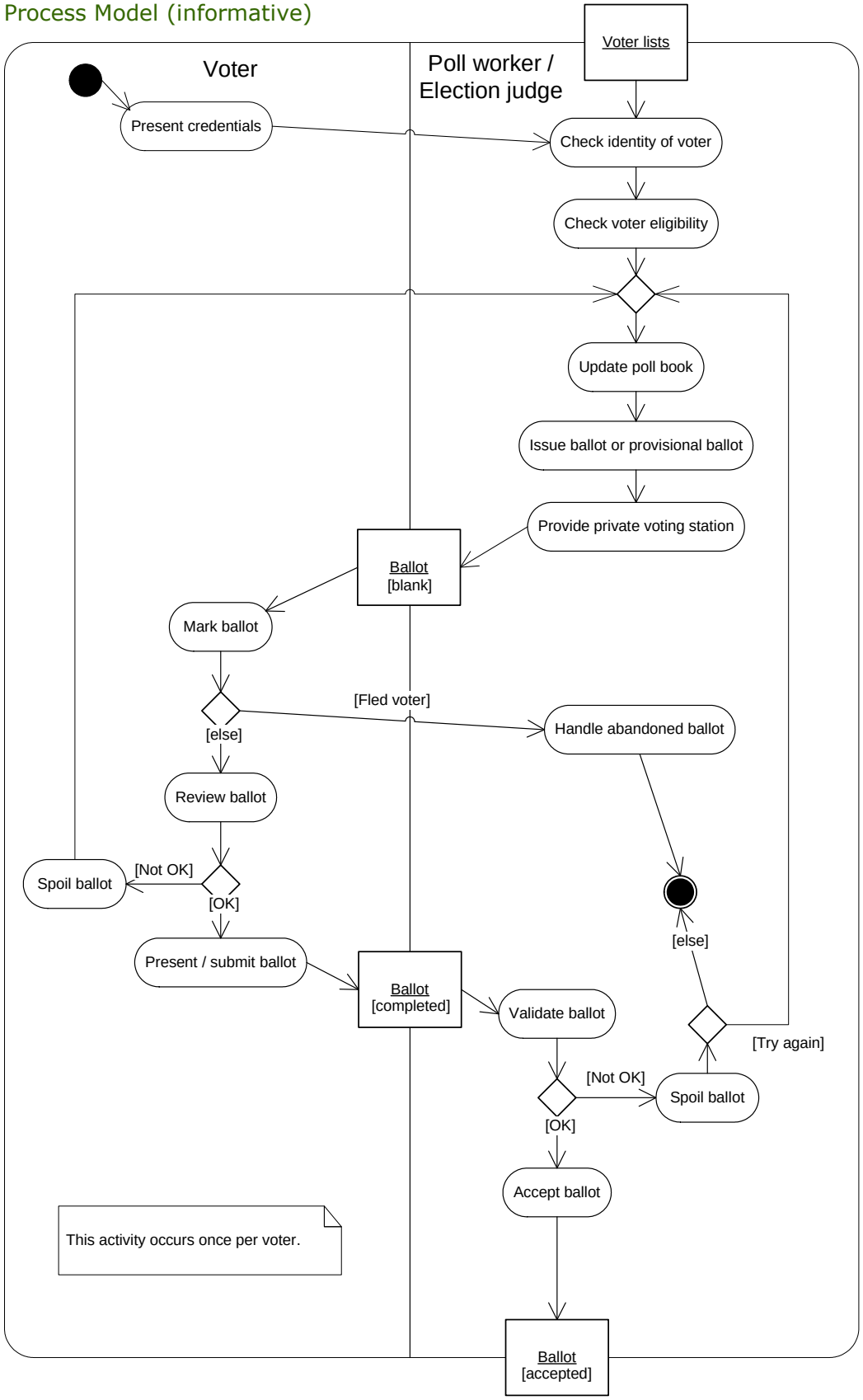



Figure 18-6 Gather in-person vote (paper-based)

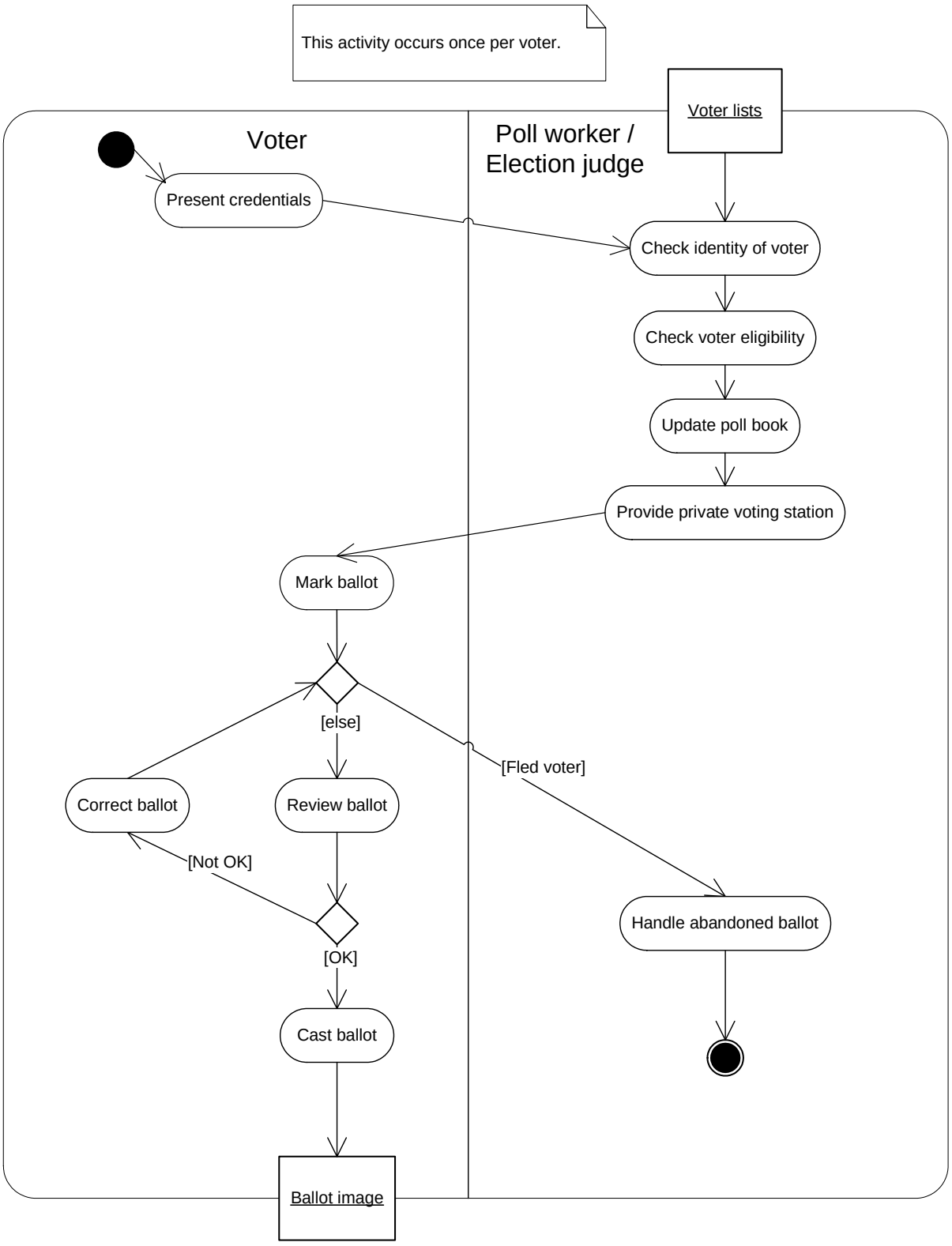



Figure 18-7 Gather in-person vote (DRE)

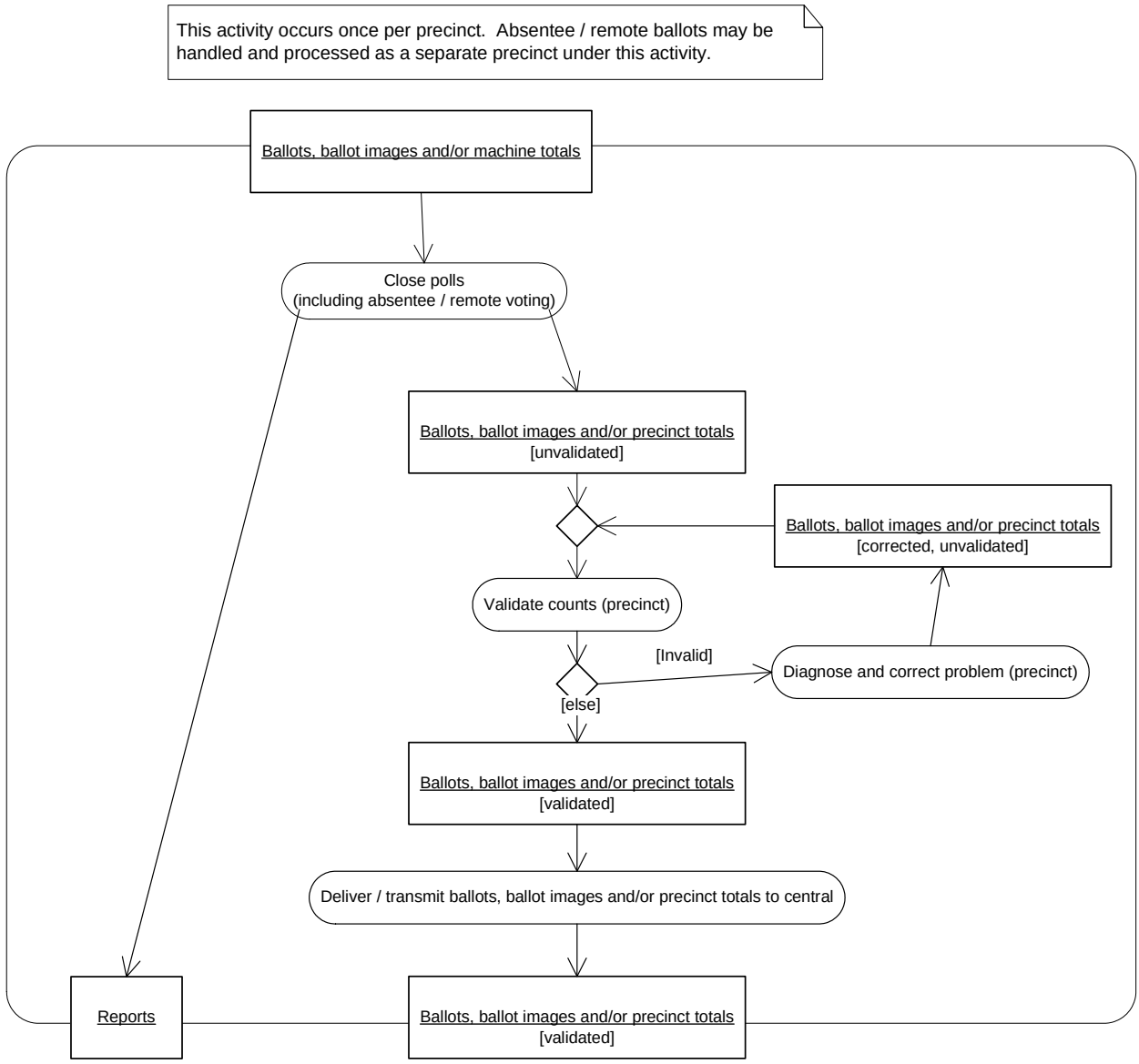



Figure 18-8 Wrap up voting (precinct)

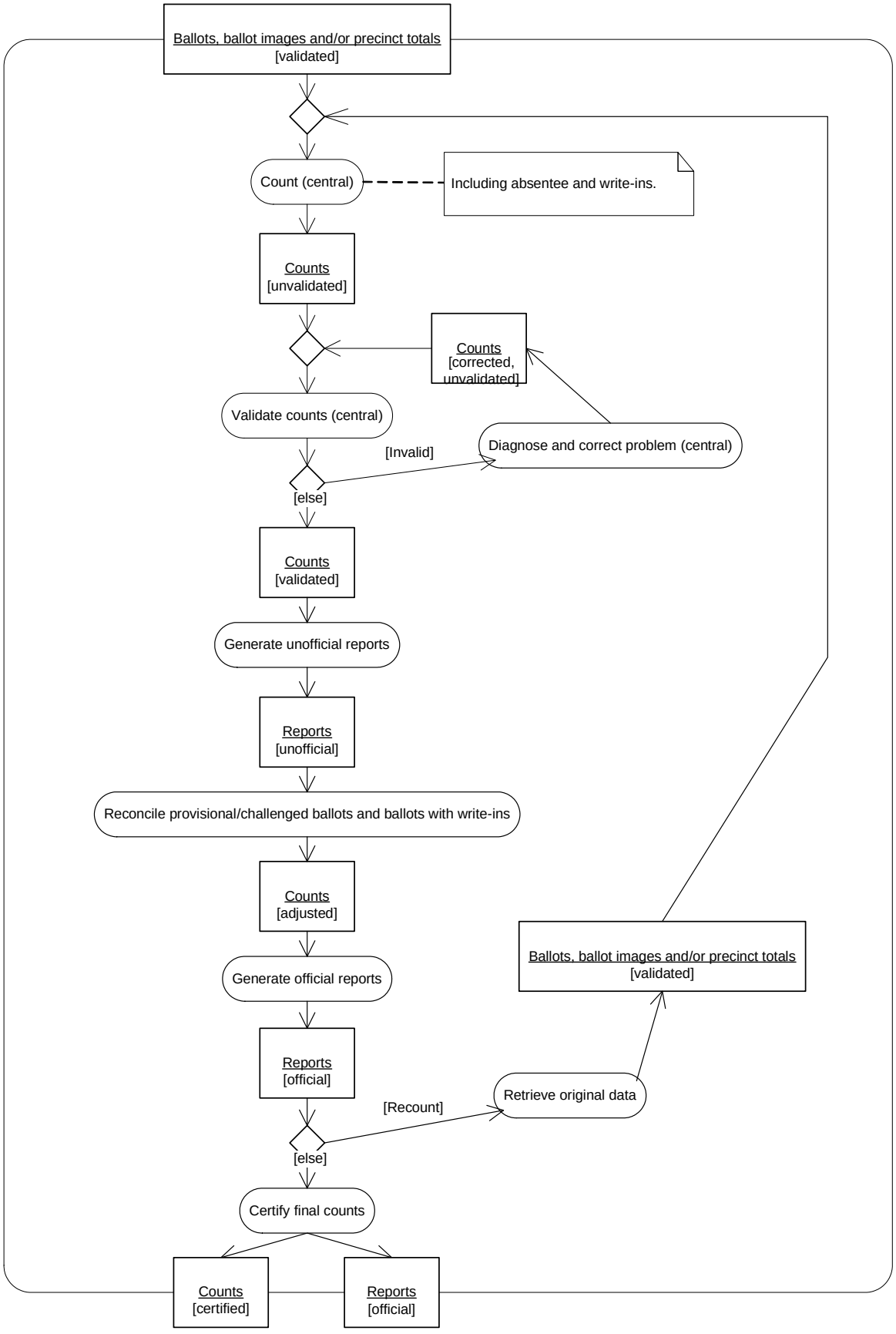



Figure 18-9 Wrap up voting (central)

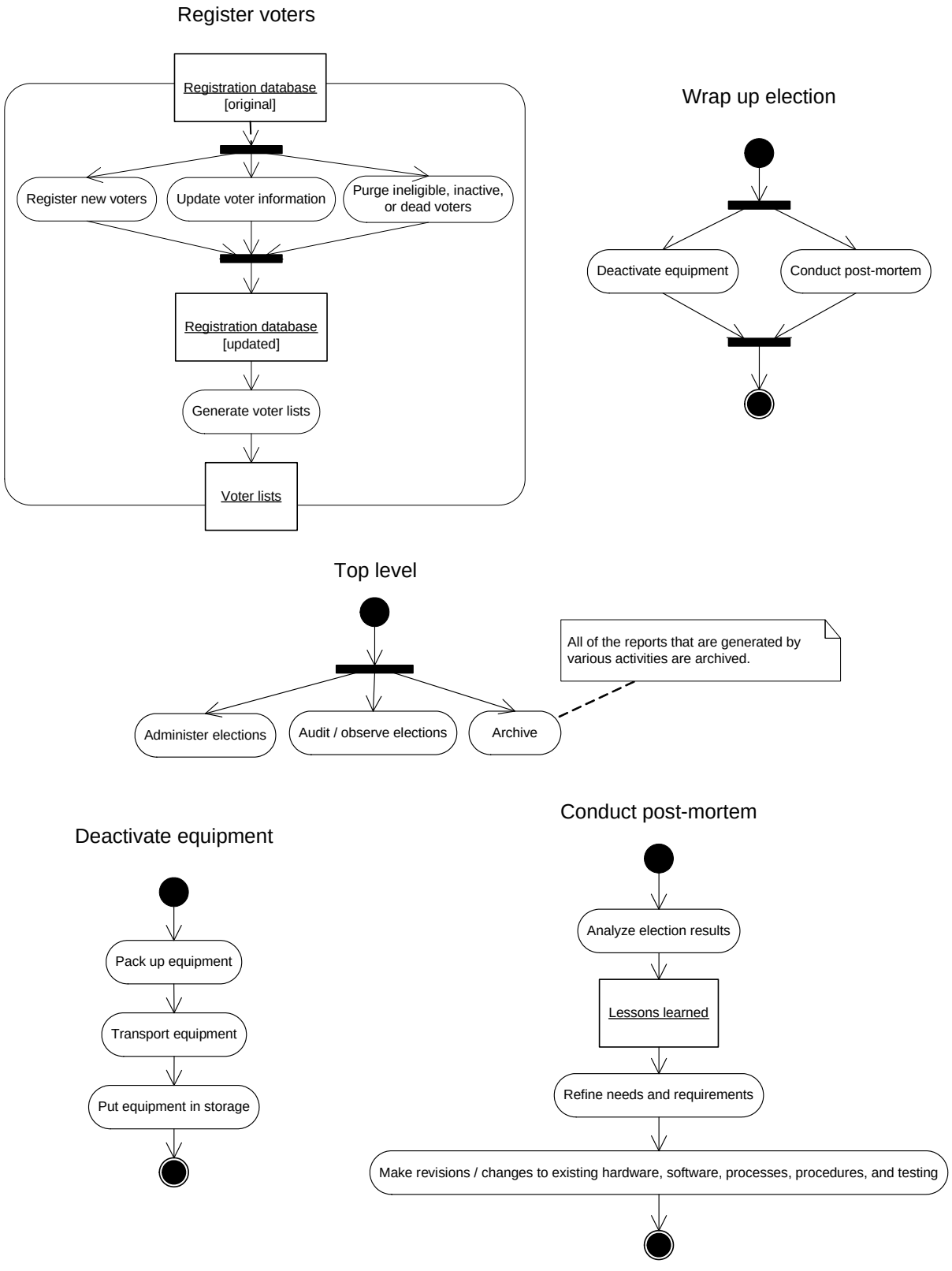



Figure 18-10 Miscellaneous activities (1)

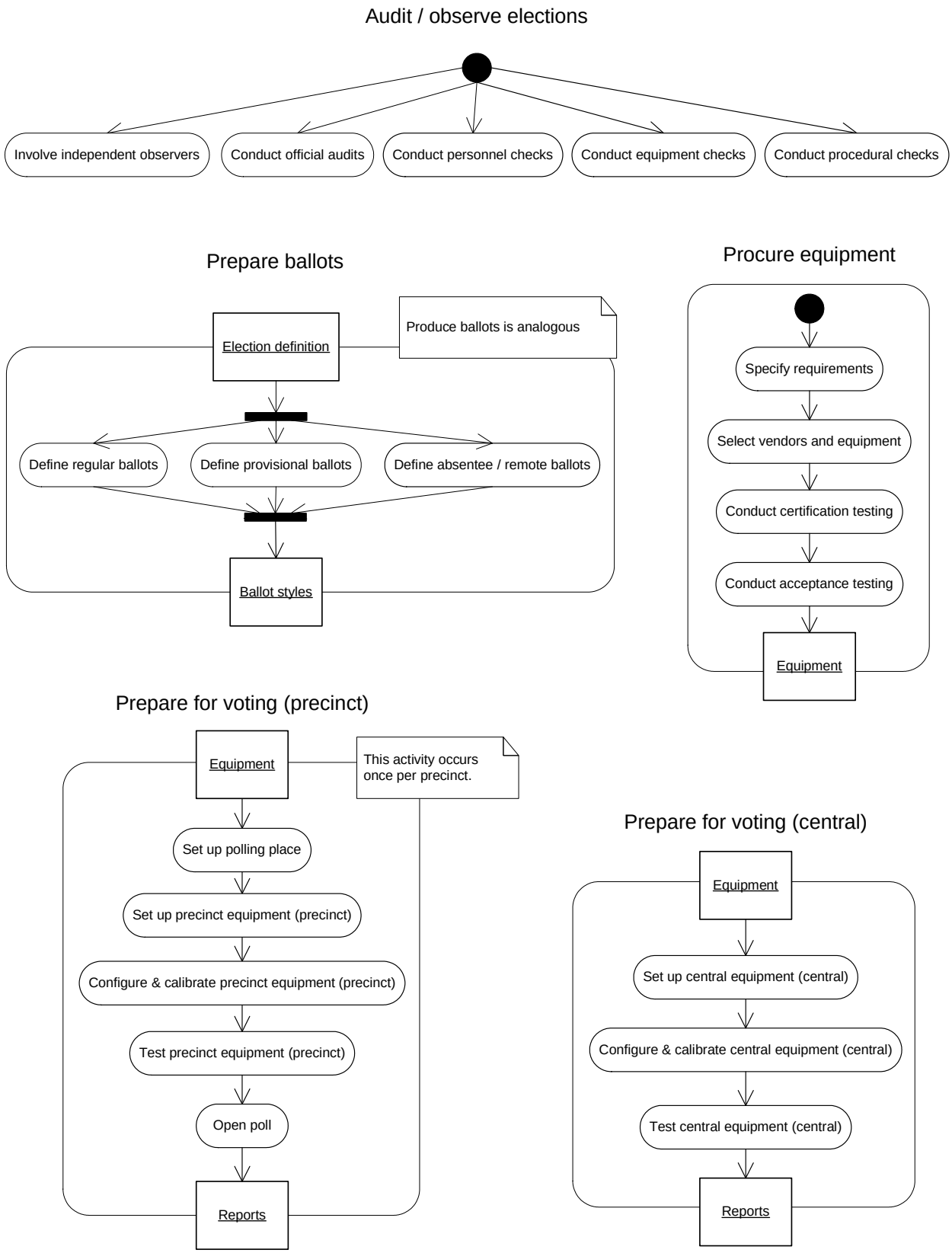



Figure 18-11 Miscellaneous activities (2)

### 18.1.3 Translation of diagrams

This subsection contains a rendering of the process model into text. The rendering is based on Petri Net Linear Form [12].

Although the form of the diagrams is being changed from drawings to text, the meanings of the diagram elements—activities, objects, etc.—continue to be as in UML 2.0 [11].

Activities are represented in this translation by the activity name in parenthesis. Objects are represented in this translation by the object name in square brackets. Sometimes the names of activities and objects will themselves be qualified by parenthetical phrases or object states in square brackets. These have been retained as-is, nesting the parenthesis or brackets as needed.

Sequential control and object flows are indicated with ->.

A flow may be qualified by a guard condition and/or a multiplicity such as 0..1. These notations are inserted immediately before and after the affected flow. For example, Daytime->0..1(Drink coffee) denotes an optional flow into the "drink coffee" activity that can only occur if the condition Daytime is true.

A node may be assigned an identifier that may be used as the target of flows from elsewhere in the diagram. The identifier is prefixed by an asterisk and is introduced by including it after the first occurrence of the node name. For example, (Do something *s) denotes an activity "do something" with the identifier *s. The node name may be omitted in subsequent references that include only the identifier.

The following special nodes appear with semantics as in UML 2.0. They are distinguished from objects and activities by being enclosed between < and >.

- <InitialNode>
- <ForkNode>
- <JoinNode>
- <DecisionNode>
- <MergeNode>
- <ActivityFinal>
- <FlowFinal>

When multiple flows follow from a node, they are listed between curly braces {} and separated by commas.

A semicolon indicates that the description is about to continue at a different node. A period indicates that the description of the diagram is complete.

Translation of the diagrams follows.

```
Diagram:  Administer elections
```

```
<InitialNode>
  -><MergeNode *merge>
  ->(Prepare for election)
  ->[Equipment, voter lists, ballot styles and/or ballots]
  -><ForkNode>{
    ->(Prepare for voting (precinct))
      -><ForkNode>{
     ->(Gather in-person vote)
       ->[Ballots and/or ballot images]
       ->(Collect *c),
     Precinct count
       ->(Count (precinct count))
       ->[Machine totals]
       ->0..1(*c)
      },
    ->(Gather absentee / remote votes)
      ->[Ballots and/or ballot images]
      ->(*c),
    ->(Prepare for voting (central))
      ->(Wrap up voting (central) *w)
  };
(*c)
  ->[Ballots, ballot images and/or machine totals]
  ->(Wrap up voting (precinct))
  ->[Ballots, ballot images and/or precinct totals]
  ->(Wrap up voting (central) *w)
  ->[Counts [certified]]
  ->(Wrap up election)
  -><*merge>.


Note (on Gather in-person vote):  Includes early voting.


Diagram:  Prepare for election

Output:  [Equipment, voter lists, ballot styles and/or ballots]

<InitialNode>
  -><ForkNode>{
    ->(Define precincts)
      ->[Precinct definitions]
      -><ForkNode>{
        ->(Train poll workers)
          -><FlowFinal>,
        ->(Register voters)
          ->[Voter lists]
          ->(Collect *c1),
        ->(Program election)
          ->[Election definition]
          ->(Prepare ballots)
          ->[ballot styles]
          -><ForkNode>{
            ->(*c1),
            Centrally programmed ballot styles
              ->[ballot styles]
              ->0..1(Configure & calibrate precinct equipment
(central) *cc)
          }
      },
    ->(Maintain equipment in storage)
      ->[Equipment [old]]
      ->(*cc),
    Need new equipment
      ->(Procure equipment)
      ->[Equipment [new]]
      ->0..1(*cc)
```

```
  };
(*c1)
  ->[Voter lists, ballot styles]
  -><ForkNode>{
    ->(Educate / notify / inform voters)
      -><FlowFinal>,
    ->(Collect *c2),
    Paper ballots
      ->(Produce ballots)
      ->[Ballots]
      ->0..1(*c2)
  };
(*cc)
  ->[Equipment [configured]]
  ->(Test precinct equipment (central))
  ->[Equipment [tested]]
  ->(Transport equipment)
  ->[Equipment [deployed]]
  ->(Collect *c2)
  ->[Equipment, voter lists, ballot styles and/or ballots].

Note (on Define precincts):  This activity refers to configuring the
voting system to realize the precincts as defined by state law.


Diagram:  Gather in-person vote (paper-based).

This diagram is divided to show which activities are done by the
voter
and which are done by the poll worker or election judge.  The
activity
Spoil ballot may be done by either.  Present credentials, Mark
ballot,
Review ballot, and Present / submit ballot are done by the voter.
All
others are done by the poll worker or election judge.

Note:  This activity occurs once per voter.

Input:  [Voter lists]
Output:  [Ballot [accepted]]

[Voter lists]
  ->(Check identity of voter *check);
<InitialNode>
  ->(Present credentials)
  ->(Check identity of voter *check)
  ->(Check voter eligibility)
  -><MergeNode *merge>
  ->(Update poll book)
  ->(Issue ballot or provisional ballot)
  ->(Provide private voting station)
  ->[Ballot [blank]]
  ->(Mark ballot)
  -><DecisionNode>{
    Fled voter
      ->(Handle abandoned ballot)
      -><ActivityFinal>,
    else
      ->(Review ballot)
      -><DecisionNode>{
        Not OK
          ->(Spoil ballot)
          -><*merge>,
        OK
          ->(Present / submit ballot)
          ->[Ballot [completed]]
          ->(Validate ballot)
```

```
          -><DecisionNode>{
            OK
              ->(Accept ballot)
              ->[Ballot [accepted]],
            Not OK
              ->(Spoil ballot)
              -><DecisionNode>{
                Try again
                  -><*merge>,
                else
                  -><ActivityFinal>
              }
          }
      }
  }.
```

Diagram:  Gather in-person vote (DRE).

This diagram is divided to show which activities are done by the voter
and which are done by the poll worker or election judge.  Present credentials, Mark ballot, Review ballot, Correct ballot, and Cast ballot are done by the voter.  All others are done by the poll worker
or election judge.

Note:  This activity occurs once per voter.

Input:  [Voter lists]
Output:  [Ballot image]

```
[Voter lists]
  ->(Check identity of voter *check);
<InitialNode>
  ->(Present credentials)
  ->(Check identity of voter *check)
  ->(Check voter eligibility)
  ->(Update poll book)
  ->(Provide private voting station)
  ->(Mark ballot)
  -><MergeNode *merge>
  -><DecisionNode>{
    Fled voter
      ->(Handle abandoned ballot)
      -><ActivityFinal>,
    else
      ->(Review ballot)
      -><DecisionNode>{
        Not OK
          ->(Correct ballot)
          -><*merge>,
        OK
          ->(Cast ballot)
          ->[Ballot image]
      }
  }.
```

Diagram:  Wrap up voting (precinct)

Note:  This activity occurs once per precinct.  Absentee / remote ballots may be handled and processed as a separate precinct under this
activity.

Input:  [Ballots, ballot images and/or machine totals]

```
Outputs:  [Reports], [Ballots, ballot images and/or precinct totals
[validated]]

[Ballots, ballot images and/or machine totals]
  ->(Close polls (including absentee / remote voting)){
    ->[Reports],
    ->[Ballots, ballot images and/or precinct totals [unvalidated]]
    -><MergeNode *merge>
    ->(Validate counts (precinct))
    -><DecisionNode>{
      Invalid
        ->(Diagnose and correct problem (precinct))
        ->[Ballots, ballot images and/or precinct totals [corrected,
unvalidated]]
        -><*merge>,
      else
        ->[Ballots, ballot images and/or precinct totals
[validated]]
        ->(Deliver / transmit ballots, ballot images and/or precinct
totals to central)
        ->[Ballots, ballot images and/or precinct totals
[validated]]
    }
  }.


Diagram:  Wrap up voting (central)

Input:  [Ballots, ballot images and/or precinct totals [validated]]
Outputs:  [Counts [certified]], [Reports [official]]

[Ballots, ballot images and/or precinct totals [validated]]
  -><MergeNode *merge1>
  ->(Count (central))
  ->[Counts [unvalidated]]
  -><MergeNode *merge2>
  ->(Validate counts (central))
  -><DecisionNode>{
    Invalid
      ->(Diagnose and correct problem (central))
      ->[Counts [corrected, unvalidated]]
      -><*merge2>,
    else
      ->[Counts [validated]]
      ->(Generate unofficial reports)
      ->[Reports [unofficial]]
      ->(Reconcile provisional/challenged ballots and ballots with
write-ins)
      ->[Counts [adjusted]]
      ->(Generate official reports)
      ->[Reports [official]]
      -><DecisionNode>{
        Recount
          ->(Retrieve original data)
          ->[Ballots, ballot images and/or precinct totals
[validated]]
          -><*merge1>,
        else
          ->(Certify final counts){
            ->[Counts [certified]],
            ->[Reports [official]]
          }
      }
  }.

Note (on Count (central)):  Including absentee and write-ins.
```

```
Diagram:  Audit / observe elections

<InitialNode>{
  ->(Involve independent observers),
  ->(Conduct official audits),
  ->(Conduct personnel checks),
  ->(Conduct equipment checks),
  ->(Conduct procedural checks)
}.


Diagram:  Prepare ballots

Note:  Produce ballots is analogous.

Input:  [Election definition]
Output:  [ballot styles]

[Election definition]
  -><ForkNode>{
    ->(Define regular ballots)
      -><JoinNode *j>,
    ->(Define provisional ballots)
      -><*j>,
    ->(Define absentee / remote ballots)
      -><*j>
  };
<*j>
  ->[ballot styles].


Diagram:  Procure equipment

Output:  [Equipment]

<InitialNode>
  ->(Specify requirements)
  ->(Select vendors and equipment)
  ->(Conduct certification testing)
  ->(Conduct acceptance testing)
  ->[Equipment].


Diagram:  Prepare for voting (precinct)

Note:  This activity occurs once per precinct.

Input:  [Equipment]
Output:  [Reports]

[Equipment]
  ->(Set up polling place)
  ->(Set up precinct equipment (precinct))
  ->(Configure & calibrate precinct equipment (precinct))
  ->(Test precinct equipment (precinct))
  ->(Open poll)
  ->[Reports].


Diagram:  Prepare for voting (central)

Input:  [Equipment]
Output:  [Reports]

[Equipment]
  ->(Set up central equipment (central))
```

```
  ->(Configure & calibrate central equipment (central))
  ->(Test central equipment (central))
  ->[Reports].


Diagram:  Register voters

Input:  [Registration database [original]]
Output:  [Voter lists]

[Registration database [original]]
  -><ForkNode>{
    ->(Register new voters)
      -><JoinNode *j>,
    ->(Update voter information)
      -><*j>,
    ->(Purge ineligible, inactive, or dead voters)
      -><*j>
  };
<*j>
  ->[Registration database [updated]]
  ->(Generate voter lists)
  ->[Voter lists].


Diagram:  Wrap up election

<InitialNode>
  -><ForkNode>{
    ->(Deactivate equipment)
      -><JoinNode *j>,
    ->(Conduct post-mortem)
      -><*j>
  };
<*j>
  -><ActivityFinal>.


Diagram:  Top level

<InitialNode>
  -><ForkNode>{
    ->(Administer elections),
    ->(Audit / observe elections),
    ->(Archive)
  }.

Note (on Archive):  All of the reports that are generated by various
activities are archived.


Diagram:  Deactivate equipment

<InitialNode>
  ->(Pack up equipment)
  ->(Transport equipment)
  ->(Put equipment in storage)
  -><ActivityFinal>.


Diagram:  Conduct post-mortem

<InitialNode>
  ->(Analyze election results)
  ->[Lessons learned]
  ->(Refine needs and requirements)
```

```
  ->(Make revisions / changes to existing hardware, software,
processes, procedures, and testing)
  -><ActivityFinal>.
```

# 18.2 Vote-Capture Device State Model (informative)

The state model shown in Figure 11 clarifies the relationship between the different equipment states that result from the opening and closing of polls and the suspension and resumption of voting in jurisdictions that allow early voting.

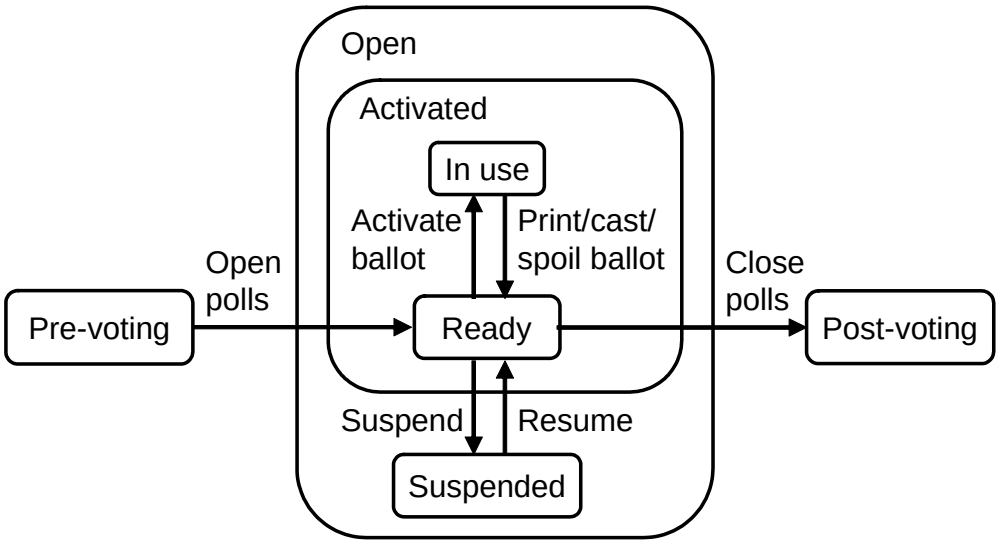



Figure 18-12 Vote-capture device states

The many steps that occur prior to the opening of polls are abstracted by the **Pre-voting** state. The many steps that occur after the close of polls are abstracted by the **Post-voting** state. Between these is a composite state **Open**, which contains the simple state **Suspended** and the composite state **Activated**. **Activated** in turn contains the simple states **Ready** and **In use**.

Upon the opening of polls, the vote-capture device transitions from the **Pre-voting** state to the **Ready** state (and, consequently, also to the **Open** and **Activated** composite states that contain it). From **Ready** it can transition to the In use state upon the activation of a ballot and return to the **Ready** state when that ballot is printed, cast or spoiled (the details depend on the technology in use). From **Ready** it can also transition to the **Suspended** state when an election official suspends voting and return to the **Ready** state when voting is resumed. Finally, from **Ready** it can transition to the **Post-voting** state when polls are closed.

In conformance with Requirement III.6.7-B.5, there is no transition from **Post-voting** back to **Open** except by beginning an entirely new election cycle, which is not modelled here.

A voting session lasts while the device is in the In use state. An active period lasts while the device is in the **Activated** state.

## 18.3 Logic Model (normative)

This model defines the results that must appear in vote data reports and is used in verification of voting system logic. It does not address ranked order voting and does not attempt to define every voting variation that jurisdictions may use. It suffices for N of M (including 1 of M) and cumulative voting.[10]

### 18.3.1 Domain of discourse

A noteworthy bound on the scope of the voting system, and hence the logic model, is that, as of the state of the practice in 2005, voting systems do not identify voters. Poll workers are responsible for maintaining the one voter, one ballot parity. The voting system is limited to handling ballots. Consequently, logic verification is limited to showing that those ballots are counted correctly.

| TERM | DEFINITION |
|---|---|
| A(*t,v*) | Boolean function, returns true if and only if ballot *v* conforms to jurisdiction-dependent criteria for accepting or rejecting entire ballots, such as stray marks policies and voter eligibility criteria, as of time *t*. This value is false for provisional, challenged, and review-required ballots that are not [yet] validated, and for spoiled ballots.<br><br>The system may not be able to determine the value of A(*t,v*) without human input; however, it may assign tentative values according to local procedures and state law, to be corrected later if necessary by input from election workers.<br><br>The value of A(*t,v*) may change over time as a result of court decisions, registrar review of voter eligibility, etc.<br><br>In a paper-based system, A(*t,v*) will be false if ballot *v* is unprocessable. |
| C(*r,t*) | The set of all candidates or choices for a contest *r*, including any write-ins appearing on ballots cast as of time *t*. In systems conforming to the *Write-ins* class, each distinct write-in candidate appears separately in C(*r,t*). Systems not conforming to the *Write-ins* class may nevertheless offer ballot positions for write-ins to be processed manually; in that case, C(*r,t*) contains entries corresponding to the anonymous write-in positions. |
| *c*, $c_n$, etc. | Individual candidates or choices. |
| D(*v*) | The time at which ballot *v* is "done" (either cast or spoiled). If a ballot is not "done" by the close of polls (e.g., an absentee ballot was never returned), it is effectively spoiled and called "done." |

| TERM | DEFINITION |
|---|---|
| J | The set of reporting contexts (including tabulators, precincts, election districts, and jurisdiction). |
| $j$, $j_n$, etc. | Individual reporting contexts. |
| K($j$,$r$,$t$) | For a given contest and reporting context, the number of read ballots for which A($t$,$v$) is true as of time t (i.e., the number of ballots that should be counted). Ballot styles that do not include contest $r$ do not contribute to this total. |
| $L_B$ | A limit on the number of ballots or ballot images that a tabulator is claimed to be capable of processing correctly. (Non-tabulating devices like EBMs have no such limit.) |
| $L_C$ | A limit on the number of ballot positions per contest that a voting device is claimed to be capable of processing correctly. (See also $L_W$) |
| $L_F$ | A limit on the number of ballot styles that a voting device is claimed to be capable of processing correctly. |
| $L_P$ | For paper-based tabulators, a limit on the ballot tabulation rate at which the device is claimed to be capable of operating correctly. |
| $L_R$ | A limit on the number of contests that a voting device is claimed to be capable of processing correctly. |
| $L_T$ | A numerical limit on vote totals that a tabulator is claimed to be capable of processing correctly. |
| $L_V$ | A limit on the number of provisional, challenged, or review-required ballots that a voting device is claimed to be capable of processing correctly. |
| $L_W$ | A limit on the total number of distinct candidates or choices per contest, including write-ins, that a voting device is claimed to be capable of processing correctly. $L_W \geq L_C$. (See also LC) |
| N($r$) | The maximum number of votes that may be cast by a given voter in contest $r$, pursuant to the definition of the contest. For N of M contests, this is the value $N$. |
| O($j$,$r$,$t$) | For a given contest and reporting context, the number of overvotes in read ballots for which A($t$,$v$) is true as of time $t$. Each ballot in which contest $r$ is overvoted contributes N($r$) to O($j$,$r$,$t$). |
| R | The set of all contests. |
| $r$, $r_n$, etc. | Individual contests in R. |
| S($c$,$r$,$t$,$v$) | Ballot $v$'s vote with respect to candidate or choice $c$ in contest $r$ as of time $t$. For checkboxes and the like, the value is 1 (selected) or 0 (not selected). For cumulative voting, the value is the number of votes that $v$ gives to candidate or choice c in contest r. If the applicable ballot style does not include contest $r$, S($c$,$r$,$t$,$v$) = 0. |

| TERM | DEFINITION |
|---|---|
| S'(*c*,*r*,*t*,*v*) | Ballot *v*'s vote with respect to candidate or choice *c* in contest *r* as accepted for counting purposes (i.e., valid votes only), as of time *t*. |
| S(*r*,*t*,*v*) | The total number of votes that ballot *v* has in contest *r* as of time *t*. $S(r,t,v) = \sum_{c \in C(r,t)} S(c,r,t,v)$ |
| T(*c*,*j*,*r*,*t*) | The vote total for candidate or choice c in contest *r* and reporting context *j* as of time *t*. This does not include votes that are invalid due to overvoting or votes from ballots for which A(*t*,*v*) is false. |
| *t*, $t_n$, etc. | Individual time points. |
| $t_O$ | The time at which polls are opened. |
| $t_C$ | The time at which polls are closed. |
| $t_E$ | The time at which the value of A(t,v) is frozen for all ballots, the counting is complete, and final vote totals are required ("end"). |
| U(*j*,*r*,*t*) | For a given contest and reporting context, the number of undervotes in read ballots for which A(*t*,*v*) is true as of time *t*. A given ballot contributes at most N(*r*) to U(*j*,*r*,*t*). Ballot styles that do not include contest *r* do not contribute to this total. |
| V(*j*,*t*) | The set of all ballots that have been distributed to voters, enabled, activated or issued within reporting context j by time t, including any that are presently being voted. Absentee ballots, provisional/challenged ballots, and review-required ballots are included in V if and only if the system claims conformance to the relevant classes. Ballots containing write-in votes may be included for systems not conforming to the *Write-ins* class if the system reports all write-in votes as a single ballot position. For more information on this exception see C(*r*,*t*) and Volume III Section 2.6.3.1. |
| *v*, $v_n$, etc. | Individual ballots in V(*j*,*t*). |

Table 18-10 Terms used in logic verification

## 18.3.2 General constraints

Invariants:

$$t_O < t_C \leq t_E$$
$$S(c,r,t,v) \geq 0$$
$$S'(c,r,t,v) \geq 0$$

The following formalize several basic integrity constraints. Each textual description is intended to elucidate the formal constraint(s) that follow it. In case of discrepancy or confusion, the formal constraints are normative.

No ballots will be accepted before polls are opened or after polls have closed, or during the process of opening or closing the polls. (N.B., in early voting, polls are considered open when vote collection begins; see Volume III Section 7.2.)

$$t_O < D(v) < t_C$$

No votes will be counted until after polls are opened.

$$t \leq t_O \rightarrow S'(c,r,t,v) = 0$$

All tallies must remain zero until after polls are opened.

$$t \leq t_O \rightarrow T(c,j,r,t) = 0$$

A cast vote record cannot change once the voting session for that ballot has ended.

$$t \geq D(v) \rightarrow S(c,r,t,v) = S(c,r,D(v),v)$$

### 18.3.3 Cumulative voting

All valid votes must be counted, and only valid votes may be counted.[11]

$$t \geq t_E \rightarrow S'(c,r,t,v) = \begin{cases} S(c,r,D(v),v) & \text{if } S(r,D(v),v) \leq N(r) \wedge A(t,v) \\ 0 & \text{otherwise} \end{cases}$$

The final vote totals must accurately reflect all valid votes and only valid votes.

$$t \geq t_E \rightarrow T(c,j,r,t) = \sum_{v \in V(j,t_E)} S'(c,r,t_E,v)$$

The overvote and undervote totals must be correct.

$$t \geq t_E \rightarrow O(j,r,t) = \sum_{v \in V(j,t_E)} \begin{cases} N(r) & \text{if } S(r,D(v),v) > N(r) \wedge A(t,v) \\ 0 & \text{otherwise} \end{cases}$$

$$t \geq t_E \rightarrow U(j,r,t) = \sum_{v \in V(j,t_E)} \begin{cases} N(r) - S(r,D(v),v) & \text{if } S(r,D(v),v) \leq N(r) \wedge A(t,v) \\ 0 & \text{otherwise} \end{cases}$$

Every vote must be accounted for.

$$t \geq t_E \rightarrow \sum_{c \in C(r,t)} T(c,j,r,t) + O(j,r,t) + U(j,r,t) = K(j,r,t) \times N(r)$$

Note that all of the above constraints are predicated by $t \geq t_E$. No assertion has been made regarding the correctness of pre-final reports. Since the transmission and processing of vote data are not instantaneous, the correctness of a pre-final report can only be judged relative to some viewpoint (e.g., a central counting site, using whatever vote data they happen to have received and processed).

### 18.3.4 N of M contests (including 1-of-M)

N of M is identical to cumulative voting but for the addition of the following invariant, which reflects the design of a ballot style that allows only one vote in each ballot position (equivalent to a checkbox). In systems conforming to the *Write-ins* class, this property must be preserved through the reconciliation of aliases and double votes (Requirement III.6.8.2-A.9).

$$S(c, r, t, v) \leq 1$$

## 18.4 Role Model

This section is to be provided by STS. Move here from STS Draft Access Control Section.

# 4 Draft VVSG Recommendations to the EAC

**May 2007 DRAFT**

**VOLUME 4:**

**DOCUMENTATION STANDARD**

DOCUMENTATION REQUIREMENTS
FOR VENDORS AND VSTLS

# Volume 4 Table of Contents

# Volume 4: Standards on Data to be Provided

# Chapter 1: Introduction

## 1.1 Scope and Applicability

This part of the Voluntary Voting System Guidelines, the Standards on Data To Be Provided, contains requirements applying to the Technical Data Package, the Voting Equipment User Documentation, the Test Plan, the Test Report, the Public Information Package, and the data for repositories.

## 1.2 Audience

The Voluntary Voting System Guidelines are intended primarily for use by:

- Designers and manufacturers of voting systems;
- Test labs performing the analysis and testing of voting systems in support of the national certification process;
- Software repositories designated by the national certification authority or by a state; and
- Test labs and consultants performing the state certification of voting systems.

This part of the Voluntary Voting System Guidelines, the Standards on Data To Be Provided, is intended primarily for use by vendors, test labs, and software repositories.

# Chapter 2: Quality Assurance and Configuration Management Data Package (vendor)

This section contains requirements on the content of the quality assurance and configuration management documentation that vendors must supply in support of the Manufacturer Registration process.

## 2.1 Quality and Configuration Management Manual

→ **2.1-A** Develop and Present

All voting system vendors ***SHALL*** develop and present to the certification authority a complete Quality and Configuration Management Manual. This presentation ***SHALL*** occur during the Manufacturer Registration process as specified in [10].

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.1** Processes and Procedures

The Manual ***SHALL*** detail the vendor's Quality Assurance and Configuration Management processes and procedures required by the VVSG. These processes and procedures ***SHALL*** conform with all requirements of the VVSG and the standards listed in Volume III, Requirement 16.4.2.1-A.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.2** A Binding Commitment

The Manual ***SHALL*** declare that meeting the requirements of the entire VVSG is a binding commitment for the entire vendor organization.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.3** Project Plan

The Manual ***SHALL*** provide for the formulation of a project plan for the design and development of a voting system. It ***SHALL*** require the project plan to be clearly and unambiguously documented.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

DISCUSSION

The project plan should be consistent with the Design and Development Planning requirements, as specified in [QACM2] Section 7.3.1.

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.4** Quality Check

The Manual ***SHALL*** require the project plan to include, at a minimum, one quality check at the end of the design phase, and one quality check at the end of the development phase. The project plan ***SHALL*** define the progress that is required before each quality check can be passed.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

A "quality check" is the sum of the activities Design and Development Review, Design and Development Verification, and Design and Development Validation, as defined in [QACM2] Sections 7.3.4. through 7.3.6.

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.5** Problem Log

The Manual ***SHALL*** require the vendor to maintain a log in which all difficulties encountered during the design and development phase for a voting system are required to be recorded. Any remedial action taken to correct a difficulty ***SHALL*** also be recorded. The log ***SHALL*** be available for inspection by the test lab.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

"Difficulties" are any occasions when it is recognized that changes in past design decisions or in the project plan (see Requirement 2.1-A.3) are necessary to complete the project.

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.6** Critical Parts, Components, and Assemblies

The Manual ***SHALL*** specify rules that define what parts, components, and assemblies of the voting system are to be considered as critical. A part, component, or assembly ***SHALL*** be defined as critical if its failure may

- cause a faulty display of options
- cause an uncertainty if voter's choice has been recorded
- cause a false recording of vote cast
- cause the change of stored votes
- cause the false transmission for polling station totals
- cause injury to voters or staff
- provide an opening for tampering
- violate a voter's privacy
- cause a false accumulation of polling station totals

- cause a false transmission for regional totals
- give the appearance of irregularity
- violate a voter's ability to vote independently
- impede the usability of the polling station for all voters.

As used here, "components" ***SHALL*** include software modules.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.7** Testing Statements for Every Part, Component, and Assembly

The Manual ***SHALL*** require that the design and development process of a voting system produce statements for every part, component, and assembly, whether to be manufactured by the vendor or obtained elsewhere, that impacts conformity to the VVSG. These statements ***SHALL*** define verifiable requirements against which the part, component, or assembly can be tested at the end of its manufacturing process, or upon delivery, as appropriate. The requirements ***SHALL*** be defined in such a way that any part, component, or assembly that meets the requirements will provide the functionality and reliability required of it for the voting system to meet the overall functionality and reliability requirements specified in the VVSG.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.8** Inspection Processes for Every Part, Component, and Assembly

The Manual ***SHALL*** require that the design and development process define or identify processes by which all parts, components, and assemblies of a voting system can be tested for compliance with requirements developed under Requirement 2.1-A.7.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.9** Testing Statements for the Entire Voting System

The Manual ***SHALL*** require that the design and development process of a voting system produce a statement that defines verifiable requirements against which any voting system can be tested at the end of its manufacturing and assembly process in such a way that passing the test provides assurance that the voting system meets all requirements defined in the VVSG.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.10** Inspection of all Purchased Parts, Components, and Assemblies

The Manual ***SHALL*** require that all purchased parts, components and assemblies are tested according to the testing requirements developed under Requirement 2.1-A.7 and the processes developed under Requirement 2.1-A.8 before they are incorporated into a voting system. The records ***SHALL*** be maintained until such time as the certification of the voting system model expires or is revoked.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.11** Inspection of all Manufactured Parts, Components, and Assemblies

The Manual ***SHALL*** require that all manufactured parts, components, and assemblies are tested according to the testing requirements developed under Requirement 2.1-A.7 and the processes developed under Requirement 2.1-A.8 before they are incorporated into a voting system. The records ***SHALL*** be maintained until such time as the certification of the voting system model expires or is revoked.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.12** Records of all Critical Parts, Components, and Assemblies

The Manual ***SHALL*** require that for each part, component, or assembly, whether purchased or manufactured by the vendor, that has been defined as critical (Requirement 2.1-A.6), records ***SHALL*** be kept that document the complete history of the part, component, or assembly. The records ***SHALL*** include:

- the source of raw materials,
- the processes used in the manufacture,
- the time when critical manufacturing steps were taken,
- the organization or person that performed each critical manufacturing step, and
- the persons who performed the required inspections.

The records ***SHALL*** also include documentation of:

- any failures, discrepancies or anomalies that might have occurred during manufacture,
- any actions taken to correct the failure, discrepancy or anomaly, and
- the final determination that the problem has been corrected.

These records ***SHALL*** be available for inspection

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.13** Technical capability for monitoring

The Manual ***SHALL*** require the vendor to identify and maintain the technical capability to monitor the in-service performance of each voting system sold throughout the life cycle of the voting system's model.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

For the purpose of this and subsequent Requirements in this section, the term life cycle of a voting system model **SHALL** be defined as the time period from the delivery of the first voting system of that model to the time when the certification of the model expires or is revoked.

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.14** Technical capability for developing and implementing remedies

The Manual ***SHALL*** require the vendor to identify and maintain the technical capability to develop and implement remedies that are suitable to correct any defects that lead to in-service difficulties in all voting systems sold, throughout the life cycle of the voting system model.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

↳ **2.1-A.15** Financial capability to provide the product support

The Manual ***SHALL*** require the vendor to identify and maintain the financial capability to provide product support, as defined in Requirements 2.1-A.13 and 2.1-A.14, throughout the life cycle of the voting system model.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Inspection. Volume V, Section 3.1, Section 4.4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

# Chapter 3: Technical Data Package (vendor)

## 3.1 Scope

This section contains a description of vendor documentation relating to the voting system that must be submitted with the system as a precondition of national certification testing. These items are necessary to define the product and its method of operation; to provide technical and test data supporting the vendor's claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance. Any other items relevant to the system evaluation, such as media, materials, source code, object code, and sample output report formats, must be submitted along with this documentation.

This documentation is used by the test lab in constructing the certification testing plan and is particularly important in constructing plans for the re-testing of systems that have been certified previously. Re-testing of systems submitted by vendors that consistently adhere to particularly strong and well documented quality assurance and configuration management practices will generally be more efficient than for systems developed and maintained using less rigorous or less well documented practices.

Both formal documentation and notes of the vendor's system development process must be submitted for certification tests. Documentation describing the system development process permits assessment of the vendor's systematic efforts to develop and test the system and correct defects. Inspection of this process also enables the design of a more precise test plan. The accredited test lab must design and conduct the appropriate tests to cover all elements of the system and to ensure conformance with all system requirements.

### 3.1.1 Content and format

The content of the Technical Data Package (TDP) is intended to provide clear, complete descriptions of the following information about the system:

1. Overall system design, including subsystems, modules and the interfaces among them;
2. Specific functional capabilities provided by the system;
3. Performance and design specifications;
4. Design constraints, applicable standards, and compatibility requirements;

5. Personnel, equipment, and facility requirements for system operation, maintenance, and logistical support;
6. Vendor practices for assuring system quality during the system's development and subsequent maintenance; and
7. Vendor practices for managing the configuration of the system during development and for modifications to the system throughout its life cycle.

#### 3.1.1.1 Required content for initial certification

➞ **3.1.1.1-A** TDP, identify full system configuration

The vendor ***SHALL*** submit to the test lab documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the test lab for system certification testing.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.9.2.*

*Impact:* *Click here to add the Impact*

➞ **3.1.1.1-B** TDP, documents list

The vendor ***SHALL*** provide a list of all documents submitted controlling the design, construction, operation, and maintenance of the system.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.1.1.*

*Impact:* *Deleted subrequirement "in order of precedence" because nobody knew what it meant.*

➞ **3.1.1.1-C** TDP contents

At minimum, the TDP ***SHALL*** contain the following documentation:

1. Implementation statement;
2. The voting equipment user documentation (Volume IV Chapter 3);
3. System hardware specification;
4. Application logic design and specification;
5. System security specifications;
6. System test and verification specification;
7. Configuration management plan;
8. Quality assurance program;
9. System change notes; and
10. Configuration for testing.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.1.1.1.*

*Impact:* *Added implementation statement, user documentation, configuration for testing; removed all that which was moved into the user documentation.*

### 3.1.1.2 Required content for system changes and recertification

➔ **3.1.1.2-A** TDP, change notes

For systems seeking recertification, vendors ***SHALL*** submit system change notes as described in Volume IV Section 2.9, as well as current versions of all documents that have been updated to reflect system changes.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Vendors may also submit other information relevant to the evaluation of the system, such as test documentation, and records of the system's performance history, failure analysis and corrective actions.

*Source:* *[2] II.2.1.1.2.*

*Impact:* *Click here to add the Impact*

### 3.1.1.3 Format

The requirements for formatting the TDP are general in nature; specific format details are of the vendor's choosing.

➞ **3.1.1.3-A** TDP, table of contents and abstracts

The TDP ***SHALL*** include a detailed table of contents for the required documents, an abstract of each document and a listing of each of the informational sections and appendices presented.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.1.1.3.*

*Impact:* *Click here to add the Impact*

➞ **3.1.1.3-B** TDP, cross-index

A cross-index ***SHALL*** be provided indicating the portions of the documents that are responsive to documentation requirements enumerated in Requirement IV.2.1.1.1-C.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.1.1.3.*

*Impact:* *Click here to add the Impact*

## 3.1.2 Other uses for documentation

Although all of the TDP documentation is required for national certification testing, some of these same items may also be required during the state certification process and local level acceptance testing. Therefore, it is recommended that the technical documentation required for certification and acceptance testing be deposited in escrow.

## 3.1.3 Protection of proprietary information

→ **3.1.3-A** TDP, identify proprietary data

The vendor ***SHALL*** identify all documents, or portions of documents, containing proprietary information not approved for public release.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Any person or accredited test lab accepting proprietary information must agree to use it solely for the purpose of analyzing and testing the system, and must agree to refrain from otherwise using the proprietary information or disclosing it to any other person or agency without the prior written consent of the vendor, unless disclosure is legally compelled.

An accredited test lab may reject a Technical Data Package if it is so encumbered by intellectual property claims as to obstruct the lab's delivery of the Test Plan (Volume IV Chapter 4), Test Report (Volume IV Chapter 5) or Public Information Package (Volume IV Chapter 6).

An overuse of trade secret and patent protection may prevent certification by the certification authority or by individual states. E.g., [46] 3.42: "The Vendor's entire proposal response package **SHALL** not be considered proprietary."

For additional details see Ch. 10 of [10].

*Source:* *[2] II.2.1.3.*

*Impact:* *Click here to add the Impact*

→ **3.1.3-B** TDP, consolidate proprietary data

The vendor should consolidate proprietary information to facilitate its removal from the Public Information Package.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Stephen Berger, CRT teleconference, 20060720.*

*Impact:* *Click here to add the Impact*

## 3.2 Implementation Statement

➞ **3.2-A** TDP, implementation statement

The TDP ***SHALL*** include an implementation statement as defined in Volume III Section 2.5.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Vendors may wish to contact their intended testing labs in advance to determine if those labs can supply them with an implementation statement pro forma to facilitate meeting this requirement.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

## 3.3 System Hardware Specification

➞ **3.3-A** TDP, system hardware specification

The vendor ***SHALL*** expand on the system overview included in the user documentation by providing detailed specifications of the hardware components of the system, including specifications of hardware used to support the telecommunications capabilities of the system, if applicable.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.4.*

*Impact:* *Click here to add the Impact*

## 3.3.1 System hardware characteristics

**3.3.1-A** TDP, system hardware characteristics

The vendor ***SHALL*** provide a detailed discussion of the characteristics of the system, indicating how the hardware meets individual requirements defined in Volume III, including:

1. **Performance characteristics**: This discussion addresses basic system performance attributes and operational scenarios that describe the manner in which system functions are invoked, describe environmental capabilities, describe life expectancy, and describe any other essential aspects of system performance;
2. **Physical characteristics**: This discussion addresses suitability for intended use, requirements for transportation and storage, health and safety criteria, security criteria, and vulnerability to adverse environmental factors;
3. **Reliability**: This discussion addresses system and component reliability stated in terms of the system's operating functions, and identification of items that require special handling or operation to sustain system reliability;
4. **Maintainability**: Maintainability represents the ease with which maintenance actions can be performed based on the design characteristics of equipment and software and the processes the vendor and election officials have in place for preventing failures and for reacting to failures. Maintainability includes the ability of equipment and software to self-diagnose problems and make non-technical election workers aware of a problem. Maintainability also addresses a range of scheduled and unscheduled events; and
5. **Environmental conditions**: This discussion addresses the ability of the system to withstand natural environments, and operational constraints in normal and test environments, including all requirements and restrictions regarding electrical service, telecommunications services, environmental protection, and any additional facilities or resources required to install and operate the system.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.4.1.*

*Impact:* *Click here to add the Impact*

## 3.3.2 Design and construction

→ **3.3.2-A** TDP, identify system configuration

The vendor ***SHALL*** provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for testing.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.4.2.*

*Impact:* *Click here to add the Impact*

↳ **3.3.2-A.1** TDP, photographs for hardware validation

The vendor ***SHALL*** provide sufficient photographs of the exterior and interior of devices included in the system to identify the hardware of the system configuration submitted for testing.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[7]*

*Impact:* *Click here to add the Impact*

→ **3.3.2-B** TDP, list of materials

The vendor ***SHALL*** provide a list of materials and components used in the system and a description of their assembly into major system components and the system as a whole.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.4.2.*

*Impact:* *Click here to add the Impact*

➞ **3.3.2-C** TDP, design and construction miscellany

Text and diagrams ***SHALL*** be provided that describe:

1. Materials, processes, and parts used in the system, their assembly, and the configuration control measures to ensure compliance with the system specification;
2. The electromagnetic environment generated by the system;
3. Operator and voter safety considerations, and any constraints on system operations or the use environment; and
4. Human factors considerations, including provisions for access by disabled voters.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.4.2.*

*Impact:* *Click here to add the Impact*

## 3.3.3 Hardwired logic

➞ **3.3.3-A** TDP, hardwired and mechanical implementations of logic

For each non-COTS hardware component (e.g., an Application-Specific Integrated Circuit or a vendor-specific integration of smaller components), the vendor ***SHALL*** provide complete design and logic specifications, such as Computer Aided Design and Hardware Description Language files, that match the version of the component submitted for certification testing.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

➞ **3.3.3-B** TDP, PLDs, FPGAs and PICs

For each Programmable Logic Device (PLD), Field-Programmable Gate Array (FPGA) or Peripheral Interface Controller (PIC) that is programmed with non-COTS logic, the vendor ***SHALL*** provide complete logic specifications, such as Hardware Description Language files or source code, that match the version of the component submitted for certification testing.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

## 3.4 Application Logic Design and Specification

➞ **3.4-A** TDP, application logic design and specification

The vendor ***SHALL*** expand on the system overview included in the user documentation by providing detailed specifications of the application logic components of the system, including those used to support the telecommunications capabilities of the system, if applicable.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.*

*Impact:* *Click here to add the Impact*

## 3.4.1 Purpose and scope

➞ **3.4.1-A** TDP, describe application logic functions

The vendor ***SHALL*** describe the function or functions that are performed by the application logic comprising the system, including that used to support the telecommunications capabilities of the system, if applicable.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.1.*

*Impact:* *Click here to add the Impact*

## 3.4.2 Applicable documents

➞ **3.4.2-A** TDP, list documents controlling application logic development

The vendor ***SHALL*** list all documents controlling the development of application logic and its specifications.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.2.*

*Impact:* *Deleted subrequirement "in order of precedence" because nobody knew what it meant.*

## 3.4.3 Application logic overview

➞ **3.4.3-A** TDP, application logic overview

The vendor ***SHALL*** provide an overview of the application logic.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.3.*

*Impact:* *Click here to add the Impact*

↳ **3.4.3-A.1** TDP, application logic architecture

The overview ***SHALL*** include a description of the architecture, the design objectives, and the logic structure and algorithms used to accomplish those objectives.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.3.a, reworded.*

*Impact:* *Click here to add the Impact*

↳ **3.4.3-A.2** TDP, application logic design

The overview ***SHALL*** include the general design, operational considerations, and constraints influencing the design.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.3.b.*

*Impact:* *Click here to add the Impact*

↳ **3.4.3-A.3** TDP, application logic overview miscellany

The overview ***SHALL*** include the following additional information for each separate software package:

1. Package identification;

2. General description;
3. Requirements satisfied by the package;
4. Identification of interfaces with other packages that provide data to, or receive data from, the package; and
5. Concept of execution for the package.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.3.d.*

*Impact:* *Click here to add the Impact*

## 3.4.4 Application logic standards and conventions

➞ **3.4.4-A** TDP, application logic standards and conventions

The vendor ***SHALL*** provide information that can be used by an accredited test lab or state certification board to support analysis and test design. The information ***SHALL*** address standards and conventions developed internally by the vendor as well as published industry standards that have been applied by the vendor.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.4.*

*Impact:* *Click here to add the Impact*

➞ **3.4.4-B** TDP, application logic standards and conventions, checklist

The vendor ***SHALL*** provide information that addresses the following standards and conventions related to application logic:

1. Development methodology;
2. Design standards, including internal vendor procedures;
3. Specification standards, including internal vendor procedures;
4. Coding conventions, including internal vendor procedures;

5. Testing and verification standards, including internal vendor procedures, that can assist in determining the correctness of the logic; and
6. Quality assurance standards or other documents that can be used to examine and test the application logic. These documents include standards for logic diagrams, program documentation, test planning, and test data acquisition and reporting.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.4.*

*Impact:* *Click here to add the Impact*

➞ **3.4.4-C** TDP, justify coding conventions

The vendor ***SHALL*** furnish evidence that the selected coding conventions are "published" and "credible" as specified in Requirement III.5.4.1.3-A.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

## 3.4.5 Application logic operating environment

➞ **3.4.5-A** TDP, application logic operating environment

The vendor ***SHALL*** describe or make reference to all operating environment factors that influence the design of application logic.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.5.*

*Impact:* *Click here to add the Impact*

### 3.4.5.1 Hardware environment and constraints

➞ **3.4.5.1-A** TDP, hardware environment and constraints

The vendor ***SHALL*** identify and describe the hardware characteristics that influence the design of the application logic, such as:

1. The logic and arithmetic capability of the processor;
2. Memory read-write characteristics;
3. External memory device characteristics;
4. Peripheral device interface hardware;
5. Data input/output device protocols; and
6. Operator controls, indicators, and displays.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.5.1.*

*Impact:* *Click here to add the Impact*

### 3.4.5.2 Application logic environment

➞ **3.4.5.2-A** TDP, identify operating system

The vendor ***SHALL*** identify the operating system and the specific version thereof, or else clarify how the application logic operates without an operating system.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.5.2.*

*Impact:* *Click here to add the Impact*

➞ **3.4.5.2-B** TDP, identify compilers and assemblers

For systems containing compiled or assembled application logic, the vendor ***SHALL*** identify the COTS compilers or assemblers used in the generation of executable code, and the specific versions thereof.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

See Requirement III.5.4.1.7-A.4. Although compiled code should not be very sensitive to the versioning of the compiler, this information should be documented in case complications arise.

*Source:* *[2] II.2.5.5.2.*

*Impact:* *Click here to add the Impact*

➞ **3.4.5.2-C** TDP, identify interpreters

For systems containing interpreted application logic, the vendor ***SHALL*** specify the COTS runtime interpreter that ***SHALL*** be used to run this code, and the specific version thereof.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

See Requirement III.5.4.1.7-A.5.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

## 3.4.6 Application logic functional specification

➞ **3.4.6-A** TDP, application logic functional specification

The vendor ***SHALL*** provide a description of the operating modes of the system and of application logic capabilities to perform specific functions.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.6.*

*Impact:* *Click here to add the Impact*

### 3.4.6.1 Functions and operating modes

➞ **3.4.6.1-A** TDP, functions and operating modes

The vendor ***SHALL*** describe all application logic functions and operating modes of the system, such as ballot preparation, election programming, preparation for opening the polls, recording votes and/or counting ballots, closing the polls, and generating reports.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

The word "function" here has the meaning suggested by the list of voting activities and should not be interpreted in the sense callable unit.

*Source:* *[2] II.2.5.6.1.*

*Impact:* *Click here to add the Impact*

➞ **3.4.6.1-B** TDP, functions and operating modes detail

For each application logic function or operating mode, the vendor ***SHALL*** provide:

1. A definition of the inputs to the function or mode (with characteristics, limits, tolerances or acceptable ranges, as applicable);
2. An explanation of how the inputs are processed; and
3. A definition of the outputs produced (again, with characteristics, limits, tolerances, or acceptable ranges, as applicable).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.6.1.*

*Impact:* *Click here to add the Impact*

### 3.4.6.2 Application logic integrity features

➞ **3.4.6.2-A** TDP, application logic integrity features

The vendor ***SHALL*** describe the application logic's capabilities or methods for detecting or handling:

1. Exception conditions;
2. System failures;
3. Data input/output errors;
4. Error logging for audit record generation;
5. Production of statistical ballot data;
6. Data quality assessment; and
7. Security monitoring and control.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.6.2.*

*Impact:* *Click here to add the Impact*

## 3.4.7 Programming specifications

➞ **3.4.7-A** TDP, programming specifications

The vendor ***SHALL*** provide in this section an overview of the application logic's design, its structure, and implementation algorithms and detailed specifications for individual modules.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.7.*

*Impact:* *Click here to add the Impact*

### 3.4.7.1 Programming specifications overview

**3.4.7.1-A** TDP, programming specifications overview

The programming specifications overview ***SHALL*** document the architecture of the application logic.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Summary of [2] II.2.5.7.1.*

*Impact:* *Click here to add the Impact*

**3.4.7.1-A.1** TDP, programming specifications overview, diagrams

This overview ***SHALL*** include such items as UML diagrams, data flow diagrams, and/or other graphical techniques that facilitate understanding of the programming specifications.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.7.1.*

*Impact:* *Click here to add the Impact*

**3.4.7.1-A.2** TDP, programming specifications overview, function

This section ***SHALL*** be prepared to facilitate understanding of the internal functioning of the individual modules.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.7.1.*

*Impact:* *Click here to add the Impact*

↳ **3.4.7.1-A.3** TDP, programming specifications overview, content

Implementation of the functions ***SHALL*** be described in terms of the architecture, algorithms, and data structures.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.7.1.*

*Impact:* *Click here to add the Impact*

### 3.4.7.2 Programming specifications details

→ **3.4.7.2-A** TDP, programming specifications details

The programming specifications ***SHALL*** describe individual application logic modules and their component units, if applicable.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.7.2.*

*Impact:* *Click here to add the Impact*

→ **3.4.7.2-B** TDP, module and callable unit documentation

For each application logic module and callable unit, the vendor ***SHALL*** document:

1. Significant module and unit design decisions, if any, such as algorithms used;
2. Any constraints, limitations, or unusual features in the design of the module or callable unit;

3. A description of its inputs, outputs, and other data elements as applicable with respect to communication over system interfaces (see Volume IV Section 2.4.9).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.7.2.a, b, and e.*

*Impact:* *Deleted subrequirement f ("If the software module or unit contains logic...") and g ("If the software module is a database..."). Both are apparently redundant, though it is less clear for f, which is strangely written.*

→ **3.4.7.2-C** TDP, justify mixed-language software

If an application logic module is written in a programming language other than that generally used within the system, the specification for the module ***SHALL*** indicate the programming language used and the reason for the difference.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.7.2.c.*

*Impact:* *Click here to add the Impact*

→ **3.4.7.2-D** TDP, references for foreign programming languages

If a module contains embedded border logic commands for an external library or package (such as menu selections in a database management system for defining forms and reports, on-line queries for database access and manipulation, input to a graphical user interface builder for automated code generation, commands to the operating system, or shell scripts), the specification for the module ***SHALL*** contain a reference to user manuals or other documents that explain them.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.7.2.d.*

*Impact:* *Removed requirement to list the commands. Should be obvious from the sources.*

➞ **3.4.7.2-E** TDP, source code

For each callable unit (function, method, operation, subroutine, procedure, etc.) in application logic, border logic, and third-party logic, the vendor ***SHALL*** supply the source code.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.1.*

*Impact:* *Windows CE and other borderline cases are now covered.*

➞ **3.4.7.2-F** TDP, inductive assertions

For each callable unit (function, method, operation, subroutine, procedure, etc.) in core logic, the vendor ***SHALL*** specify:

1. The preconditions and postconditions of the callable unit, formally stated using the terms defined in Volume III Section 7.3.1 and possibly other terms defined by the vendor, including any assumptions about capacities and limits within which the system is expected to operate; and
2. Using the pre- and postconditions of any invoked units as given partial proofs, a sound argument (possibly, but not necessarily, a formal proof) that the preconditions and postconditions of the callable unit accurately represent its behavior.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Sufficient invariants and assertions should be provided to make it possible to perform the verification of Volume V Section 4.7 through purely local checks (i.e., using the callable unit itself, the pre- and postconditions of any invoked units, and the invariants of any global data accessed by the callable unit, but not the source code of the invoked units nor any other logic).

The use of preconditions and postconditions as inductive assertions derives primarily from [15], but a list of relevant work predating [15] can be found in [17]. As a pragmatic compromise to avert "analysis paralysis," the verification described here is considerably less rigorous than was envisioned in the literature.

A sound argument need not be complicated. In cases where the relationship between preconditions and postconditions and the behavior of the callable unit is completely obvious or trivial, it may suffice to state as much. The acceptance of such a statement is at the discretion of the test lab.

Postconditions that impact something outside the domain of discourse are not of interest unless that thing impacts the behavior of some function with respect to the domain of discourse. The vendor must define such terms as are necessary to state any and all dependencies and assumptions that may impact the behavior and use them consistently in all affected preconditions and postconditions. *An excess of extraneous dependencies may negatively impact the test lab's ability to verify the system's correctness and thereby prevent certification.*

A callable unit that has no impact on anything in the domain of discourse and no dependency on anything in the domain of discourse is not core logic.

*Source:* *New requirement.*

*Impact:* *Part of response to TGDC Resolution #29-05.*

→ **3.4.7.2-G** TDP, high-level constraints

Using the preconditions and postconditions of callable units as given partial proofs, the vendor ***SHALL*** specify a sound argument (possibly, but not necessarily, a formal proof) that the core logic as a whole satisfies each of the constraints indicated in Volume III Section 7.3 for all cases within the aforementioned capacities and limits.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Part of response to TGDC Resolution #29-05.*

→ **3.4.7.2-H** TDP, justify long units

The vendor ***SHALL*** justify any callable unit lengths that violate Requirement III.5.4.1.4-B.1.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] II.5.4.2.i.*

*Impact:* *Click here to add the Impact*

## 3.4.8 System database

➞ **3.4.8-A** TDP, system database

The vendor ***SHALL*** identify and provide a diagram and narrative description of the system's databases and any external files used for data input or output.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.8.*

*Impact:* *Click here to add the Impact*

➞ **3.4.8-B** TDP, database design levels

For each database or external file, the vendor ***SHALL*** specify the number of levels of design and the names of those levels (such as conceptual, internal, logical, and physical).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.8.a.*

*Impact:* *Click here to add the Impact*

**3.4.8-C** TDP, database design conventions

For each database or external file, the vendor ***SHALL*** specify any design conventions and standards (which may be incorporated by reference) needed to understand the design.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.8.b.*

*Impact:* *Click here to add the Impact*

**3.4.8-D** TDP, data models

For each database or external file, the vendor ***SHALL*** identify and describe all logical entities and relationships and how these are implemented physically (e.g., tables, files).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

This requirement calls for a data model but a specific modelling language is no longer mandated.

*Source:* *[2] II.2.5.8.c and d.*

*Impact:* *Click here to add the Impact*

**3.4.8-E** TDP, schemata

The vendor ***SHALL*** document the details of table, record or file contents (as applicable), individual data elements and their specifications, including:

1. Names/identifiers;
2. Data type (alphanumeric, integer, etc.);
3. Size and format (such as length and punctuation of a character string);
4. Units of measurement (such as meters, seconds);
5. Range or enumeration of possible values (such as 0–99);
6. Accuracy (how correct) and precision (number of significant digits);

7. Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply;
8. Security and privacy constraints; and
9. Sources (setting/sending entities) and recipients (using/receiving entities).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

The majority of this requirement may be satisfied by supplying the source of the database schema if it is in a widely recognized and standardized language.

*Source:* *[2] II.2.5.8.e.*

*Impact:* *Click here to add the Impact*

➞ **3.4.8-F** TDP, external file maintenance and security

For external files, vendors ***SHALL*** document the procedures for file maintenance, management of access privileges, and security.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.8.f.*

*Impact:* *Click here to add the Impact*

## 3.4.9 Interfaces

➞ **3.4.9-A** TDP, identify and describe interfaces

Using a combination of text and diagrams, the vendor ***SHALL*** identify and provide a complete description of all major internal and external interfaces.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

"Major" interfaces are at the level of those identified in the system overview (Volume IV Section 3.1). These are interfaces between subsystems and components, not callable units.

*Source:* *[2] II.2.5.9.*

*Impact:* *Click here to add the Impact*

### 3.4.9.1 Interface identification

➞ **3.4.9.1-A** TDP, interface identification details

For each interface identified in the system overview, the vendor ***SHALL***:

1. Provide a unique identifier assigned to the interface;
2. Identify the interfacing entities (systems, configuration items, users, etc.) by name, number, version, and documentation references, as applicable; and
3. Identify which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed on them).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.9.1.*

*Impact:* *Click here to add the Impact*

### 3.4.9.2 Interface description

➞ **3.4.9.2-A** TDP, interface types

For each interface identified in the system overview, the vendor ***SHALL*** describe the type of interface (such as real-time data transfer or data storage-and-retrieval) to be implemented.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.9.2.a.*

*Impact:* *Click here to add the Impact*

➞ **3.4.9.2-B** TDP, interface signatures

For each interface identified in the system overview, the vendor ***SHALL*** describe characteristics of individual data elements that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:

1. Names/identifiers;
2. Data type (alphanumeric, integer, etc.);
3. Size and format (such as length and punctuation of a character string);
4. Units of measurement (such as meters, seconds);
5. Range or enumeration of possible values (such as 0–99);
6. Accuracy (how correct) and precision (number of significant digits);
7. Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply;
8. Security and privacy constraints; and
9. Sources (setting/sending entities) and recipients (using/receiving entities).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.9.2.b.*

*Impact:* *Click here to add the Impact*

➞ **3.4.9.2-C** TDP, interface protocols

For each interface identified in the system overview, the vendor ***SHALL*** describe characteristics of communication methods that the interfacing entity(ies) will use for the interface, such as:

1. Communication links/bands/frequencies/media and their characteristics;
2. Message formatting;
3. Flow control (such as sequence numbering and buffer allocation);
4. Data transfer rate, whether periodic/aperiodic, and interval between transfers;
5. Routing, addressing, and naming conventions;
6. Transmission services, including priority and grade; and
7. Safety/security/privacy considerations, such as encryption, user authentication, compartmentalization, and auditing.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

STS: Communications: STS (Bill Burr) should revise this.

*Source:* *[2] II.2.5.9.2.c.*

*Impact:* *Click here to add the Impact*

→ **3.4.9.2-D** TDP, protocol details

For each interface identified in the system overview, the vendor ***SHALL*** describe characteristics of protocols the interfacing entity(ies) will use for the interface, such as:

1. Priority/layer of the protocol;
2. Packeting, including fragmentation and reassembly, routing, and addressing;
3. Legality checks, error control, and recovery procedures;
4. Synchronization, including connection establishment, maintenance, termination; and
5. Status, identification, and any other reporting features.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

STS: Communications: STS (Bill Burr) should revise this. Requiring vendors to use industry standard protocols would reduce the need for this.

*Source:* *[2] II.2.5.9.2.d.*

*Impact:* *Click here to add the Impact*

→ **3.4.9.2-E** TDP, interface etceteras

For each interface identified in the system overview, the vendor ***SHALL*** describe any other pertinent characteristics, such as physical compatibility of the interfacing entity(ies) (dimensions, tolerances, loads, voltages, plug compatibility, etc.).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.9.2.e.*

*Impact:* *Click here to add the Impact*

### 3.4.10 Appendices

The vendor may provide descriptive material and data supplementing the various sections of the body of the logic specifications. The content and arrangement of appendices are at the discretion of the vendor. Topics recommended for amplification or treatment in appendix form include:

1. **Glossary:** A listing and brief definition of all module names and variable names, with reference to their locations in the logic structure. Abbreviations, acronyms, and terms should be included, if they are either uncommon in data processing and software development or are used with an unorthodox meaning;
2. **References:** A list of references to all related vendor documents, data, standards, and technical sources used in logic development and testing; and
3. **Program Analysis:** The results of logic configuration analysis algorithm analysis and selection, timing studies, and hardware interface studies that are reflected in the final logic design and coding.

## 3.5 System Security Specifications

This section is to be provided by STS.

## 3.6 System Test and Verification Specification

➔ **3.6-A** TDP, development and certification tests

The vendor ***SHALL*** provide test and verification specifications for:

1. Development test specifications; and
2. National certification test specifications.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.7.*

*Impact:* *Click here to add the Impact*

## 3.6.1 Development test specifications

➞ **3.6.1-A** TDP, development test specifications

The vendor ***SHALL*** describe the plans, procedures, and data used during development and system integration to verify system logic correctness, data quality, and security. This description ***SHALL*** include:

1. Test identification and design, including test structure, test sequence or progression, and test conditions;
2. Standard test procedures, including any assumptions or constraints;
3. Special purpose test procedures including any assumptions or constraints;
4. Test data, including the data source, whether it is real or simulated, and how test data are controlled;
5. Expected test results; and
6. Criteria for evaluating test results.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Documentation that is already required under the life cycle process adopted by the vendor may satisfy this requirement.

Previous iterations of these Guidelines cited MIL-STD-498, Software Test Plan and Software Test Description. That standard was cancelled in 1998. Currently applicable standards include [39] and [40].

*Source:* *[2] II.2.7.1.*

*Impact:* *Click here to add the Impact*

## 3.6.2 National certification test specifications

➞ **3.6.2-A** TDP, usability test reports

The vendor ***SHALL*** document all the usability testing performed as required in Dangling ref: PleaseAddReference_HFP_UsabilityTestingByVendor and report the test results using the Common Industry Format (CIF).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

→ **3.6.2-B** TDP, functional test specifications

The vendor ***SHALL*** provide specifications for verification and validation of overall system performance. These specifications ***SHALL*** cover:

1. Control and data input/output;
2. Processing accuracy;
3. Data quality assessment and maintenance;
4. Ballot interpretation logic;
5. Exception handling;
6. Security;
7. Production of audit trails and statistical data;
8. Expected test results; and
9. Criteria for evaluating test results.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

*Source:* *[2] II.2.7.2.*

*Impact:* *Clarified "acceptance criteria."*

→ **3.6.2-C** TDP, demonstrate fitness for purpose

The specifications ***SHALL*** identify procedures for assessing and demonstrating the suitability of the system for election use.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.7.2.*

*Impact:* *Click here to add the Impact*

## 3.7 System Change Notes

→ **3.7-A** TDP, system change notes

Vendors submitting modifications for a system that has been tested previously and received national certification ***SHALL*** submit system change notes.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

These will be used by the accredited test lab to assist in developing and executing the test plan for the modified system.

*Source:* *[2] II.2.13.*

*Impact:* *Click here to add the Impact*

➞ **3.7-B** TDP, system change notes content

The system change notes ***SHALL*** include the following information:

1. Summary description of the nature and scope of the changes, and reasons for each change;
2. A listing of the specific changes made, citing the specific system configuration items changed and providing detailed references to the documentation sections changed;
3. The specific sections of the documentation that are changed (or completely revised documents, if more suitable to address a large number of changes); and
4. Documentation of the test plan and procedures executed by the vendor for testing the individual changes and the system as a whole, and records of test results.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.13.*

*Impact:* *Click here to add the Impact*

# 3.8 Configuration for Testing

Configuration of hardware and software, both operating systems and applications, is critical to proper system functioning. Correct test design and sufficient test execution must account for the intended and proper configuration of all system components. If the voting system can be set up in both conforming and nonconforming configurations, the configuration actions necessary to obtain conforming behavior must be specified.

→ **3.8-A** TDP, photographs illustrating hardware set-up

The vendor ***SHALL*** provide photographs illustrating the proper set-up of the voting system hardware.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[7] as clarified 2006-07-20.*

*Impact:* *Click here to add the Impact*

→ **3.8-B** TDP, provide answers to installation prompts

The vendor ***SHALL*** provide a record of all user selections made during software/firmware installation.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Screen shots showing the installation actions may be helpful.

*Source:* *[2] I.4.1.1.*

*Impact:* *Click here to add the Impact*

→ **3.8-C** TDP, post-install configuration

The vendor ***SHALL*** also submit a record of all configuration changes made to the software or firmware following its installation.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Screen shots showing the configuration actions may be helpful.

*Source:* *[2] I.4.1.1.*

*Impact:* *Click here to add the Impact*

➜ **3.8-D** TDP, configuration data

The vendor ***SHALL*** submit all configuration data needed to set up and operate the voting system.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

# Chapter 4: Voting Equipment User Documentation (vendor)

This section contains requirements on the content of the documentation that vendors supply to jurisdictions that use their systems. The user documentation is also included in the TDP given to test labs.

It is not the intent of these requirements to prescribe an outline for user documentation. Vendors are encouraged to innovate in the quality and clarity of their user documentation. The intent of these requirements is to ensure that certain information that is of interest to end users and test labs alike will be included somewhere in the user documentation. To speed the test lab review, vendors should provide test labs with a short index that points out which sections of the user documentation are responsive to which sections of these requirements.

## 4.1 System Overview

→ **4.1-A** User docs, system overview

In the system overview, the vendor ***SHALL*** provide information that enables the user to identify the functional and physical components of the system, how the components are structured, and the interfaces between them.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] II.2.2.*

*Impact:* *Click here to add the Impact*

↳ **4.1-A.1** System overview, functional diagram

The system overview ***SHALL*** include a high-level functional diagram of the voting system that includes all of its components. The diagram ***SHALL*** portray how the various components relate and interact.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[10] 4.3.2.3*

*Impact:* *Click here to add the Impact*

## 4.1.1 System description

➔ **4.1.1-A** User docs, system description

The system description ***SHALL*** include written descriptions, drawings and diagrams that present:

1. A description of the functional components (or subsystems) as defined by the vendor (e.g., environment, election management and control, vote recording, vote conversion, reporting, and their logical relationships);
2. A description of the operational environment of the system that provides an overview of the hardware, firmware, software, and communications structure;
3. A concept of operations that explains each system function and how the function is achieved in the design;
4. Descriptions of the functional and physical interfaces between subsystems and components;
5. Identification of all COTS products (both hardware and software) included in the system and/or used as part of the system's operation, identifying the name, vendor, and version used for each such component;
6. Communications (dial-up, network) software;
7. Interfaces among internal components and interfaces with external systems. For components that interface with other components for which multiple products may be used, the vendor **SHALL** identify file specifications, data objects, or other means used for information exchange, and the public standard used for such file specifications, data objects, or other means; and
8. Benchmark directory listings for all software and firmware and associated documentation included in the vendor's release in the order in which each piece of software or firmware would normally be installed upon system setup and installation.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] II.2.2.1.*

*Impact:* *Click here to add the Impact*

→ **4.1.1-B** User docs, identify software and firmware by origin

The system description ***SHALL*** include the identification of all software and firmware items, indicating items that were:

1. Written in-house;
2. Written by a subcontractor;
3. Procured as COTS; and
4. Procured and modified, including descriptions of the modifications to the software or firmware and to the default configuration options.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.5.3.c.*

*Impact:* *Click here to add the Impact*

→ **4.1.1-C** User docs, traceability of procured software

The system description ***SHALL*** include a certification that procured software items were obtained directly from the manufacturer or a licensed dealer or distributor.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

For most noncommercial software, this would mean certifying that the software was downloaded from the canonical site or a trustworthy mirror. It is generally accepted practice for the core contributors to major open-source software packages to digitally sign the distributions. Verifying these signatures provides greater assurance that the package has not been modified.

*Source:* *[2] II.2.5.3.*

*Impact:* *Click here to add the Impact*

## 4.1.2 System performance

**4.1.2-A** User docs, system performance

The vendor ***SHALL*** provide system performance information including:

1. The device capacities and limits that were stated in the implementation statement (see Volume III Section 2.5);
2. If not already covered in the implementation statement, the performance characteristics of each operating mode and function in terms of expected and maximum speed, throughput capacity, maximum volume (maximum number of voting positions and maximum number of ballot styles supported), and processing frequency;
3. Quality attributes such as reliability, maintainability, availability, usability, and portability;
4. Provisions for safety, security, privacy, and continuity of operation; and
5. Design constraints, applicable standards, and compatibility requirements.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.2.2.*

*Impact:* *Click here to add the Impact*

**4.1.2-A.1** User docs, central tabulator capacity

The capacity for a central tabulator ***SHALL*** be documented by the vendor. This documentation ***SHALL*** include the capacity for individual components that impact the overall capacity.

*Applies to:* *Central tabulator*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

The capacity to convert the marks on individual ballots into signals is uniquely important to central count systems.

*Source:* *[2] I.3.2.5.1.1.*

*Impact:* *Click here to add the Impact*

↳ **4.1.2-A.2** User docs, reliably detectable marks

For an optical scanner, the vendor ***SHALL*** document what constitutes a reliably detectable mark versus a marginal mark.

*Applies to:* *Optical scanner*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

See Volume III Section 1.4.4. The specification may be parameterized by configuration values and should state the uncertainty.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

## 4.2 System Functionality Description

➞ **4.2-A** User docs, system functionality description

The vendor ***SHALL*** provide a listing of the system's functional processing capabilities, encompassing capabilities required by the Guidelines and any additional capabilities provided by the system, with a simple description of each capability.

1. The vendor **SHALL** explain, in a manner that is understandable to users, the capabilities of the system that were declared in the implementation statement;
2. Additional capabilities (extensions) **SHALL** be clearly indicated;
3. Required capabilities that may be bypassed or deactivated during installation or operation by the user **SHALL** be clearly indicated;
4. Additional capabilities that function only when activated during installation or operation by the user **SHALL** be clearly indicated; and
5. Additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user **SHALL** be clearly indicated.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.3.*

*Impact:* *Removed redundancy with implementation statement.*

## 4.3 System Security Specification

This section to be provided by STS. Resolution #18-05.

## 4.4 System Operations Manual

➞ **4.4-A** User docs, system operations manual

The system operations manual ***SHALL*** provide all information necessary for system use by all personnel who support pre-election and election preparation, polling place activities and central counting activities, as applicable, with regard to all system functions and operations identified in Volume IV Section 3.2.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

The nature of the instructions for operating personnel will depend upon the overall system design and required skill level of system operations support personnel.

*Source:* *[2] II.2.8.*

*Impact:* *Click here to add the Impact*

➞ **4.4-B** Operations manual, support training

The system operations manual ***SHALL*** contain all information that is required for the preparation of detailed system operating procedures and for the training of administrators, central election officials, election judges and poll workers.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.8.*

*Impact:* *Click here to add the Impact*

## 4.4.1 Introduction

**4.4.1-A** Operations manual, functions and modes

The vendor ***SHALL*** provide a summary of system operating functions and modes in sufficient detail to permit understanding of the system's capabilities and constraints.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.8.1.*

*Impact:* *Click here to add the Impact*

**4.4.1-B** Operations manual, roles

The roles of operating personnel ***SHALL*** be identified and related to the operating modes of the system.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.8.1.*

*Impact:* *Click here to add the Impact*

**4.4.1-C** Operations manual, conditional actions

Decision criteria and conditional operator functions (such as error and failure recovery actions) ***SHALL*** be described.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.8.1.*

*Impact:* *Click here to add the Impact*

➞ **4.4.1-D** Operations manual, references

The vendor ***SHALL*** also list all reference and supporting documents pertaining to the use of the system during election operations.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.8.1.*

*Impact:* *Click here to add the Impact*

## 4.4.2 Operational environment

➞ **4.4.2-A** Operations manual, operational environment

The vendor ***SHALL*** describe the system environment and the interface between the user or operator and the system.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.8.2.*

*Impact:* *Click here to add the Impact*

➞ **4.4.2-B** Operations manual, operational environment details 1

The vendor ***SHALL*** identify all facilities, furnishings, fixtures, and utilities that will be required for equipment operations, including equipment that operates at the:

1. Polling place;
2. Central count facility; and
3. Other locations.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.8.2.*

*Impact:* *Click here to add the Impact*

➞ **4.4.2-C** Operations manual, operational environment details 2

The user documentation supplied by the vendor ***SHALL*** include a statement of all requirements and restrictions regarding environmental protection, electrical service, recommended auxiliary power, telecommunications service, and any other facility or resource required for the proper installation and operation of the system.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.2.*

*Impact:* *Click here to add the Impact*

## 4.4.3 System installation and test specification

➞ **4.4.3-A** Operations manual, readiness testing

The vendor ***SHALL*** provide specifications for validation of system installation and readiness.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.8.3.*

*Impact:* *Click here to add the Impact*

↳ **4.4.3-A.1** Operations manual, test everything

These specifications ***SHALL*** address all components of the system and all locations of installation (e.g., polling place, central count facility), and ***SHALL*** address all elements of system functionality and operations identified in Volume IV Section 3.2 above, including general capabilities and functions specific to particular voting activities.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.8.3.*

*Impact:* *Removed references to acceptance testing (out of scope).*

## 4.4.4 Operational features

➞ **4.4.4-A** Operations manual, features

The vendor ***SHALL*** provide documentation of system operating features that includes:

1. A detailed description of all input, output, control, and display features accessible to the operator or voter;
2. Examples of simulated interactions to facilitate understanding of the system and its capabilities;
3. Sample data formats and output reports; and
4. Illustration and description of all status indicators and information messages.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.8.4.*

*Impact:* *Click here to add the Impact*

➞ **4.4.4-B** Operations manual, document scratch vote algorithms

For systems that support straight party voting, the vendor ***SHALL*** document the available algorithms for counting scratch votes.

*Applies to:* *Straight party voting*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

See Requirement III.6.8.2-A.12.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

➞ **4.4.4-C** Operations manual, document double vote reconciliation algorithms

For systems that support write-in voting, the vendor ***SHALL*** document the available algorithms for reconciling write-in double votes.

*Applies to:* *Write-ins*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

See Requirement III.6.8.2-A.9.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

## 4.4.5 Operating procedures

➞ **4.4.5-A** Operations manual, operating procedures

The vendor ***SHALL*** provide documentation of system operating procedures that:

1. Provides a detailed description of procedures required to initiate, control, and verify proper system operation;
2. Provides procedures that clearly enable the operator to assess the correct flow of system functions (as evidenced by system-generated status and information messages);
3. Provides procedures that clearly enable the administrator to intervene in system operations to recover from an abnormal system state;

4. Defines and illustrates the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system;
5. Defines and illustrates procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved. Such information also **SHALL** be provided for the interaction of the system with other data processing systems or data interchange protocols;
6. Provides administrative procedures and off-line operator duties (if any) if they relate to the initiation or termination of system operations, to the assessment of system status, or to the development of an audit trail;
7. Supports successful ballot and program installation and control by central election officials;
8. Provides a schedule and steps for the software and ballot installation, including a table outlining the key dates, events and deliverables; and
9. Specifies diagnostic tests that may be employed to identify problems in the system, verify the correction of problems, and isolate and diagnose faults from various system states.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.3.a and II.2.8.5.*

*Impact:* *Click here to add the Impact*

## 4.4.6 Documentation for poll workers

These requirements were incorporated from HFP. The requirements on content (as opposed to usability) are partly or wholly redundant with the preceding sections, are they not?

→ **4.4.6-A** Documentation Usability

The system ***SHALL*** include clear, complete, and detailed instructions and messages for setup, polling and shutdown.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

This requirement covers documentation for those aspects of system operation normally performed by poll workers and other "non-expert" operators. It does not address inherently complex operations such as ballot definition. The instructions would usually be in the form of a written manual, but could also be presented on

other media, such as a DVD or videotape. In the context of this requirement "message" means information delivered by the system to the poll worker as he/she attempts to perform a setup, polling, or shutdown operation.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

↳ **4.4.6-A.1** Poll Workers as Target Audience

The documentation required for normal system operation ***SHALL*** be presented at a level appropriate for non-expert poll workers.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

For instance, the documentation should not presuppose familiarity with personal computers.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

↳ **4.4.6-A.2** Usability at the Polling Place

The documentation ***SHALL*** be in a format suitable for practical use in the polling place.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

For instance, a single large reference manual that simply presents details of all possible operations would be difficult to use, unless accompanied by aids such as a simple "how-to" guide.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

↳ **4.4.6-A.3** Enabling Verification of Correct Operation

The instructions and messages ***SHALL*** enable the poll worker to verify that the system

1. Has been set up correctly (setup);
2. Is in correct working order to record votes (polling); and
3. Has been shut down correctly (shutdown).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

The poll worker should not have to guess whether he/she has performed the operation correctly. The documentation should make it clear what the system "looks like" when correctly configured.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

## 4.4.7 Operations support

→ **4.4.7-A** Operations manual, operations support

The vendor ***SHALL*** provide documentation of system operating procedures that:

1. Defines the procedures required to support system acquisition, installation, and readiness testing; and
2. Describes procedures for providing technical support, system maintenance and correction of defects and for incorporating hardware upgrades and new software releases.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.8.6.*

*Impact:* *Click here to add the Impact*

## 4.4.8 Transportation and storage

→ **4.4.8-A** Operations manual, transportation

The user documentation ***SHALL*** include any special instructions for preparing voting devices for shipment.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

➞ **4.4.8-B** Operations manual, storage

The user documentation ***SHALL*** include any special storage instructions for voting devices.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.2.1.*

*Impact:* *Click here to add the Impact*

➞ **4.4.8-C** Operations manual, procedures to ensure archivalness

The user documentation ***SHALL*** detail the care and handling precautions necessary for removable media and records to satisfy Requirement III.5.5.1-A.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

## 4.4.9 Appendices

The vendor may provide descriptive material and data supplementing the various sections of the body of the system operations manual. The content and

arrangement of appendices are at the discretion of the vendor. Topics recommended for discussion include:

4. Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer operations;
5. References: A list of references to all vendor documents and to other sources related to operation of the system;
6. Detailed Examples: Detailed scenarios that outline correct system responses to faulty operator input. Alternative procedures may be specified depending on the system state; and
7. Manufacturer's Recommended Security Procedures: Security procedures that are to be executed by the system operator.

# 4.5 System Maintenance Manual

➞ **4.5-A** User docs, system maintenance manual

The system maintenance manual ***SHALL*** provide information in sufficient detail to support election workers, information systems personnel, or maintenance personnel in the adjustment or removal and replacement of components or modules in the field.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Technical documentation needed solely to support the repair of defective components or modules ordinarily done by the manufacturer or software developer is not required.

*Source:* *[2] II.2.9.*

*Impact:* *Click here to add the Impact*

➞ **4.5-B** Maintenance manual, general contents

The vendor ***SHALL*** describe service actions recommended to correct malfunctions or problems, personnel and expertise required to repair and maintain the system and equipment, and materials, and facilities needed for proper maintenance.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] II.2.9.*

*Impact:* *Click here to add the Impact*

## 4.5.1 Introduction

→ **4.5.1-A** Maintenance manual, equipment overview, maintenance viewpoint

The vendor ***SHALL*** describe the structure and function of the equipment and related software/firmware for election preparation, programming, vote recording, tabulation, and reporting in sufficient detail to provide an overview of the system for maintenance and for identification of faulty hardware or software.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] II.2.9.1.*

*Impact:* *Click here to add the Impact*

↳ **4.5.1-A.1** Maintenance manual, equipment overview details

The description ***SHALL*** include a concept of operations that fully describes such items as:

1. The electrical and mechanical functions of the equipment;
2. How the processes of ballot handling and reading are performed (paper-based systems);
3. For electronic vote-capture devices, how vote selection and casting of the ballot are performed;
4. How transmission of data over a network is performed (if applicable);
5. How data are handled in the processor and memory units;
6. How data output is initiated and controlled;
7. How power is converted or conditioned; and
8. How test and diagnostic information is acquired and used.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.9.1.*

*Impact:* *Click here to add the Impact*

## 4.5.2 Maintenance procedures

→ **4.5.2-A** Maintenance manual, maintenance procedures

The vendor ***SHALL*** describe preventive and corrective maintenance procedures for hardware, firmware and software.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.9.2.*

*Impact:* *Click here to add the Impact*

### 4.5.2.1 Preventive maintenance procedures

→ **4.5.2.1-A** Maintenance manual, preventive maintenance procedures

The vendor ***SHALL*** identify and describe:

1. All required and recommended preventive maintenance tasks, including software and data backup, database performance analysis, and database tuning;
2. Number and skill levels of personnel required for each task;
3. Parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance; and
4. Any maintenance tasks that must be coordinated with the vendor or a third party (such as coordination that may be needed for COTS used in the system).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.9.2.1.*

*Impact:* *Click here to add the Impact*

### 4.5.2.2 Corrective maintenance procedures

→ **4.5.2.2-A** Maintenance manual, troubleshooting procedures

The vendor ***SHALL*** provide fault detection, fault isolation, correction procedures, and logic diagrams for all operational abnormalities identified by design analysis and operating experience.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.9.2.2.*

*Impact:* *Click here to add the Impact*

→ **4.5.2.2-B** Maintenance manual, troubleshooting procedures details

The vendor ***SHALL*** identify specific procedures to be used in diagnosing and correcting problems in the system hardware, firmware and software. Descriptions ***SHALL*** include:

1. Steps to replace failed or deficient equipment;
2. Steps to correct deficiencies or faulty operations in software or firmware;
3. Modifications that are necessary to coordinate any modified or upgraded software or firmware with other modules;
4. The number and skill levels of personnel needed to accomplish each procedure;
5. Special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure; and
6. Any coordination required with the vendor, or other party, for COTS.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.9.2.2.*

*Impact:* *Click here to add the Impact*

## 4.5.3 Maintenance equipment

**4.5.3-A** Maintenance manual, special equipment

The vendor ***SHALL*** identify and describe any special purpose test or maintenance equipment recommended for fault isolation and diagnostic purposes.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.9.3.*

*Impact:* *Click here to add the Impact*

## 4.5.4 Parts and materials

**4.5.4-A** Maintenance manual, parts and materials

Vendors ***SHALL*** provide detailed documentation of parts and materials needed to operate and maintain the system.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.9.4.*

*Impact:* *Click here to add the Impact*

### 4.5.4.1 Common standards

**4.5.4.1-A** Maintenance manual, approved parts list

The vendor ***SHALL*** provide a complete list of approved parts and materials needed for maintenance. This list ***SHALL*** contain sufficient descriptive information to identify all parts by:

1. Type;

2. Size;
3. Value or range;
4. Manufacturer's designation;
5. Individual quantities needed; and
6. Sources from which they may be obtained.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.3.4.1.b, II.2.9.4.1.*

*Impact:* *Click here to add the Impact*

### 4.5.4.2 Paper-based systems

→ **4.5.4.2-A** Maintenance manual, parts and materials, marking devices

The user documentation ***SHALL*** identify specific marking devices that, if used to make the prescribed form of mark, produce readable marked ballots so that the system meets the performance requirements for accuracy.

*Applies to:* *Optical scanner*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Includes pens and pencils for MCOS or the appropriate EBM for ECOS.

*Source:* *Simplified from [2] I.3.2.4.2.3.*

*Impact:* *Deleted requirement to specify performance characteristics of marking devices because the certification only covers the ones used in testing.*

↳ **4.5.4.2-A.1** Maintenance manual, marking devices, approved vendors

For marking devices manufactured by multiple external sources, the vendor ***SHALL*** specify a listing of sources and model numbers that satisfy these requirements.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.3.2.4.2.3.c and II.2.9.4.2.*

*Impact:* *Click here to add the Impact*

➞ **4.5.4.2-B** Maintenance manual, ballot stock specification

The user documentation ***SHALL*** specify the required paper stock, weight, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of vote response fields and to identify unique ballot styles, placement of alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system.

*Applies to:* *Paper-based device*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.1.3.1.c, I.3.2.4.2.1.c, II.2.9.4.2.*

*Impact:* *Click here to add the Impact*

➞ **4.5.4.2-C** Maintenance manual, ballot stock specification criteria

User documentation for optical scanners ***SHALL*** include specifications for ballot materials to ensure that vote selections are read from only a single ballot at a time, without bleed-through or transferal of marks from one ballot to another.

*Applies to:* *Optical scanner*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.1.3.2, revised.*

*Impact:* *Click here to add the Impact*

→ **4.5.4.2-D** Maintenance manual, printer paper specification

User documentation for voting systems that include printers ***SHALL*** include specifications of the paper necessary to ensure correct operation, minimize jamming, and satisfy Requirement III.5.4.4-B and Requirement III.5.5.1-A.

*Applies to:* *Voting system*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

This requirement covers all printers, either stand-alone or integrated with another device, regardless whether they are used for reporting, for logging, for VVPR, etc.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

## 4.5.5 Maintenance facilities and support

→ **4.5.5-A** Maintenance manual, maintenance environment

The vendor ***SHALL*** identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.9.5.*

*Impact:* *Click here to add the Impact*

→ **4.5.5-B** Maintenance manual, maintenance support and spares

Vendors ***SHALL*** specify:

1. Recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation;
2. Recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation; and
3. Organizational affiliation (i.e., jurisdiction, vendor) of qualified maintenance personnel.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.3.4.5, II.2.9.5.*

*Impact:* *Removed references to availability.*

### 4.5.6 Appendices

The vendor may provide descriptive material and data supplementing the various sections of the body of the system maintenance manual. The content and arrangement of appendices are at the discretion of the vendor. Topics recommended for amplification or treatment in appendix include:

8. **Glossary:** A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer maintenance;
9. **References:** A list of references to all vendor documents and other sources related to maintenance of the system;
10. **Detailed Examples:** Detailed scenarios that outline correct system responses to every conceivable faulty operator input; alternative procedures may be specified depending on the system state; and
11. **Maintenance and Security Procedures:** Technical illustrations and schematic representations of electronic circuits unique to the system.

## 4.6 Personnel Deployment and Training Requirements

➔ **4.6-A** User docs, training manual

The vendor ***SHALL*** describe the personnel resources and training required for a jurisdiction to operate and maintain the system.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] II.2.10.*

*Impact:* *Click here to add the Impact*

## 4.6.1 Personnel

→ **4.6.1-A** Training manual, personnel

The vendor ***SHALL*** specify the number of personnel and skill levels required to perform each of the following functions:

1. Pre-election or election preparation functions (e.g., entering an election, contest and candidate information; designing a ballot; generating pre-election reports);
2. System operations for voting system functions performed at the polling place;
3. System operations for voting system functions performed at the central count facility;
4. Preventive maintenance tasks;
5. Diagnosis of faulty hardware, firmware or software;
6. Corrective maintenance tasks; and
7. Testing to verify the correction of problems.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.10.1.*

*Impact:* *Click here to add the Impact*

→ **4.6.1-B** Training manual, user functions versus vendor functions

The vendor ***SHALL*** distinguish which functions may be carried out by user personnel and which must be performed by vendor personnel.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.10.1.*

*Impact:* *Click here to add the Impact*

## 4.6.2 Training

**4.6.2-A** Training manual, training requirements

The vendor ***SHALL*** specify requirements for the orientation and training of administrators, central election officials, election judges, and poll workers.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Volume V Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.2.10.2.*

*Impact:* *Deleted "vendor personnel" from list, harmonized with newly defined roles.*

# Chapter 5: Certification Test Plan (test lab)

This chapter defines required content for the National Certification Test Plan, which is to be prepared by the test lab. It does not specify an overall organization for the test plan, nor does it enumerate all of the content that would be reasonable and customary for a test lab to include. Test labs are encouraged to apply relevant external standards, such as [39] and [40] or their logical successors, to determine the organization and content of test plans, provided that the information described in this chapter does appear in the result.

The purpose of the test plan is to document the test lab's development of the complete or partial certification test suite. To some extent, the test plan is determined by the Testing Standard (Volume V). To the extent that it is not, the test plan must document the test suite so that the results of certification testing are reproducible.

Prior to development of any test plan, the test lab must obtain the Technical Data Package (TDP) from the vendor submitting the voting system for certification. The TDP contains information necessary to the development of the test plan, such as the vendor's hardware specifications, application logic specifications, operating manual and maintenance manual.

## 5.1 Requirements

→ **5.1-A** Test plan references

The test lab ***SHALL*** list all documents that contain material used in preparing the test plan.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[6] II.A.1.1*

*Impact:* *Click here to add the Impact*

➞ **5.1-B** Test plan, implementation statement

The test lab ***SHALL*** include a copy of the implementation statement provided by the vendor.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Revision of [6] II.A.1.*

*Impact:* *Informal system identification replaced with implementation statement.*

↳ **5.1-B.1** Test plan, clarifications to implementation statement

The test lab ***SHALL*** document any interpretations made by the test lab to fully identify the implementation under test and the scope of certification that is desired.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **5.1-C** Test plan, inventory of materials delivered

The test lab ***SHALL*** enumerate the materials delivered by the vendor to the test lab to enable certification testing to occur.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Materials include hardware, software, the TDP, evidence of prior certifications, test ballots, test data, etc.

*Source:* *[6] II.A.3*

*Impact:* *Click here to add the Impact*

↳ **5.1-C.1** Test plan, specificity of inventory

Where applicable, materials ***SHALL*** be identified by specific version, serial number, etc., and the quantity of each ***SHALL*** be noted.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **5.1-D** Test plan, previous work

The test lab ***SHALL*** document all prior certifications, reviews, tests, or other conditions that impact the test lab's determination of the scope of certification testing, and document what that impact was.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The test lab may recognize certifications, reviews, and tests conducted by other labs, whether they are accredited for voting system certification testing or not, as making some portions of the voting system test campaign redundant. For example, a COTS computer should already have been certified to comply with the Rules and Regulations of the Federal Communications Commission, Part 15, Subpart B requirements for both radiated and conducted emissions and need not be retested for that. Also, if a slightly modified system is submitted for recertification, the test lab's finding that some or all of the test campaign need not be repeated would be documented under this requirement.

Sometimes new systems use a combination of new devices interfaced with the devices of a previously certified system. For example, a vendor can submit a voting system for certification testing that has a new DRE voting device, but that integrates the election management subsystem from a previously certified system. In this situation the accredited test lab may design and perform a test procedure that draws on the results of testing performed previously on reused subsystems. However, irrespective of previous testing performed, the scope of testing is expected to cover:

12. All functionality performed by new devices;
13. All functionality performed by modified devices;
14. Functionality that is accomplished using any interfaces to new devices, or that shares inputs or outputs from new devices;
15. All functionality related to vote tabulation and election results reporting; and
16. All functionality related to audit trail maintenance.

*Source:* *[6] II.3.2.4, II.A.2, II.B.1.2.*

*Impact:* *Click here to add the Impact*

➞ **5.1-E** Test plan, reproducible testing

The test lab ***SHALL*** provide the complete information needed to reproduce the testing that it performs, including facility requirements, test set-up, test sequence, test operations procedures, data recording requirements and pass criteria.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Condensed from [6] II.A.5 and 6.*

*Impact:* *Click here to add the Impact*

↳ **5.1-E.1** Test plan, standard test suites

For applicable test cases that are specified in Volume V, the test lab ***SHALL*** document the implementation details that determine how the standard test cases are realized for the implementation under test.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

↳ **5.1-E.2** Test plan, public test suites

For test cases that the test lab is adopting from publicly available test suites, the test lab ***SHALL*** identify the public reference and document the implementation details that determine how the public test cases are realized for the implementation under test.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

↳ **5.1-E.3** Test plan, other test suites

For all other test cases, the test lab ***SHALL*** incorporate all relevant information into the test plan as needed to reproduce the testing.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

➞ **5.1-F** Test plan, responsible parties

The test lab ***SHALL*** identify the parties responsible for conducting the conformity assessment, including subcontracted test labs and engineers assigned to the task.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[7]*

*Impact:* *Click here to add the Impact*

# Chapter 6: Test Report for Certification Authority (test lab)

## 6.1 Requirements

→ **6.1-A** Test report, include revision history

For modifications to previously certified systems, the test lab ***SHALL*** include the test reports that are precedential to the current evaluation.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

It is anticipated that the test report will be delivered in electronic form, so the volume of data should not be a problem.

*Source:* *[7] as clarified 2006-07-20.*

*Impact:* *Click here to add the Impact*

→ **6.1-B** Test report, include test plan as amended

The test lab ***SHALL*** include a copy of the test plan, amended to reflect any changes that were allowed during the course of the testing campaign.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

[10] 4.5.1 states: "Any changes to a voting system, initiated as a result of the testing process, will require submission of an updated Implementation Statement, functional diagram, and System Overview document and, potentially, an updated test plan. Test plans must be updated whenever a change to a voting system requires deviation from the test plan originally approved by the EAC. Changes requiring alteration or deviation from the originally approved test plan must be submitted to the EAC (by the VSTL) for approval before the completion of testing. [...] Changes not affecting the test plan **SHALL** be reported in the test report."

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **6.1-C** Test report, implementation statement as amended

The test lab ***SHALL*** include the implementation statement submitted by the vendor, amended to reflect any changes that were allowed during the course of the testing campaign.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

See [10] 4.5.1 (quoted in discussion of Requirement IV.5.1-B). Because minor defects in a system may be corrected during the course of the testing campaign, the system that is forwarded for certification might not be identical to the one for which an implementation statement was submitted. The product identification for the revised system must be different. Also, if a system fails a test for a particular voting variation, the vendor and test lab may agree to eliminate that voting variation from the list of classes to which certification is desired rather than correct the system.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **6.1-D** Test report, witness build

The test lab ***SHALL*** include a copy of the record of the final (witnessed) build and sufficient description of the build process to reproduce it.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

See Volume V Section 2.7.1.

*Source:* *[7]*

*Impact:* *Click here to add the Impact*

→ **6.1-E** Test report, setup validation info

The test lab ***SHALL*** identify the repository for software reference information and include the unique identifier assigned to the software reference information by the repository.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

See Ch. 5 of [10].

*Source:* *[7]*

*Impact:* *Click here to add the Impact*

→ **6.1-F** Test report, summary finding

The test lab ***SHALL*** include a summary finding of whether or not the implementation under test satisfies all applicable, mandatory ("***SHALL***") requirements of the Voluntary Voting System Guidelines.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **6.1-G** Test report, reasons for adverse opinion

If the test lab finds that the implementation under test does not satisfy all applicable, mandatory ("***SHALL***") requirements of the Voluntary Voting System Guidelines, the test lab ***SHALL*** identify each of the specific requirements that is not satisfied.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **6.1-H** Test report, evidence supporting adverse opinion

For each unsatisfied mandatory requirement, the test lab ***SHALL*** describe the inspections or tests that detected the nonconformities and include applicable evidence (e.g., vote data report, citation of logic error in source code).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **6.1-I** Test report, anomalies

The test lab ***SHALL*** summarize all failures, errors, nonconformities and anomalies that were observed during conformity assessment, no matter how minor.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

[10] 4.5.2 clarifies: "All test failures, anomalies and actions taken to resolve such failures and anomalies **SHALL** be documented by the VSTL in an appendix to the test report submitted to the EAC. These matters **SHALL** be reported in a matrix, or similar format, that identifies the failure or anomaly, the applicable voting system standards, and a description of how the failure or anomaly was resolved. Associated or similar anomalies/failures may be summarized and reported in a single entry on the report (matrix) as long as the nature and scope of the anomaly/failure is clearly identified."

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **6.1-I.1** Test report, deficiencies corrected during test campaign

The test lab ***SHALL*** identify those deficiencies that were corrected during the course of the testing campaign and identify the inspections or tests that confirm that the deficiencies were corrected.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

For minor defects of a localized nature, the test lab may permit the vendor to correct the fault without incurring a complete regression test of the system. However, [10] requires that revised documents be submitted to the EAC when changes are made. See [10] 4.5.1 (quoted in discussion of Requirement IV.5.1-B).

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **6.1-J** Test report, benchmarks

For requirements that specify benchmarks, the test lab ***SHALL*** report the result of the measurement for the implementation under test.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **6.1-J.1** Test report, failure rate

This ***SHALL*** include the observed cumulative failure rate and the failure rate that was demonstrated with 90 % confidence for each type of device, for each applicable failure type in Table 6 (Volume III Section 5.3.1.5).

*Applies to:* *Voting device*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

See also Volume V Section 5.3.2.

"Type of device" refers to the different models produced by the vendor. These are not the same as device classes. The system may include several different models of the same class, and a given model may belong to more than one class.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **6.1-J.2** Test report, error rate

This ***SHALL*** include the observed cumulative report total error rate and the report total error rate that was demonstrated with 90 % confidence for the system as a whole.

*Applies to:* *Voting system*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

See Volume V Section 5.3.3.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **6.1-J.3** Test report, misfeed rate

For paper-based tabulators, this ***SHALL*** include the observed cumulative misfeed rate and the misfeed rate that was demonstrated with 90 % confidence for each type of device.

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

See Volume V Section 5.3.4.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **6.1-K** Test report, ballot tabulation rate

For paper-based tabulators, the test lab ***SHALL*** report the ballot tabulation rate used in typical case and capacity tests.

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **6.1-L** Test report, shoulds that were not done

The test lab ***SHALL*** identify each applicable, non-mandatory ("should") requirement to which nonconformity was demonstrated.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Some requirements are "shoulds" instead of "**SHALL**s" specifically because there is no known method of demonstrating conformity; thus, the test lab is not expected to test every "should." However, those "shoulds" that are shown to be unsatisfied must be reported.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **6.1-M** Test report, waived tests

The test lab ***SHALL*** identify all tests for which the verdict was Waived.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

A test case is waived if the documented assumptions of an applicable test case are not met by the implementation under test. A test that pertains to a system or device class that was not claimed in the implementation statement is implicitly assigned the verdict Not Applicable.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **6.1-N** Test report, timeline

The test lab ***SHALL*** include a timeline of the testing campaign as it actually occurred.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **6.1-O** Test report, compensatory procedures

The test lab ***SHALL*** list any specific election management practices that are required for the voting system to satisfy the requirements of the VVSG.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

For example, if additional procedures must be followed in order to safeguard the secrecy of the vote, these must be documented. Where possible, additional procedures should be specified by reference to EAC Election Management Guidelines.

If a system requires unusually onerous procedural compensations because customary system safeguards are absent, this may impact the certification decision.

*Source:* *[7]*

*Impact:* *Click here to add the Impact*

➞ **6.1-P** Test report, warrant of accepting change control responsibility

If any changes to the system are required to attain certification, the test lab ***SHALL*** include a signed warrant from the vendor that those changes will be included in the product that is delivered to customers.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[7] as clarified 2006-07-20.*

*Impact:* *Click here to add the Impact*

➜ **6.1-Q** Test report, issues list

The test lab ***SHALL*** list and explain any concerns that should be brought to the attention of the certification authority.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

A formal process for requesting interpretations is provided in Ch. 9 of [10]. Any unresolved concerns may be documented in the test report. "Concerns" would include ambiguities in the Guidelines, interpretation conflicts, requirements that appear to do more harm than good, loopholes in the Guidelines (where it is possible to satisfy the technical requirements while failing to satisfy their intent), and other issues whose resolution would require action by the certification authority and/or standards maintenance.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

# Chapter 7: Public Information Package (test lab)

## 7.1 Requirements

➞ **7.1-A** Public Information Package (PIP)

The test lab ***SHALL*** provide the certification authority with a Public Information Package.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **7.1-A.1** PIP, application package

The PIP ***SHALL*** include a copy of the vendor's application package.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The application package is defined in [10] 4.3.2 and includes the application form (with identification and description of the system), the implementation statement (redundant), and the functional diagram and system overview from the TDP.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **7.1-A.2** PIP, test report

The PIP ***SHALL*** satisfy the requirements for the Test Report (all requirements in Volume IV Chapter 5).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The same minimal requirements apply to the PIP as apply to the test report, and the same minimal requirements apply to the test plan contained in the PIP as apply to the test plan contained in the test report. The difference is that the test report for the certification authority may contain additional, vendor-proprietary information that would not be suitable for publication.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

5

# Draft VVSG Recommendations to the EAC

## May 2007 DRAFT

**VOLUME 5:**

**TESTING STANDARD**

TESTING METHODS OVERVIEWS

# Volume 5 Table of Contents

# Volume 5: Testing Standard

# Chapter 1: Introduction

## 1.1 Scope and Applicability

This part of the Voluntary Voting System Guidelines, the Testing Standard, contains requirements applying to the national certification testing to be conducted by test labs.

## 1.2 Audience

The Voluntary Voting System Guidelines are intended primarily for use by:

- Designers and manufacturers of voting systems;
- Test labs performing the analysis and testing of voting systems in support of the national certification process;
- Software repositories designated by the national certification authority or by a state; and
- Test labs and consultants performing the state certification of voting systems.

This part of the Voluntary Voting System Guidelines, the Testing Standard, is intended primarily for use by test labs.

# Chapter 2: Conformity Assessment Process

## 2.1 Overview

Certification testing encompasses the examination and testing of software and firmware; tests of hardware under conditions simulating the intended storage, operation, transportation, and maintenance environments; inspection and evaluation of system documentation; and operational tests to validate system performance and functioning under normal and abnormal conditions. The testing also evaluates the completeness of the vendor's developmental test program, including the sufficiency of vendor tests conducted to demonstrate compliance with stated system design and performance specifications, and the vendor's documented quality assurance and configuration management practices. The tests address individual system components or elements as well as the integrated system as a whole.

Beginning in 1994, the National Association of State Election Directors (NASED) began accrediting Independent Test Authorities for the purpose of conducting qualification testing of voting systems. The qualification testing process was originally based on the 1990 voting system standards and evolved to encompass the new requirements contained in the 2002 version of the standards.

The Help America Vote Act (HAVA) directs the U.S. Election Assistance Commission (EAC) to provide for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories. HAVA also introduces different terminology for these functions. Under the EAC process, test labs are "accredited" and voting systems are "certified." The term "standards" has been replaced with the term "Guidelines."

The certification test process may be performed by one or more accredited test labs that together perform the full scope of tests required. Testing may be coordinated across accredited test labs so that equipment and materials tested by one accredited test lab can be used in the tests performed by another accredited test lab.

When multiple accredited test labs are being used, the development of the test plan (see Volume IV Chapter 4) and the test report (see Volume IV Chapter 5) must be coordinated by a lead accredited test lab. The lead lab is responsible for ensuring that all testing has been performed and documented in accordance with the Guidelines and is ultimately responsible for the summary finding of conformance (see Requirement IV.5.1-F).

Whether one or more accredited test labs are used, the testing generally consists of three phases:

- Pre-test activities;
- Certification testing; and
- Post-test activities.

## 2.2 Rules of Engagement

The rights and responsibilities of each party to the certification testing process are specified in [10].

## 2.3 Scope of Assessment

The national certification testing process is intended to discover vulnerabilities that, should they appear in actual election use, could result in failure to complete election operations in a satisfactory manner. This involves

- Operational accuracy in the recording and processing of voting data, as measured by report total error rate;
- Operational failures or the number of unrecoverable failures under conditions simulating the intended storage, operation, transportation, and maintenance environments for voting systems;
- System performance and function under normal and abnormal conditions; and
- Completeness and accuracy of the system documentation and configuration management records to enable purchasing jurisdictions to effectively install, test, and operate the system.

Conformity assessment involves several different kinds of testing, including

- Inspections, where the conformity of the voting system and vendor practices for configuration management and quality assurance are evaluated via expert review;
- Hardware testing, where the ability of the system to tolerate the physical conditions of its operation, transportation and storage is evaluated;
- Functional testing, where the conformity of the voting system's observable behaviors is evaluated;
- Performance testing, where the satisfaction of specified benchmarks is either evaluated in specific tests or monitored concurrent with other testing;
- Usability testing, where the performance is evaluated with human test subjects; and
- Vulnerability testing, where the system's resistance to attack is evaluated.

In practice, the nonconformities observed during a particular testing phase do not necessarily relate to the focus of that phase of testing. For example, the test scenarios employed during usability testing may trigger systematic failures that

demonstrate that the system reliability benchmark has not been satisfied. A demonstrable violation of any applicable requirement of the VVSG during the execution of any test case results in a failure verdict, regardless of whether the nonconformity relates to the focus of the test (see Requirement V.5.2.1.2-D).

Voting system hardware, software, communications and documentation are examined and tested to determine suitability for elections use. Examination and testing address the broad range of system functionality and components, including system functionality for pre-voting, voting, and post-voting functions. All products for election use are tested in accordance with the applicable procedures.

Certification tests are conducted for new systems seeking initial certification as well as for modified versions of systems that have been certified.

Not all systems are required to complete every category of testing. Consistent with Requirement IV.4.1-D, the test lab may find that proven performance of COTS hardware, software and communications components in commercial applications other than elections obviates the need for certain specific evaluations. However, as most functional testing exercises the complete system, COTS components are always tested together with other components of the voting system. Similarly, if a previous version of the same system has been certified, the test lab may find that complete retesting would be redundant, but some tests that exercise the entire system are always conducted. The background and rationale for these decisions regarding the scope of testing must be documented in the test plan, which must be approved by the certification authority.

The accredited test lab determines which tests are necessary to recertify a modified system based on a review of the nature and scope of changes and other submitted information including the system documentation, vendor test documentation, configuration management records, and quality assurance information. The accredited test lab may determine that a modified system is subject only to limited certification testing if the vendor demonstrates that the change does not affect demonstrated compliance with these Guidelines for:

1. Performance of voting system functions;
2. Voting system security and privacy;
3. Overall flow of system control; and
4. The manner in which ballots are defined and interpreted, or voting data are processed.

Limited testing is intended to facilitate the correction of defects, the incorporation of improvements, the enhancement of portability and flexibility, and the integration of vote counting software with other systems and election software.

In all cases, the system documentation and configuration management records are examined to confirm that they completely and accurately reflect the components and component versions that comprise the voting system.

## 2.4 Testing Sequence

Tests and inspections required by these guidelines need not be conducted in any particular order. Test labs should organize the test campaign to maximize overall testing effectiveness, to test in as efficient a manner as possible, and to minimize the amount of regression testing that is incurred when nonconformities are found and corrected. Test anomalies and errors are communicated to the system vendor throughout the process.

## 2.5 Pre-Test Activities

Pre-test activities include the request for initiation of testing and the pre-test preparation.

### 2.5.1 Initiation of testing

Certification testing is conducted at the request of the vendor. The vendor must:

1. Request the performance of certification testing from among the accredited testing laboratories;
2. Enter into formal agreement with the accredited test lab for the performance of testing; and
3. Prepare and submit materials required for testing consistent with the requirements of the Guidelines.

Certification testing is conducted for the initial version of a voting system as well as for all subsequent revisions to the system that are to be used in elections. As described in Volume V Section 2.3, the nature and scope of testing for system changes or new versions is determined by the accredited test lab based on the nature and scope of the modifications to the system and on the quality of system documentation and configuration management records submitted by the vendor.

Specific details of when certification testing is required and the process for initiating certification testing are found in Ch. 3, "When Voting Systems Must Be Submitted for Testing and Certification," and Ch. 4, "Certification Testing and Technical Review," of [10].

### 2.5.2 Pre-test preparation

Pre-test preparation encompasses the following activities:

1. The vendor and accredited test lab enter into an agreement for the testing to be performed by the accredited test lab.
2. The vendor prepares and submits a TDP to the accredited test lab. The TDP consists of the materials described in Volume IV Chapter 2.

3. The accredited test lab performs an initial review of the TDP for completeness and clarity and requests additional information as required.
4. The vendor provides additional information if requested by the accredited test lab.
5. The test lab witnesses the production of the implementation for testing.
6. The vendor delivers to the accredited test lab all hardware and software needed to perform testing.

### 2.5.2.1 Documentation submitted by vendor

→ **2.5.2.1-A** Submit Technical Data Package

The vendor ***SHALL*** submit to the test lab a Technical Data Package conforming to the requirements of Volume IV Chapter 2.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

The vendor must submit all the documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the accredited test lab for conducting system certification testing. This documentation collectively is referred to as the Technical Data Package (TDP). The TDP provides information that defines the voting system's design, method of operation, and related resources. It provides a system overview and documents the system's functionality, hardware, software, security, test and verification specifications, operations procedures, maintenance procedures, and personnel deployment and training requirements. It also documents the vendor's configuration management plan and quality assurance program. If another version of the system was previously certified, the TDP would also include appropriate system change notes.

*Source:* *[6] II.1.5*

*Impact:* *Click here to add the Impact*

### 2.5.2.2 Voting equipment submitted by vendor

Vendors may seek to market a complete voting system or an interoperable component of a voting system. In all instances, vendors must submit for testing the specific system configuration that will be offered to jurisdictions or that comprises the component to be marketed plus the other components with which the component is to be used. Under no circumstances will a component be certified except as part of a complete voting system, and that certification is valid only when that component is used with that same system (see Volume III Section 2.4).

→ **2.5.2.2-A** Submit system without COTS

If needed for compliance with Dangling ref: PleaseAddReference_STS_TestLabIntegrateCOTS, the vendor ***SHALL*** supply the system with the COTS components omitted, for subsequent integration performed by or witnessed by the test lab.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

See Dangling ref: PleaseAddReference_STS_TestLabIntegrateCOTS.

*Source:* *COTS verification process per STS and CRT consensus, June 2006.*

*Impact:* *Click here to add the Impact*

→ **2.5.2.2-B** Hardware equivalent to production version

The hardware submitted for certification testing ***SHALL*** be equivalent, in form and function, to the actual production version of the hardware units specified for use in the TDP.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[6] II.1.6.a*

*Impact:* *Click here to add the Impact*

→ **2.5.2.2-C** Logic equivalent to production version

The firmware and software submitted for certification testing ***SHALL*** be the exact firmware and software that will be used in production units.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[6] II.1.6.b*

*Impact:* *Click here to add the Impact*

➞ **2.5.2.2-D** No prototypes

Developmental prototypes ***SHALL*** not be submitted unless the vendor can show that the equipment to be tested is equivalent to standard production units both in performance and construction.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[6] II.1.6.c*

*Impact:* *Click here to add the Impact*

➞ **2.5.2.2-E** Benchmark directory listings

Benchmark directory listings ***SHALL*** be submitted for all software/firmware elements (and associated documentation) included in the vendor's release as they would normally be installed upon setup and installation.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[6] II.1.6.d*

*Impact:* *Click here to add the Impact*

### 2.5.2.3 Witness of initial system build

This section is to be provided by STS.

## 2.6 Certification Testing

Certification testing encompasses the preparation of a test plan, the establishment of the appropriate test conditions, the use of appropriate test fixtures, the witness of the system build and installation, the maintenance of certification test data, and the evaluation of the data resulting from tests and examinations.

## 2.6.1 Certification test plan

→ **2.6.1-A** Prepare test plan

The accredited test lab ***SHALL*** prepare a test plan to define all tests and procedures required to demonstrate compliance with the Guidelines, including:

1. Verifying or checking equipment operational status by means of manufacturer operating procedures;
2. Establishing the test environment or the special environment required to perform each test;
3. Initiating and completing operating modes or conditions necessary to evaluate the specific performance characteristics under test;
4. Measuring and recording the value or range of values for the characteristics to be tested, demonstrating expected performance levels;
5. Verifying, as above, that the equipment is still in normal condition and status after all required measurements have been obtained;
6. Confirming that documentation submitted by the vendor corresponds to the actual configuration and operation of the system; and
7. Confirming that documented vendor practices for quality assurance and configuration management comply with the Guidelines.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Requirements on the content of the test plan are contained in Volume IV Chapter 4.

*Source:* *[6] II.1.8.2.1*

*Impact:* *Click here to add the Impact*

## 2.6.2 Certification test conditions

The accredited test lab may perform the tests in any facility capable of supporting the test environment.

→ **2.6.2-A** Witness test preparation

Preparations for testing, arrangement of equipment, verification of equipment status, and the execution of procedures ***SHALL*** be witnessed by at least one independent, qualified observer, who ***SHALL*** certify that all test and data acquisition requirements have been satisfied.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.9.6.2.2.a*

*Impact:* *[6] II.1.8.2.2.a said "at least one independent, qualified observer in the form of an accredited testing laboratory," which seems to suggest that the lab could "witness" itself.*

➞ **2.6.2-B** Ambient conditions

When a test is to be performed at "standard" or "ambient" conditions, this ***SHALL*** refer to a nominal laboratory or office environment with a temperature in the range of 20.0 °C to 23.9 °C (68 °F to 75 °F) and prevailing atmospheric pressure and relative humidity.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[6] II.1.8.2.2.b*

*Impact:* *Click here to add the Impact*

➞ **2.6.2-C** Tolerances for specified temperatures and voltages

Otherwise, the test ***SHALL*** be performed at the required temperature and electrical supply voltage, regulated within the following tolerances:

1. Temperature ± 2.2 °C (± 4 °F)
2. AC electrical supply voltage ± 2 V

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[6] II.1.8.2.2.c*

*Impact:* *Click here to add the Impact*

## 2.6.3 Certification test fixtures

→ **2.6.3-A** Complete system testing

Except as provided in Requirement V.2.6.3-B, the test lab ***SHALL*** not use simulation devices or software that bypass portions of the voting system that would be exercised in an actual election.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Devices or software that closely and validly simulate actual election use of the system are permissible.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **2.6.3-B** Exceptions to complete system testing

The test lab may bypass the user interface of an interactive device in the case of environmental tests that

1. Would require subjecting test "voters" to unsafe or unhealthy conditions; or
2. Would be invalidated by the presence of a test "voter."

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

## 2.6.4 Certification test data requirements

→ **2.6.4-A** Test log

A test log of the procedure ***SHALL*** be maintained. This log ***SHALL*** identify the system and equipment by model and serial number.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[6] II.1.8.2.5.a*

*Impact:* *Click here to add the Impact*

→ **2.6.4-B** Test environment conditions

Test environment conditions ***SHALL*** be noted.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[6] II.1.8.2.5.b*

*Impact:* *Click here to add the Impact*

→ **2.6.4-C** Items to be logged

All operating steps, the identity and quantity of simulated ballots, annotations of output reports, the elapsed time for each procedure step, observations of equipment performance and, in the case of non-operating hardware tests, the condition of the equipment ***SHALL*** be recorded.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[6] II.1.8.2.5.c*

*Impact:* *Click here to add the Impact*

## 2.6.5 Certification test practices

**2.6.5-A** Conduct all tests

The accredited test lab ***SHALL*** conduct the examinations and tests defined in the test plan to determine compliance with the voting system requirements described in Volume III and Volume IV.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[6] II.1.8.2.6*

*Impact:* *Click here to add the Impact*

**2.6.5-B** Log all anomalies

If any failure, malfunction or data error is detected, its occurrence and the duration of operating time preceding it ***SHALL*** be recorded for inclusion in the analysis of data obtained from the test.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[6] II.1.8.2.6.a*

*Impact:* *Click here to add the Impact*

**2.6.5-C** Critical software defects are unacceptable

If a logic defect is responsible for the incorrect recording, tabulation, or reporting of a vote, the test campaign ***SHALL*** be terminated and the system ***SHALL*** be rejected.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Conformity assessment is not quality assurance. If a critical software defect is found, the system cannot be considered trustworthy even after the known fault is corrected, because the cases that the test lab does not have the opportunity to test can be expected to conceal similar faults. Any subsequent testing of a system based on or derived from the rejected system requires a new application and starting over.

*Source:* *[1] 7.1.1, [2] Overview, [6] II.1.8.2.6.b.*

*Impact:* *Click here to add the Impact*

→ **2.6.5-D** Software defects are not field-serviceable

If a logic defect is found that is not responsible for the incorrect recording, tabulation, or reporting of a vote, the test campaign ***SHALL*** be suspended and the system returned to the vendor for correction and quality assurance.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Rejection may be a foregone conclusion if sufficient evidence has been collected to show that the reliability benchmark is not satisfied (see Volume V Section 5.3.2). Notwithstanding that, the vendor will be given the opportunity to correct noncritical software defects. Revisions to the software must be performed within the vendor's quality assurance and configuration management processes and must undergo vendor regression testing before the certification process is resumed. When it is resumed, the test plan should be revised to include regression testing for the change that was made.

*Source:* *[6] II.1.8.2.6.b, clarified and strengthened.*

*Impact:* *Click here to add the Impact*

→ **2.6.5-E** Hardware failures are field-serviceable

If the anomaly is other than a logic defect, and if corrective action is taken to restore the equipment to a fully operational condition within 8 hours, then the test campaign may be resumed at the point of suspension.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Rejection may be a foregone conclusion if sufficient evidence has been collected to show that the reliability benchmark is not satisfied (see Volume V Section 5.3.2). Notwithstanding that, the vendor may replace a component that has suffered a random failure, or the vendor may opt to suspend the test campaign in order to correct a hardware design defect that caused a nonrandom failure.

*Source:* *[6] II.1.8.2.6.c*

*Impact:* *Click here to add the Impact*

→ **2.6.5-F** Pauses in test campaign

If the test campaign is suspended for an extended period of time, the accredited test lab ***SHALL*** maintain a record of the procedures that have been satisfactorily completed. When testing is resumed at a later date, repetition of the successfully completed procedures may be waived provided that no design or manufacturing change has been made that would invalidate the earlier test results.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The considerations for resumption of testing are similar to those of Requirement IV.4.1-D.

*Source:* *[6] II.1.8.2.6.d*

*Impact:* *Click here to add the Impact*

→ **2.6.5-G** Resumption after deficiency

The test campaign may resume after a deficiency is found if:

1. The vendor submits a design, manufacturing, or packaging change notice to correct the deficiency, together with test data to verify the adequacy of the change;
2. The examiner of the equipment agrees that the proposed change is responsive to the full scope of the deficiency;
3. Any previously failed tests are passed by the revised system; and
4. The vendor certifies that the change will be incorporated into all existing and future production units.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Consistent with configuration management, the corrected system is formally a different system from the one that failed. The failure of the previous version is never "purged;" rather, a new revision of the system is found not to suffer the same defect

*Source:* *[6] II.1.8.2.6.e, clarified*

*Impact:* *Click here to add the Impact*

# 2.7 Post-Test Activities

## 2.7.1 Witness of final system build

To be written by STS / superseded by trusted build in Ch. 5 of [10].

## 2.7.2 Final test report

The accredited test lab may issue interim reports to the vendor, informing the vendor of the testing status, findings to date, and other information.

→ **2.7.2-A** Prepare test report

The accredited test lab ***SHALL*** prepare a test report conforming to the requirements of Volume IV Chapter 5.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[6] II.1.8.3.b*

*Impact:* *Click here to add the Impact*

→ **2.7.2-B** Consolidated test report

Where a system is tested by multiple accredited test labs, the lead accredited test lab ***SHALL*** prepare a consolidated test report.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[6] II.1.8.3.c*

*Impact:* *Click here to add the Impact*

→ **2.7.2-C** Test report delivery

The accredited test lab ***SHALL*** deliver the report to the vendor and to the certification authority.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[6] II.1.8.3.d*

*Impact:* *Click here to add the Impact*

Upon review and acceptance of the test report, the EAC issues a Certification Number for the system to the vendor and to the accredited test lab. The issuance of a Certification Number indicates that the system has been tested by the accredited test lab for compliance with the Guidelines. For details see Ch. 5 of [10].

The Certification Number applies to the system as a whole only for the configuration and versions of the system elements tested and identified in the National Certification Test Report. The Certification Number does not apply to individual system components or untested configurations. The EAC Certification Number is intended for use by the states and their jurisdictions to support state and jurisdiction processes concerning voting systems. States and their jurisdictions request National Certification Test Reports based on the EAC Certification Number to support their voting system certification and procurement processes.

## 2.8 Resolution of Testing Issues

Prior to the transition of this function to the EAC, the NASED Voting Systems Board (the Board) was responsible for resolving questions about the application of the Guidelines in the testing of voting systems. The EAC's process for accredited test labs and vendors to request an interpretation of the Guidelines is documented in Ch. 9 of [10]. Interpretations will be published for reference by interested parties. The EAC will periodically assess the interpretations to determine which topics should be reflected in a future version of the Guidelines.

# Chapter 3: Introduction to General Testing Approaches

## 3.1 Inspection

Inspection is the examination of a product design, product, process or installation and determination of its conformity with specific requirements or, on the basis of professional judgement, with general requirements. [37]

Inspection is indicated when there is no operational test for assessing conformity to a given requirement. Inspection can be as simple as a visual confirmation that a particular design element or function is present or review of documentation to ensure inclusion of specific content, or it can be as complex as formal evaluation by an accredited specialist.

Logic verification is an example of inspection. Although formal proofs can be checked automatically, the determination that the premises correctly describe the behavior of the system requires professional judgement.

## 3.2 Functional Testing

Functional testing is the determination through operational testing of whether the behavior of a system or device in specific scenarios conforms to requirements. Functional tests are derived by analyzing the requirements and the behaviors that should result from implementing those requirements. For example, one could determine through functional testing that a tabulator reports the correct totals for a specific simulated election day scenario.

Functional testing is indicated when the requirements on the behavior of a system or device are sufficiently precise and constraining that conformity can be objectively demonstrated.

Strategies for conducting functional testing are broadly characterized as either "black box" or "white box" (see Volume V Section 1.4.3.3). However, a given test is neither black-box nor white-box. That distinction pertains to the strategy by which applicable tests are developed and/or selected, not to the tests themselves. For example, if a given input is tested because it is a special case in the functional specification of the system, then it is black box testing; but if that same input is tested because it exercises an otherwise unused block of code found during the review of source code, then it is white box testing.

Functional testing can be performed using a test suite or it can be open-ended.

## 3.3 Performance Testing (Benchmarking)

Performance testing, a.k.a. benchmarking, is the measurement of a property of a system or device in specific scenarios. For example, one could determine through performance testing the amount of time that a tabulator takes to report its totals in a specific simulated election day scenario.

What distinguishes performance testing from functional testing is the form of the experimental result. A functional test yields a yes or no verdict, while a performance test yields a quantity. This quantity may subsequently be reduced to a yes or no verdict by comparison with a benchmark, but in the case of functional testing there is no such quantity to begin with. (E.g., there is no concept of "*x* % conforming" for the requirement to support 1-of-M voting. Either it is supported or it is not.)

Performance testing is indicated when the requirements supply a benchmark for a measurable property.

Usability testing is an example of performance testing. The property being measured in usability testing involves the behavior of human test subjects.

## 3.4 Vulnerability Testing

Vulnerability testing is an attempt to bypass or break the security of a system or a device. Like functional testing, vulnerability testing can falsify a general assertion (namely, that the system or device is secure) but it cannot verify the security (show that the system or device is secure in all cases). Vulnerability testing is also referred to as penetration testing. Vulnerability testing can be performed using a test suite or it can be open-ended. Vulnerability testing involves the testing of a system or device using the experience and expertise of the tester; using the knowledge of system or device design and implementation; using the publicly available knowledge base of vulnerabilities in the system or device; using the publicly available knowledge base of vulnerabilities in similar system or device; using the publicly available knowledge base of vulnerabilities in similar and related technologies; and using the publicly available knowledge base of vulnerabilities generally found in hardware and software (e.g., buffer overflow, memory leaks, etc.)

## 3.5 Interoperability Testing

Interoperability testing is the determination through operational testing of whether existing products are able to cooperate meaningfully for some purpose. It consists of bringing together existing products, configuring them to work together, and performing a functional test to determine whether the operation succeeds.

Conformance testing and interoperability testing are fundamentally different. Conformance testing focuses on the relationship of a given product to the standard; interoperability testing focuses on the practical cooperation of two or more products,

irrespective of any standard. Conformance to a standard is neither necessary nor sufficient to achieve interoperability.

Because interoperability testing focuses on practical cooperation, the use of test scaffolding is to be avoided. All of the components should be actual product.

# Chapter 4: Documentation and Design Reviews (Inspections)

An inspection or review is logically reported as one or more test cases with a verdict of Pass or Fail. The number of test cases reported corresponds to how the test lab chooses to structure the inspection.

To the extent possible, these Guidelines provide guidance on the criteria to be applied. However, the nature of some of these inspections is to rely on the professional judgement of an expert reviewer to assess conformity with general guidelines.

## 4.1 Initial Review of Documentation

The accredited test lab reviews the documentation submitted by the vendor for its completeness and satisfaction of requirements.

➔ **4.1-A** Initial review of documentation

At the beginning of inspection, the test lab ***SHALL*** verify that the documentation submitted by the vendor in the TDP meets all requirements applicable to the TDP, is sufficient to enable the inspections specified in this chapter and is sufficient to enable the tests specified in Volume V Chapter 5.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

This includes verifying that source code has been supplied compliant with Requirement IV.2.4.7.2-E.

*Source:* *[2]/[6] II.5.3, generalized.*

*Impact:* *Click here to add the Impact*

➔ **4.1-B** Review of COTS suppliers' specifications

For COTS components, such as printers and touchscreens, that were integrated into a voting device by the vendor, the test lab ***SHALL*** review the COTS manufacturers' specifications to verify that those manufacturers

approve of their products' use under the conditions specified by these Guidelines for voting systems.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

For example, if the operating and/or storage environmental conditions specified by the manufacturer of a printer do not meet or exceed the requirements of these Guidelines, a system that includes that printer is not certifiable.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

STS needs to add to this section. The documentation reviews in [6] II.6.4, Security Testing, would go here if not superseded by new STS text.

## 4.2 Physical Configuration Audit

The Physical Configuration Audit (PCA) is the formal examination of the as-built version of a voting system against its design documentation in order to establish the product baseline. After successful completion of the audit, subsequent changes are subject to test lab review and reexamination.

→ **4.2-A** As-built configuration reflected by records

The test lab ***SHALL*** audit the system's documentation and quality assurance records to verify that the as-built configuration is reflected by the documentation and records.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

This includes both hardware and logic (software, firmware, etc.).

*Source:* *[41] ¶80.1, [6] II.6.6*

*Impact:* *Click here to add the Impact*

→ **4.2-B** Check identity of previously certified devices

If a limited scope of testing is planned for a system containing previously certified devices or subsystems, the test lab ***SHALL*** verify that the affected devices or subsystems are identical to those previously certified.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] II.6.3.a / [6] II.6.3*

*Impact:* *Click here to add the Impact*

→ **4.2-C** Accuracy of system and device classification

The test lab ***SHALL*** verify that the classes claimed in the implementation statement accurately characterize the system and devices submitted for testing.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Any *Electronic device* that includes software or firmware installed or commissioned by the voting system vendor is a *Programmed device*. Vendors claiming that an electronic device is not programmed must demonstrate to the satisfaction of the testing and certifying authorities that the device contains no software or firmware that should be subject to the requirements indicated for programmed devices.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

→ **4.2-D** Validate configuration

The test lab ***SHALL*** confirm the propriety and correctness of the configuration choices described in Volume IV Section 2.10.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[2] I.4.1.1.*

*Impact:* *Click here to add the Impact*

## 4.3 Verification of Design Requirements

Many design requirements state simply that the system **SHALL** have some physical feature without any additional constraints. Such requirements are easily verified by inspection. Other requirements that state that the system **SHALL** prevent something from occurring are not verifiable through operational testing, so inspection (with expert judgment) is the only effective testing strategy.

→ **4.3-A** Verify design requirements

For each requirement of Volume III that is not amenable to operational testing, the test lab ***SHALL*** review the application logic, border logic, third-party logic, configuration data, and/or design of the voting system as needed to verify that the requirement is satisfied.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Following is a partial list of requirements that would need to be verified in this manner. HFP, STS: Add yours.

7. Requirement III.5.1-A
8. Requirement III.5.1-D
9. Requirement III.5.1-E
10. Requirement III.5.1-F
11. Requirement III.5.1-G
12. Requirement III.5.1-H
13. Requirement III.5.3.1-A
14. Requirement III.5.3.1-C
15. Requirement III.5.3.1-D
16. Requirement III.5.4.4-A
17. Requirement III.5.4.6-A
18. Requirement III.5.4.6-B
19. Requirement III.5.4.6-C

20. Requirement III.5.4.8-C
21. Requirement III.5.5.1-A12
22. Requirement III.5.6-A13
23. Requirement III.6.1-G
24. Requirement III.6.6.4-B
25. Requirement III.6.6.5-A
26. Requirement III.6.9.1-C

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

# 4.4 Vendor Practices for Quality Assurance and Configuration Management

## 4.4.1 Examination of Quality Assurance and Configuration Management Data Package

➔ **4.4.1-A** Quality and Configuration Management Manual

The Quality and Configuration Management Manual delivered as part of the Manufacturer Registration process ***SHALL*** be reviewed for its fulfillment of Volume III, Requirement 16.4.2.1-A, and the requirements specified in Volume IV, Section 2.2.1.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The review of the Manual would be in accordance with procedures and policies established in [10].

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

## 4.4.2 Examination of Voting Systems Submitted for Testing

These requirements deal with the quality assurance and configuration examination of voting systems submitted for testing to an accredited test lab.

### 4.4.2.1 Configuration Management

→ **4.4.2.1-A** Identification of Systems

The test lab ***SHALL*** verify that the voting system has an identification tag attached to the main body as described in Volume III, Requirement 16.4.2.2-A.1 and A.2.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

→ **4.4.2.1-B** Configuration Log

The test lab ***SHALL*** verify that the voting system has associated with it a Configuration Log, as described in Volume III, Requirement 16.4.2.2-B.1 and B.2.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *New requirement*

*Impact:* *Click here to add the Impact*

## 4.5 Accessibility

This section is to be provided by HFP.

## 4.6 Source Code Review

In the source code review, the accredited test lab will look at programming completeness, consistency, correctness, modifiability, structure, modularity and construction.

## 4.6.1 Workmanship

Although these requirements are scoped to application logic, in some cases the test lab may need to inspect border logic and third-party logic to assess conformity. Per Requirement IV.2.4.7.2-E, the source code for all of these must be provided.

→ **4.6.1-A** Review source versus vendor specifications

The test lab ***SHALL*** assess the extent to which the application logic adheres to the specifications made in its design documentation.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Since the nature of the requirements specified by the vendor is unknown, conformity may be subject to interpretation. Nevertheless, egregious disagreements between the application logic and its design documentation should lead to a defensible adverse finding.

*Source:* *[2] II.5.4.*

*Impact:* *Click here to add the Impact*

→ **4.6.1-B** Review source versus coding conventions

The test lab ***SHALL*** assess the extent to which the application logic adheres to the published, credible coding conventions chosen by the vendor.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

See Requirement III.5.4.1.3-A.

Since the nature of the requirements specified by the coding conventions is unknown, conformity may be subject to interpretation. Nevertheless, egregious disagreements between the application logic and the coding conventions should lead to a defensible adverse finding.

*Source:* *[2] II.5.4, II.5.4.2.*

*Impact:* *Click here to add the Impact*

➞ **4.6.1-C** Review source versus workmanship requirements

The test lab ***SHALL*** assess the extent to which the application logic adheres to the requirements of Volume III Section 5.4.1.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

With respect to Requirement III.5.4.1.4-B, see Requirement IV.2.4.7.2-H. The reviewer should consider the functional organization of each module or callable unit and the use of formatting, such as blocking into readable units, that supports the intent of Requirement III.5.4.1.4-B.

*Source:* *[2] II.5.4.*

*Impact:* *Click here to add the Impact*

➞ **4.6.1-D** Efficacy of built-in self-tests

The test lab ***SHALL*** verify the efficacy of built-in measurement, self-test, and diagnostic capabilities described in Volume III Section 6.4.2.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2] I.2.3.4.1.a2 (the second a).*

*Impact:* *Click here to add the Impact*

## 4.6.2 Security

This section is to be provided by STS.

# 4.7 Logic Verification

This inspection is to assess conformity with Requirement III.5.3.2-A and related requirements.

Because of its high complexity, the scope of logic verification is pragmatically limited to core logic. Software modules that are solely devoted to interacting with the user or formatting reports are not subject to logic verification. However, they

are required to conform with Requirement III.5.1-A, which is tested in Volume V Section 4.3 and Volume V Section 4.6.2.

Although these requirements are scoped to core logic, in some cases the test lab may need to inspect other application logic, border logic and third-party logic to assess conformity. Per Requirement IV.2.4.7.2-E, the source code for all of these must be provided.

[18] provides the following description of logic verification, therein known as "program proving:"

> Assertions are made at various locations in the program which are used as pre- and post-conditions to various paths through the program. The proof consists of two parts. The first involves showing that the program transfers the pre-conditions into the post-conditions according to a set of logical rules defining the semantics of the programming language, provided that the program actually terminates (i.e. reaches its proper conclusion). The second part is to demonstrate that the program does indeed terminate (e.g. does not go into an infinite loop). Both parts may need inductive arguments.

The inspection specified here does not assume that the programming language has formally specified semantics. Consequently, a formal proof at any level cannot be mandated. Instead, a combination of informal arguments (see Requirement IV.2.4.7.2-F.b) and limitations on complexity (see Requirement III.5.4.1.4-B.1) seeks to make the correctness of callable units at the lowest level intuitively obvious and to enable the verification of higher level units using the pre- and postconditions of invoked units as given partial proofs. The resulting inspection is not as rigorous as a formal proof, but still provides greater assurance than is provided by operational testing alone.

Inasmuch as the following behaviors would almost certainly preclude a demonstration of the correctness of the logic, logic verification will almost certainly involve a demonstration that they cannot occur:

- Numeric errors such as overflow and divide-by-zero;
- Buffer overruns / out-of-bounds accesses of arrays or strings;
- Null pointer dereferences;
- Stack overflows;
- Invocations of undefined or implementation-dependent behaviors;
- Race conditions or other nondeterministic execution;
- Abrupt termination.

It is acceptable, even expected, that logic verification will show that some or most exception handlers in the source code cannot logically be invoked. These exception handlers are not redundant—they provide defense-in-depth against faults that escape detection during logic verification and unpredictable failures that compromise the system.

→ **4.7-A** Validate inductive assertions

For each callable unit (function, method, operation, subroutine, procedure, etc.) in core logic, the test lab ***SHALL*** verify that the preconditions and postconditions correctly describe the behavior of the unit in all cases.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

See Requirement IV.2.4.7.2-F. For a callable unit at the lowest level, this verification should be achievable through code reading. For a higher level unit, the pre- and postconditions of the units that it invokes serve as given partial proofs in the argument that the pre- and postconditions of the higher level unit are correct.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **4.7-B** Validate limits

The test lab ***SHALL*** verify that the assumptions about capacities and limits that appear in the preconditions, postconditions, and proofs are consistent with the capacities and limits that the devices are claimed in the implementation statement to be capable of processing correctly.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

See Requirement IV.2.4.7.2-F.a and Requirement III.2.5-A.e.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **4.7-C** Verify constraints

For the core logic as a whole, and for each constraint indicated in Volume III Section 7.3, the test lab ***SHALL*** verify that the constraint is satisfied in all cases within the aforementioned capacities and limits.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

See Requirement IV.2.4.7.2-G.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **4.7-D** Burden of proof

If the test lab finds that the preconditions, postconditions, and proofs provided by the vendor are insufficient or incorrect, the responsibility for completing or correcting them ***SHALL*** be the vendor's.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Although test labs will doubtless provide advice and assistance to their clients, they are not required to fill in gaps in the vendor's submission.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

# Chapter 5: Test Methods

The accredited test lab must design and perform procedures to test a voting system against the requirements outlined in Volume III. Test procedures must be designed and performed that address:

1. Overall system capabilities;
2. Pre-voting functions;
3. Voting functions;
4. Post-voting functions;
5. System maintenance; and
6. Transportation and storage.

The specific procedures to be used must be identified in the National Certification Test Plan prepared by the accredited test lab (see Volume IV Chapter 4). These procedures must not rely on vendor testing as a substitute for independent testing.

## 5.1 Hardware

### 5.1.1 Electromagnetic Compatibility (EMC) Immunity

Testing of voting systems for EMC immunity will be conducted using the black box testing approach, which "ignores the internal mechanism of a system or component and focuses solely on the outputs generated in response to selected inputs and execution conditions" (from [EMC 12]). It will be necessary to subject voting systems to a regimen of tests including most, if not all, disturbances that might be expected to impinge on the system, as recited in the requirements of Volume III.

**Note:** *Some EMC immunity requirements have been established by Federal Regulations or for compliance with authorities having jurisdiction as a condition for offering equipment to the US market. In such cases, part of the requirements include affixing a label or notice stating that the equipment complies with the technical requirements, and therefore the VVSG does not suggest performing a redundant test.*

The VVSG required tests are briefly described in the following sections.

#### 5.1.1.1 Steady-state Conditions

Accredited testing laboratories that perform certification tests can be expected to have readily available a 120 V power supply from an energy service provider and access to a landline telephone service provider that will enable them to simulate the environment of a typical polling place and therefore perform the required tests.

### 5.1.1.2 Conducted Disturbances Immunity

Immunity to conducted disturbances will be demonstrated by appropriate industry-recognized tests and criteria, for the ports involved in the operation of the voting system.

Adequacy of the product is demonstrated by satisfying specific “pass criteria” as outcome of the required tests, which include not producing failure in the functions, firmware, or hardware.

The test procedure, test equipment and test sequences will be based on some benchmark tests, and observation of the voltage and current waveforms during the tests, including, if relevant, detection of a “walking wounded” condition resulting from a severe but not immediately lethal stress that would produce a hardware failure some time later on.

→ **5.1.1.2-A** Power Port Disturbances

Testing ***SHALL*** be conducted in accordance with the power port stress testing specified in IEEE Std C62.41.2™-2002 [EMC 10] and IEEE Std C62.45™-2002 [EMC 11].

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Both the IEEE and the IEC have developed test protocols for immunity of equipment power ports. In the case of a voting system intended for application in the United States, test equipment tailored to perform tests according to these two IEEE standards is readily available in tests laboratories, thus facilitating the process of compliance testing.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **5.1.1.2-A.1** Combination Wave

Testing ***SHALL*** be conducted in accordance with the power port stress of “Category B” to be applied by a Combination Waveform generator, in the powered mode, between line and neutral as well as between line and equipment grounding conductor.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

To satisfy this requirement, voting systems **SHALL** be capable of withstanding a 1.2/50 – 8/20 Combination Wave of 6 kV open-circuit voltage, 3 kA short-circuit current, with the following application points.

- Three surges, positive polarity at the positive peak of the line voltage.
- Three surges, negative polarity at the negative peak of the line voltage, line to neutral
- Three surges, positive polarity at the positive peak of the line voltage, line to equipment grounding conductor
- Three surges, negative polarity at the negative peak of the line voltage, line to equipment grounding conductor

The requirement of three successive pulses is based on the need to monitor any possible change in the equipment response caused by the application of the surges.

*Source:* *[EMC 10], Table 3.*

*Impact:* *Click here to add the Impact*

↳ **5.1.1.2-A.2** Ring Wave

Testing ***SHALL*** be conducted in accordance with the power port stress of "Category B" to be applied by a "Ring Wave" generator, in the powered mode, between line and neutral as well as between line and equipment grounding conductor and neutral to equipment grounding conductor, at the levels shown below.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Two different levels are recommended:

1. 6 kV open-circuit voltage per Table 2 of [EMC 10], applied as follows:
- Three surges, positive polarity at the positive peak of the line voltage, line to neutral
- Three surges, negative polarity at the negative peak of the line voltage, line to neutral
- Three surges, positive polarity at the positive peak of the line voltage, line to equipment grounding conductor
- Three surges, negative polarity at the negative peak of the line voltage, line to equipment grounding conductor

2. 3 kV open circuit voltage, per Table 5 of [EMC 10], applied as follows:

- Three surges, positive polarity at the positive peak of the line voltage, neutral to equipment grounding conductor
- Three surges, negative polarity at the negative peak of the line voltage, neutral to equipment grounding conductor

*Source:* *[EMC 10], Table 2 and Table 5.*

*Impact:* *Click here to add the Impact*

↳ **5.1.1.2-A.3** Electrical Fast Transient Burst

Testing ***SHALL*** be conducted in accordance with the recommendations of IEEE Std C62.41.2™-2002 [EMC 10] and IEEE Std C62.45™-2002 [EMC 11].

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Unlike the preceding two tests that are deemed to represent possibly destructive surges, the Electrical Fast Transient (EFT) Burst has been developed to demonstrate equipment immunity to non-destructive but highly disruptive events. Repetitive bursts of unidirectional 5/50 ns pulses lasting 15 ms and with 300 ms separation are coupled into terminals of the voting system by coupling capacitors for the power port and by the coupling clamp for the telephone connection cables.

*Source:* *[EMC 10], Table 6, [EMC 19]*

*Impact:* *Click here to add the Impact*

↳ **5.1.1.2-A.4** Sags and Swells

Testing ***SHALL*** be conducted by applying gradual steps of overvoltage across the line and neutral terminals of the voting system unit.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Testing for sag immunity within the context of EMC is not necessary in view of the requirement (Volume III, Section 16.3.3.2-A.4) that the voting system be provided with a two-hour back-up capability (to be verified by inspection). Testing for swells and permanent overvoltage conditions is necessary to ensure immunity to swells (no loss of data) and to permanent overvoltages (no overheating or operation of a protective fuse)

A) Short-duration Swells

As indicated by the ITI Curve [EMC 23], it is necessary to ensure that voting systems not be disturbed by a temporary overvoltage of 120 % normal line voltage lasting from 3 ms to 0.5 s. (Shorter durations fall within the definition of "surge.")

B) Permanent Overvoltage

As indicated by the ITI Curve [EMC 23], it is necessary to ensure that voting systems not be disturbed nor overheat for a permanent overvoltage of 110 % of the nominal 120 V rating of the voting system

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **5.1.1.2-B** Communications (Telephone) Port Disturbances

Testing ***SHALL*** be conducted in accordance with the telephone port stress testing specified in industry-recognized standards developed for telecommunications in general, particularly equipment connected to landline telephone service providers.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Voting systems, by being connected to the outside service provider via premises wiring, can be exposed to a variety of electromagnetic disturbances. These have been classified as emissions from adjacent equipment, lightning-induced, power-fault induced, power contact, Electrical Fast Transient (EFT), and steady-state induced voltage.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

↳ **5.1.1.2-B.1** Emissions from Other Connected Equipment

Testing ***SHALL*** be conducted in accordance with the emissions limits stipulated for other equipment of the voting system connected to the premises wiring of the polling place.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Emission limits for the power port of voting systems are discussed in Volume III, Requirement 16.3.3.2-B.1, with reference to numerical values stipulated in [EMC

27]. EMC of a complete voting system installed in a polling facility thus implies that individual components of voting systems must demonstrate immunity against disturbances at a level equal to the limits stipulated for emissions of adjacent pieces of equipment.

*Source:* *[EMC 27], subclause 3.2.3*

*Impact:* *Click here to add the Impact*

↳ **5.1.1.2-B.2** Lightning-induced Disturbances

Testing ***SHALL*** be conducted in accordance with the requirements of Telcordia GR-1089 [EMC 27] for simulation of lightning.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Telcordia GR-6089 [EMC 27] lists two types of tests, respectively (First-Level Lightning Surge Test and Second-Level Lightning Surge Test, as follows:

A) First-Level Lightning Surge Test

The particular voting system piece of equipment under test (generally referred to as "EUT") is placed in a complete operating system performing its intended functions, while monitoring proper operation, with checks performed before and after the surge sequence. Manual intervention or power cycling is not permitted before verifying proper operation of the voting system.

B) Second-Level Lightning Surge Test

Second-level lightning surge test is performed as a fire hazard indicator with cheesecloth applied to the particular EUT.

This second-level test, which can be destructive, may be performed with the EUT operating at a sub-assembly level equivalent to the standard system configuration, by providing dummy loads or associated equipment equivalent to what would be found in the complete voting system, as assembled in the polling place.

*Source:* *[EMC 27], subclauses 4.6.7 and 4.6.8*

*Impact:* *Click here to add the Impact*

↳ **5.1.1.2-B.3** Power Faults-induced Disturbances

Testing ***SHALL*** be conducted in accordance with the requirements of Telcordia GR-1089 [EMC 27] for simulation power-faults-induced events.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Tests that can be used to assess the immunity of voting systems to power fault-induced disturbances are described in detail in [EMC 27] for several scenarios and types of equipment, each involving a specific configuration of the test generator, test circuit, and connection of the equipment.

*Source:* *[EMC 27], subclause 4.6*

*Impact:* *Click here to add the Impact*

↳ **5.1.1.2-B.4** Power Contact Disturbances

Testing ***SHALL*** be conducted in accordance with the requirements of Telcordia GR-1089 [EMC 27] for simulation of power-contact events.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Tests for power contact (sometimes called “power cross”) immunity of voting systems immunity are described in detail in [EMC 27] for several scenarios and types of equipment, each involving a specific configuration of the test generator, test circuit, and connection of the equipment.

*Source:* *[EMC 27], subclause 4.6*

*Impact:* *Click here to add the Impact*

↳ **5.1.1.2-B.5** Electrical Fast Transient (EFT)

Testing ***SHALL*** be conducted in accordance with the requirements of Telcordia GR-1089 for simulation of electrostatic discharges.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Telcordia GR-1089 [EMC 27] calls for performing EFT tests but refers to [EMC 19] for details of the procedure. While EFT generators, per the IEC standard [EMC 19], offer the possibility of injecting the EFT burst into a power port by means of coupling capacitors, the other method described by the IEC standard, the so-called “capacitive coupling clamp” is the recommended method for coupling the burst into leads connected to the telephone port of the voting system under test. Therefore,

the reference standard to apply is the [EMC 19] rather than the [EMC 27] document.

*Source:* *[EMC 19], clause 6*

*Impact:* *Click here to add the Impact*

↳ **5.1.1.2-B.6** Steady-state Induced Voltage

Testing ***SHALL*** be conducted in accordance with the requirements of Telcordia GR-1089 [EMC 27] for simulation of steady-state induced voltages.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Telcordia GR-1089 [EMC 27] describes two categories of tests, depending on the length of loops, the criterion being a loop length of 20 kft (sic). For metric system units, that criterion may be considered to be 6 km, a distance that can be exceeded for some low-density rural or suburban locations of a polling place. Therefore, the test circuit to be used should be the one applying the highest level of induced voltage,

*Source:* *[EMC 27], sub-clause 5.2*

*Impact:* *Click here to add the Impact*

→ **5.1.1.2-C** Interaction between Power Port and Telephone Port

Inherent immunity against data corruption and hardware damage caused by interaction between the power port and the telephone port ***SHALL*** be demonstrated by applying a 0.5 µs – 100 kHz Ring wave between the power port and the telephone port.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Although IEEE is in the process of developing a standard (IEEE PC62.50) to address the interaction between the power port and communications port, no standard has been promulgated at this date, but published papers in peer-reviewed literature [EMC 25] suggest that a representative surge can be the Ring Wave of [EMC 10], applied between the equipment grounding conductor terminal of the voting system component under test and each of the tip and ring terminals of the voting system components intended to be connected to the telephone network.

Inherent immunity of the voting system might have been achieved by the manufacturer, as suggested in PC62.50, by providing a surge-protective device between these terminals that will act as a temporary bond during the surge, a function which can be verified by monitoring the voltage between the terminals when the surge is applied.

The IEEE project is IEEE PC62.50 "Draft Standard for Performance Criteria and Test Methods for Plug-in, Portable, Multiservice (Multiport) Surge Protective Devices for Equipment Connected to a 120/240 V Single Phase Power Service and Metallic Conductive Communication Line(s)". This is an unapproved standard, with estimated approval date 2008.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

### 5.1.1.3 Radiated Disturbances Immunity

→ **5.1.1.3-A** Electromagnetic Field Immunity (80 MHz to 6.0 GHz)

Testing ***SHALL*** be conducted according to procedures in CISPR 24 [EMC 7], and either IEC 61000-4-3 [EMC 18] or IEC 61000-4-21:2003 [EMC 22].

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

IEC 61000-4-3 [EMC 18] specifies using an absorber lined shielded room (fully or semi anechoic chamber) to expose the device-under-test. An alternative procedure is the immunity testing procedures of IEC [EMC 22], performed in a reverberating shielded room (radio-frequency reverberation chamber).

*Source:* *[EMC 7], [EMC 18], [EMC 22]*

*Impact:* *Click here to add the Impact*

→ **5.1.1.3-B** Electromagnetic Field Immunity (150 kHz to 80 MHz)

Testing for electromagnetic fields below 80 MHz ***SHALL*** be conducted according to procedures defined in IEC 61000-4-6 [EMC 20].

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[EMC 1], [EMC 20]*

*Impact:* *Click here to add the Impact*

➞ **5.1.1.3-C** Electrostatic Discharge Immunity

Testing ***SHALL*** be conducted in accordance with the recommendations of ANSI Std C63.16 [EMC 3], applying an air discharge or a contact discharge according to the nature of the enclosure of the voting system.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Electrostatic discharges occurring as an intruder, simulated by a portable ESD simulator approaches the EUT involve an air discharge that can upset the logic operations of the circuits, depending on their status. In the case of a conducting enclosure, the resulting discharge current flowing in the enclosure can couple with the circuits and also upset the logic operations. Therefore, it is necessary to apply a sufficient number of discharges to significantly increase the probability that the circuits will be exposed to the interference at the time of the most critical transition of the logic. This condition can be satisfied by using a simulator with repetitive discharge capability while a test operator interacts with the voting terminal, mimicking the actions of a voter or initiating a data transfer from the terminal to the local tabulator.

*Source:* *[EMC 3], [EMC 17]*

*Impact:* *Click here to add the Impact*

## 5.1.2 Electromagnetic Compatibility (EMC) Emissions Limits

Testing of voting systems for EMC emission limits will be conducted using the black testing approach, which "ignores the internal mechanism of a system or component and focuses solely on the outputs generated in response to selected inputs and execution conditions" [EMC 12].

It will be necessary to subject voting systems to a regimen of tests to demonstrate compliance with emission limits. The test program should include most, if not all disturbances that might be expected to be emitted from the system under test, unless compliance with mandatory limits such as FCC regulations is explicitly stated for the voting system under test. These tests are described in the following paragraphs.

### 5.1.2.1 Conducted Emissions Limits

I. Power Port

1) Low Frequency Range

As discussed in Volume III, Section 16.3.4, , the relative importance of low-frequency harmonic emissions and the current drawn by other loads in the polling place will result in a negligible percentage of harmonics at the point of common connection, as discussed in [EMC 13]. Thus no test is required to assess the harmonic emission of a voting station.

2) High Frequency Range

High-frequency emission limits have been established by Federal Regulations [EMC 1] as a condition for offering equipment to the US market. In such cases, part of the requirements include affixing a label or notice stating that the equipment complies with the stipulated limits. Therefore the VVSG does not suggest performing a redundant test.

II. Communications (Telephone) Port

→ **5.1.2.1-A** Communications Port Emissions

Unintended conducted emissions from a voting system telephone port ***SHALL*** be tested for its analog voice band leads in the metallic as well as its longitudinal voltage limits.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Telcordia GR-1089 [EMC 27] stipulates limits for both the common mode (longitudinal) and differential mode (metallic) over a frequency range defined by maximum voltage and terminating impedances.

*Source:* *[EMC 27], subclause 3.2.3*

*Impact:* *Click here to add the Impact*

## 5.1.2.2 Radiated Emissions

→ **5.1.2.2-A** Radiated Emission Limits

Compliance with emission limits ***SHALL*** be documented on the hardware in accordance with the stipulations of FCC Part 15, Class B [EMC 1].

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

### 5.1.3 Other (non-EMC) Industry-mandated Requirements

#### 5.1.3.1 Dielectric Stresses

➞ **5.1.3.1-A** Dielectric Withstand

Testing ***SHALL*** be conducted in accordance with the stipulations of industry-consensus telephone requirements of Telcordia GR-1089 [EMC 27].

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *[EMC 27], section 4.9.5*

*Impact:* *Click here to add the Impact*

#### 5.1.3.2 Leakage via Grounding Port

➞ **5.1.3.2-A** Leakage Current via Grounding Port

Simple verification of an acceptable low leakage current ***SHALL*** be performed by powering the voting system under test via a listed Ground-Fault Circuit Interrupter (GFCI) and noting that no tripping of the GFCI occurs when the voting system is turned on.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

#### 5.1.3.3 Safety

The presence of a listing label (required by authorities having jurisdiction) referring to a safety standard, such as [EMC 29], makes repeating the test regimen unnecessary. Details on the safety considerations are addressed in Volume III, Section 12.2.8.3.

#### 5.1.3.4 Label of Compliance

Some industry mandated requirements require demonstration of compliance, while for others the manufacturer affixes of label of compliance, which then makes repeating the tests unnecessary and economically not justifiable.

## 5.2 Functional Testing

Functional testing is performed to confirm the functional capabilities of a voting system. The accredited test lab designs and performs procedures to test a voting system against the requirements outlined in Volume III. Additions or variations in testing may be appropriate depending on the system's use of specific technologies and configurations, the system capabilities, and the outcomes of previous testing.

Functional tests cover the full range of system operations. They include tests of fully integrated system components, internal and external system interfaces, HFP: usability and accessibility?, and security. During this process, election management functions, ballot-counting logic, and system capacity are exercised.

The accredited test lab tests the interface of all system modules and subsystems with each other against the vendor's specifications. For systems that use telecommunications capabilities, components that are located at the poll site or separate vote counting site are tested for effective interface, accurate vote transmission, failure detection, and failure recovery. For voting systems that use telecommunications lines or networks that are not under the control of the vendor (e.g., public telephone networks), the accredited test lab tests the interface of vendor-supplied components with these external components for effective interface, vote transmission, failure detection, and failure recovery.

STS: Fix this paragraph after security sections are written. The security tests focus on the ability of the system to detect, prevent, log, and recover from a broad range of security risks as identified in Volume III Chapter 3. The range of risks tested is determined by the design of the system and potential exposure to risk. Regardless of system design and risk profile, all systems are tested for effective access control and physical data security. For systems that use public telecommunications networks to transmit election management data or election results (such as ballots or tabulated results), security tests are conducted to ensure that the system provides the necessary identity-proofing, confidentiality, and integrity of transmitted data. The tests determine if the system is capable of detecting, logging, preventing, and recovering from types of attacks known at the time the system is submitted for qualification. The accredited test lab may meet these testing requirements by confirming the proper implementation of proven commercial security software.

## 5.2.1 General guidelines

### 5.2.1.1 General test template

Most test cases will follow this general template. Different test cases will elaborate on the general template in different ways, depending on what is being tested.

1. Establish initial state (clean out data from previous tests, verify resident software/firmware)
2. Program election and prepare ballots and/or ballot styles
3. Generate pre-election audit reports
4. Configure voting devices
5. Run system readiness tests
6. Generate system readiness audit reports
7. Precinct count only:
   A. Open poll
   B. Run precinct count test ballots
   C. Close poll
8. Run central count test ballots (central count / absentee ballots only)
9. Generate in-process audit reports
10. Generate data reports for the specified reporting contexts
11. Inspect ballot counters
12. Inspect reports

### 5.2.1.2 General pass criteria

➞ **5.2.1.2-A** Applicable tests

The test lab need only consider tests that apply to the classes specified in the implementation statement, including those tests that are designated for all systems. The test verdict for all other tests ***SHALL*** be Not Applicable.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **5.2.1.2-B** Test assumptions

If the documented assumptions for a given test are not met, the test verdict ***SHALL*** be Waived and the test ***SHALL*** not be executed.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **5.2.1.2-C** Missing functionality

If the test lab is unable to execute a given test because the system does not support functionality that is required per the implementation statement or is required for all systems, the test verdict ***SHALL*** be Fail.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **5.2.1.2-D** Any demonstrable violation justifies an adverse opinion

A demonstrable violation of any applicable requirement of the VVSG during the execution of any test case ***SHALL*** result in a test verdict of Fail.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

See Volume V Section 2.6.5 for directions on termination, suspension, and resumption of testing following a verdict of Fail.

## 5.2.2 Structural coverage (white box testing)

This section specifies requirements for "white box" (glass box, clear box) testing of voting system logic.

For voting systems that reuse components or subsystems from previously tested and qualified systems, the test lab may, per Requirement IV.4.1-D, find it unnecessary to repeat instruction, branch, and interface testing on the previously qualified, unmodified components. However, the test lab must fully test all new or modified components and perform what regression testing is necessary to ensure that the complete system remains compliant.

→ **5.2.2-A** Instruction and branch testing

The test lab ***SHALL*** execute test cases that provide coverage of every accessible instruction and branch outcome in application logic and border logic.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

[18] p. 266 writes: "Exhaustive path testing is, in general, almost impossible." This is not exhaustive path testing, but testing of paths sufficient to cover every instruction and every branch outcome, which [18] p. 265 calls decision/branch coverage. See [16] p. 39 for a frank explanation of how these differ and why the required testing is the minimum acceptable.

Full coverage of third-party logic is not mandated because it might include a large amount of code that is never used by the voting application. Nevertheless, the relevant portions of third-party logic should be tested diligently.

There should be no inaccessible code in application logic and border logic other than defensive code (including exception handlers) that is provided to defend against the occurrence of "can't happen" conditions.

*Source:* *Clarification of [2]/[6] II.6.2.1 and II.A.4.3.3.*

*Impact:* *Click here to add the Impact*

→ **5.2.2-B** Interface testing

The test lab ***SHALL*** execute test cases that test the interfaces of all application logic and border logic modules and subsystems, and all third-

party logic modules and subsystems that are in any way used by application logic or border logic.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Clarification of [2]/[6] II.6.3*

*Impact:* *Click here to add the Impact*

→ **5.2.2-C** Pass criteria for structural testing

The test lab ***SHALL*** define pass criteria using the VVSG (for standard functionality) and the vendor-supplied system documentation (for implementation-specific functionality) to determine acceptable ranges of performance.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Since the nature of the requirements specified by the vendor-supplied system documentation is unknown, conformity for implementation-specific functionality may be subject to interpretation. Nevertheless, egregious disagreements between the behavior of the system and the behavior specified by the vendor should lead to a defensible adverse finding.

*Source:* *[2]/[6] II.A.4.3.3*

*Impact:* *Click here to add the Impact*

## 5.2.3 Functional coverage (black box testing)

All voting system logic, including any embedded in COTS components, is subject to functional testing.

For voting systems that reuse components or subsystems from previously tested and qualified systems, the test lab may, per Requirement IV.4.1-D, find it unnecessary to repeat functional testing on the previously qualified, unmodified components. However, the test lab must fully test all new or modified components and perform what regression testing is necessary to ensure that the complete system remains compliant.

➔ **5.2.3-A** Functional testing, VVSG requirements

The test lab ***SHALL*** execute test cases that provide coverage of every applicable, mandatory ("***SHALL***"), functional requirement of the VVSG.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Depending upon the design and intended use of the voting system, all or part of the functions listed below must be tested.

1. Ballot preparation subsystem;
2. Test operations performed prior to, during, and after processing of ballots, including:
   A. Logic tests to verify interpretation of ballot styles, and recognition of precincts to be processed;
   B. Accuracy tests to verify ballot reading accuracy;
   C. Status tests to verify equipment statement and memory contents;
   D. Report generation to produce test output data; and
   E. Report generation to produce audit data records;
3. Procedures applicable to equipment used in the polling place for:
   A. Opening the polls and enabling the acceptance of ballots;
   B. Maintaining a count of processed ballots;
   C. Monitoring equipment status;
   D. Verifying equipment response to operator input commands;
   E. Generating real-time audit messages;
   F. Closing the polls and disabling the acceptance of ballots;
   G. Generating election data reports;
   H. Transfer of ballot counting equipment, or a detachable memory module, to a central counting location; and
   I. Electronic transmission of election data to a central counting location; and
4. Procedures applicable to equipment used in a central counting place:
   A. Initiating the processing of a ballot deck, programmable memory device, or other applicable media for one or more precincts;
   B. Monitoring equipment status;
   C. Verifying equipment response to operator input commands;
   D. Verifying interaction with peripheral equipment, or other data processing systems;
   E. Generating real-time audit messages;

F. Generating precinct-level election data reports;

G. Generating summary election data reports;

H. Transfer of a detachable memory module to other processing equipment;

I. Electronic transmission of data to other processing equipment; and

J. Producing output data for interrogation by external display devices.

This requirement is derived from [2]/[6] II.A.4.3.4, "Software Functional Test Case Design," in lieu of a canonical functional test suite. Once a complete, canonical test suite is available, the execution of that test suite will satisfy this requirement. For reproducibility, use of a canonical test suite is preferable to development of custom test suites.

In those few cases where requirements specify "fail safe" behaviors in the event of freak occurrences and failures that cannot be reproduced and should not be reproducible by a test lab, the requirement is considered covered if the test campaign concludes with no occurrences of an event to which the requirement would apply. However, if a triggering event occurs, the test lab must assess conformity to the requirement based on the behaviors observed.

*Source:* *[2]/[6] II.A.4.3.4*

*Impact:* *Click here to add the Impact*

→ **5.2.3-B** Functional testing, capacity tests

The test lab ***SHALL*** execute test cases to verify that the system and its constituent devices are able to operate correctly at the limits specified in the implementation statement, including

1. Maximum number of ballots;
2. Maximum number of ballot positions;
3. Maximum number of ballot styles;
4. Maximum number of contests;
5. Maximum vote total (counter capacity);
6. Maximum number of provisional, challenged, or review-required ballots;
7. Maximum number of candidates or choices per contest; and
8. Any similar limits that apply.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

See Volume III Section 2.5.

*Source:* *Generalization from [2]/[6] II.6.2.3.*

*Impact:* *Click here to add the Impact*

↳ **5.2.3-B.1** Practical limit on capacity operational tests

If an implementation limit is sufficiently great that it cannot be verified through operational testing without severe expense and hardship, the test lab ***SHALL*** attest this in the test report and substitute a combination of design review, logic verification, and operational testing to a reduced limit.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

For example, since counter capacity can easily be designed to $2^{32}$ and beyond without straining current technology, some reasonable limit for required operational testing is needed. However, it is preferable to test the limit operationally if there is any way to accomplish it.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **5.2.3-C** Functional testing, stress tests

The test lab ***SHALL*** execute test cases to verify that the system is able to respond gracefully to attempts to process more than the expected number of ballots per precinct, more than the expected number of precincts, higher than expected volume or ballot tabulation rate, or any similar conditions that tend to overload the system's capacity to process, store, and report data.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

In particular, Requirement III.6.6.6-A should be verified through operational testing if the limit is practically testable.

*Source:* *[2]/[6] II.A.4.3.5*

*Impact:* *Click here to add the Impact*

→ **5.2.3-D** Functional testing, volume test

The test lab ***SHALL*** conduct a volume test in conditions approximating normal use in an election. The entire system ***SHALL*** be tested, from election definition through the reporting and auditing of final results.

*Applies to:* *Voting system*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Data collected during this test contribute substantially to the evaluations of reliability, accuracy, and probability of misfeed (see Volume V Section 5.3).

*Source:* *[5]*

*Impact:* *Click here to add the Impact*

↳ **5.2.3-D.1** Volume test, vote-capture devices

For systems that include VEBDs, a minimum of 100 VEBDs ***SHALL*** be tested and a minimum of 110 ballots ***SHALL*** be cast manually on each VEBD.

*Applies to:* *VEBD*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

For vote-by-phone systems, this would mean having 100 concurrent callers, not necessarily 100 separate servers to answer the calls, if one server suffices to handle many incoming calls simultaneously. Other client-server systems would be analogous.

To ensure that the correct results are known, test voters should be furnished with predefined scripts that specify the votes that they should cast.

*Source:* *[5]*

*Impact:* *Click here to add the Impact*

↳ **5.2.3-D.2** Volume test, precinct tabulator

For systems that include precinct tabulators, a minimum of 50 precinct tabulators ***SHALL*** be tested and a minimum of 400 ballots ***SHALL*** be counted by each precinct tabulator.

*Applies to:* *Precinct tabulator*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

[1] 7.5 specified, "The total number of ballots to be processed by each precinct counting device during these tests **SHALL** be at least ten times the number of ballots expected to be counted on a single device in an election (500 to 750), but in no case less than 5,000."

*Source:* *[5]*

*Impact:* *Click here to add the Impact*

↳ **5.2.3-D.3** Volume test, central tabulator

For systems that include central tabulators, a minimum of 2 central tabulators ***SHALL*** be tested and a minimum of 75000 ballots ***SHALL*** be counted in total.

*Applies to:* *Central tabulator*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

[5] did not specify test parameters for central tabulators. The test parameters specified here are based on the smallest case provided for central count systems in Exhibit J-1 of Appendix J, Acceptance Test Guidelines for P&M Voting Systems, of [1]. An alternative would be to derive test parameters from the test specified in [1] 7.3.3.2 and (differently) in [2]/[6] II.4.7.1. A test of duration 163 hours with a ballot tabulation rate of 300 / hour yields a total ballot volume of 48900—presumably, but not necessarily, on a single tabulator.

[1] 7.5 specified, "The number of test ballots for each central counting device **SHALL** be at least thirty times the number that would be expected to be voted on a single precinct count device, but in no case less than 15,000."

*Source:* *[1] Exhibit J-1 (Central Count)*

*Impact:* *Click here to add the Impact*

↳ **5.2.3-D.4** Test imperfect marks and folds

The testing of MCOS ***SHALL*** include marks filled according to the recommended instructions to voters, imperfect marks as specified in Requirement III.6.8.5-D, and ballots with folds that do not intersect with voting targets.

*Applies to:* *MCOS*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Numerous public comments and issues raised by TGDC.*

*Impact:* *Click here to add the Impact*

→ **5.2.3-E** Functional testing, languages

The test lab ***SHALL*** execute test cases to verify that the system is able to produce and utilize ballots in all of the languages that are claimed to be supported in the implementation statement.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

See Volume III Section 2.5.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **5.2.3-F** Functional testing, error cases

The test lab ***SHALL*** execute test cases to verify that the system is able to detect, handle, and recover from abnormal input data, operator actions, and conditions.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

See Requirement III.5.4.1.8-A and Volume III Section 5.4.1.9.

*Source:* *[2]/[6] II.A.4.3.4*

*Impact:* *Click here to add the Impact*

↳ **5.2.3-F.1** Procedural errors

The test lab ***SHALL*** execute test cases to verify that the system detects and handles operator errors such as inserting control cards out of sequence or attempting to install configuration data that are not properly coded for the device.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[1] 8.8*

*Impact:* *Click here to add the Impact*

↳ **5.2.3-F.2** Hardware failures

The test lab ***SHALL*** execute test cases to verify that the system is able to respond to hardware malfunctions in a manner compliant with the requirements of Volume III Section 5.4.1.9.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

This capability may be validated by any convenient means (e.g., power off, disconnect a cable, etc.) in any equipment associated with ballot processing.

*Source:* *[1] 8.5*

*Impact:* *Click here to add the Impact*

↳ **5.2.3-F.3** Communications errors

For systems that use networking and/or telecommunications capabilities, the test lab ***SHALL*** execute test cases to verify that the system is able to detect, handle, and recover from interference with or loss of the communications link.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2]/[6] II.6.3*

*Impact:* *Click here to add the Impact*

➞ **5.2.3-G** Functional testing, vendor functionality

The test lab ***SHALL*** execute test cases that provide coverage of the full range of system functionality specified in the vendor's documentation, including functionality that exceeds the specific requirements of the VVSG.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Since the nature of the requirements specified by the vendor-supplied system documentation is unknown, conformity for implementation-specific functionality may be subject to interpretation. Nevertheless, egregious disagreements between the behavior of the system and the behavior specified by the vendor should lead to a defensible adverse finding.

*Source:* *[2]/[6] II.3.2.3, II.6.7*

*Impact:* *Click here to add the Impact*

➞ **5.2.3-H** Functional test matrix

The test lab ***SHALL*** prepare a detailed matrix of VVSG requirements, system functions, and the test cases that exercise them.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *[2]/[6] II.A.4.3.4*

*Impact:* *Click here to add the Impact*

➞ **5.2.3-I** Pass criteria for functional testing

The test lab ***SHALL*** define pass criteria using the VVSG (for standard functionality) and the vendor-supplied system documentation (for implementation-specific functionality) to determine acceptable ranges of performance.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Since the nature of the requirements specified by the vendor-supplied system documentation is unknown, conformity for implementation-specific functionality may be subject to interpretation. Nevertheless, egregious disagreements between the behavior of the system and the behavior specified by the vendor should lead to a defensible adverse finding.

*Source:* *[2]/[6] II.A.4.3.4*

*Impact:* *Click here to add the Impact*

### 5.2.4 Security coverage

This section is to be provided by STS.

## 5.3 Benchmarks

### 5.3.1 General method

Reliability, accuracy, and probability of misfeed are measured using ratios, each of which is the number of some kind of event (failures, errors, or misfeeds, respectively) divided by some measure of voting volume. The test method discussed here is applicable generically to all three ratios; hence, this discussion will refer to events and volume without specifying a particular definition of either.

By keeping track of the number of events and the volume over the course of a test campaign, one can trivially calculate the observed cumulative event rate by dividing the number of events by the volume. However, the observed event rate is not necessarily a good indication of the true event rate. The true event rate describes the expected performance of the system in the field, but it cannot be observed in a test campaign of finite duration, using a finite-sized sample. Consequently, the true event rate can only be estimated using statistical methods.

The system submitted for testing is assumed to be a representative sample (see [10] Ch. 8), so the variability of devices of the same type is out of scope.

The test method makes the simplifying assumption that events occur in a Poisson distribution, which means that the probability of an event occurring is assumed to be the same for each unit of volume processed. In reality, there are random events that satisfy this assumption but there are also nonrandom events that do not. For example, a logic error in tabulation software might be triggered every time a particular voting option is used. Consequently, a test campaign that exercised that voting option often would be more likely to indicate rejection based on reliability or accuracy than a test campaign that used different test cases. However, since these Guidelines require absolute correctness of tabulation logic, the only undesirable outcome is the one in which the system containing the logic error is accepted. Other evaluations specified in these Guidelines, such as functional testing and logic verification, are better suited to detecting systems that produce nonrandom errors and failures. Thus, when all specified evaluations are used together, the different test methods complement each other and the limitation of this particular test method with respect to nonrandom events is not bothersome.

For simplicity, all three cases (failures, errors, and misfeeds) are modelled using a continuous distribution (Poisson) rather than a discrete distribution (Binomial). In this application, where the probability of an event occurring within a unit of volume

is small, the difference in results from the discrete and continuous models is negligible.

These Guidelines specify rejection of a voting system if, at the conclusion of testing, under the specified assumptions, the probability that the requirement is satisfied is less than 0.1. This means that an 80 % confidence interval for the ratio being measured does not include the benchmark value, and we may be more than 90 % confident that the system is nonconforming.

Assuming an event rate of r, the probability of observing n or less events for volume v is the value of the Poisson cumulative distribution function,

$$P(n, rv) = \sum_{x=0}^{n} \frac{e^{-rv}(rv)^x}{x!}$$

For an observed event count $n > 0$, volume $v$, and event rate benchmark $r$, the probability that the true event rate is worse than the benchmark is equal to the probability that a system with true event rate $r$ would show less than $n$ events under the same conditions, which is $P(n-1, rv)$. Consequently, the minimum volume that is required to tolerate $n$ events without rejecting the system is found by solving $P(n-1, rv) = 0.9$ for $v$.

If a test campaign ends with acceptance, the test lab is required to report the event rate that was demonstrated with 90 % confidence, which is at the other end of the 80 % confidence interval. For $n$ observed events after $v$ volume, the demonstrated event rate is found by solving $P(n, rv) = 0.1$ for $r$.

In the general case, both equations must be solved numerically. However, for a fixed probability and a fixed value of $n$, the value of $rv$ is a constant. Table 9 provides the values of $rv$ for the probabilities 0.1 and 0.9, for n up to 20.

The demonstrated event rate given $n$ events and volume $v$ is found by dividing the pertinent value from the second column by $v$. For example, a volume of 600 with no events demonstrates an event rate of 2.302585093 / 600, or roughly $3.8376 \times 10^{-3}$.

The minimum volume required to tolerate $n$ events for an event rate benchmark $r$ is found by dividing the pertinent value from the third column by $r$. Since the condition was $P(n-1, rv) = 0.9$, the pertinent value is in the row for $n-1$, not $n$. For example, to tolerate one event with a benchmark of $10^{-7}$ would require a volume of $0.105360516 / 10^{-7}$, or 1053605.16. Where the measurement of volume is discrete rather than continuous, one would round up to the next integer.

Please note that the length of testing is determined in advance by the approved test plan. To adjust the length of testing based on the observed performance of the system in the tests already executed would bias the results and is not permitted. A Probability Ratio Sequential Test (PRST) [13][14][42] as was specified in previous versions of these Guidelines varies the length of testing without introducing bias, but practical difficulties result when the length of testing determined by the PRST disagrees with the length of testing that is otherwise required by the test plan.

| N | RV FOR P(N,RV) = 0.1 | RV FOR P(N,RV) = 0.9 |
|---|---|---|
| 0 | 2.302585093 | 0.105360516 |
| 1 | 3.889720170 | 0.531811608 |
| 2 | 5.322320338 | 1.102065328 |
| 3 | 6.680783068 | 1.744769563 |
| 4 | 7.993589586 | 2.432591026 |
| 5 | 9.274673893 | 3.151898030 |
| 6 | 10.532072106 | 3.894766805 |
| 7 | 11.770914462 | 4.656118177 |
| 8 | 12.994711541 | 5.432468058 |
| 9 | 14.205990292 | 6.221304605 |
| 10 | 15.406641172 | 7.020746595 |
| 11 | 16.598122144 | 7.829342026 |
| 12 | 17.781585636 | 8.645942495 |
| 13 | 18.957961272 | 9.469621186 |
| 14 | 20.128011869 | 10.299617307 |
| 15 | 21.292372541 | 11.135297238 |
| 16 | 22.451578759 | 11.976126635 |
| 17 | 23.606086947 | 12.821649940 |
| 18 | 24.756289913 | 13.671475021 |
| 19 | 25.902528607 | 14.525261465 |
| 20 | 27.045101225 | 15.382711505 |

Table 5-1 Factors for calculation of volume cutoff and demonstrated event rate

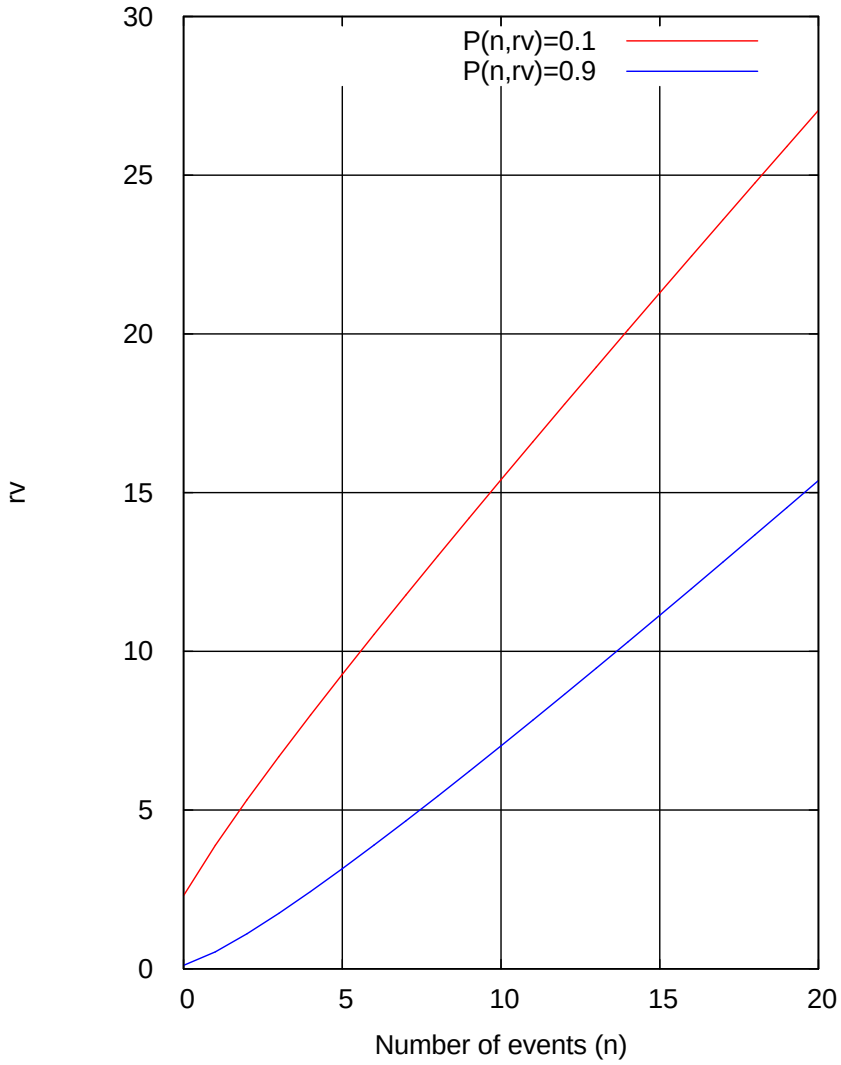



Table 5-2 Plot of values from Table 9

Table 5-2 can be extended for *n* up to 750 by running the following script through Octave[2] version 2.1.73.

```
silent_functions=1

# Function for the root finder to zero.  fsolve won't pass extra
# parameters to the function being solved, so we must use globals.
# nGlobal is number of events; pGlobal is probability.
function rvRootFn = rvRoot (rv)
  global nGlobal pGlobal
  rvRootFn = poisson_cdf (nGlobal, rv) - pGlobal
endfunction

# Find rv given n and p.  To initialize the root finder, provide
# startingGuess that is greater than zero and approximates the
answer.
function rvFn = rv (n, p, startingGuess)
  global nGlobal pGlobal
  nGlobal = n
```

```
  pGlobal = p
  startingGuess > 0 || error ("bad starting guess")
  [rvFn, info] = fsolve ("rvRoot", startingGuess)
  if (info != 1)
    perror ("fsolve", info)
  endif
endfunction

function table
  printf (" n      P=0.1        P=0.9\n")
  for n = 0:750
    rv01 = rv (n, 0.1, -4.9529e-05*n*n + 1.0715*n + 2.302585093)
    rv09 = rv (n, 0.9,  4.9522e-05*n*n + 0.9285*n + 0.105360516)
    printf ("%3u %12.8f %12.8f\n", n, rv01, rv09)
  endfor
endfunction

fsolve_options ("tolerance", 5e-12)
table
```

## 5.3.2 Reliability

→ **5.3.2-A** Reliability, pertinent tests

All test cases executed during conformity assessment ***SHALL*** be considered "pertinent" for assessment of reliability, with the following exceptions:

1. Tests in which failures are forced;
2. Tests in which portions of the system that would be exercised during an actual election are bypassed (see Volume V Section 2.6.3).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **5.3.2-B** Failure rate data collection

The test lab ***SHALL*** record the number of failures and the applicable measure of volume for each pertinent test execution, for each type of device, for each applicable failure type in Table 6 (Volume III Section 5.3.1.5).

*Applies to:* *Voting device*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

"Type of device" refers to the different models produced by the vendor. These are not the same as device *classes*. The system may include several different models of the same class, and a given model may belong to more than one class.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **5.3.2-C** Failure rate pass criteria

When operational testing is complete, the test lab ***SHALL*** calculate the failure total and total volume accumulated across all pertinent tests, for each type of device and failure type. If analysis of the cumulative behavior across all pertinent tests indicates that the probability of the true failure rate being worse than a benchmark specified in Requirement III.5.3.1.5-B is greater than 90 % for any type of device, the verdict on conformity to Requirement III.5.3.1.5-B ***SHALL*** be Fail. Otherwise, the verdict ***SHALL*** be Pass.

*Applies to:* *Voting device*

*Test Reference:* *Click here to add the Test Reference*

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

## 5.3.3 Accuracy

The informal concept of voting system accuracy is formalized using the ratio of the number of errors that occur to the volume of data processed, also known as error rate.

→ **5.3.3-A** Accuracy, pertinent tests

All test cases executed during conformity assessment ***SHALL*** be considered "pertinent" for assessment of accuracy, with the following exceptions:

1. Tests in which errors are forced;
2. Tests in which portions of the system that would be exercised during an actual election are bypassed (see Volume V Section 2.6.3).

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

➞ **5.3.3-B** Calculation of report total error rate

Given a set of vote data reports resulting from the execution of test cases, the observed cumulative report total error rate ***SHALL*** be calculated as follows.

1. Define a "report item" as any one of the numeric values (totals or counts) that must appear in any of the vote data reports. Each ballot count, each vote, overvote, and undervote total for each contest, and each vote total for each candidate or choice in each contest is a separate report item. The required report items are detailed in Volume III Section 6.9.3.
2. For each report item, compute the "report item error" as the absolute value of the difference between the correct value and the reported value. Special cases: If a value is reported that should not have appeared at all (spurious item), or if an item that should have appeared in the report does not (missing item), assess a report item error of one. Additional values that are reported as a vendor extension to the standard are not considered spurious items.
3. Compute the "report total error" as the sum of all of the report item errors from all of the reports.
4. Compute the "report total volume" as the sum of all of the correct values for all of the report items that are supposed to appear in the reports. Special cases: When the same logical contest appears multiple times, e.g. when results are reported for each ballot configuration and then combined or when reports are generated for multiple reporting contexts, each manifestation of the logical contest is considered a separate contest with its own correct vote totals in this computation.
5. Compute the observed cumulative report total error rate as the ratio of the report total error to the report total volume. Special cases: If both values are zero, the report total error rate is zero. If the report total volume is zero but the report total error is not, the report total error rate is infinite.

*Applies to:* *Voting system*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Click here and type the discussion about this requirement

*Source:* *Revision of [1] F.6*

*Impact:* *Click here to add the Impact*

→ **5.3.3-C** Error rate data collection

The test lab ***SHALL*** record the report total error and report total volume for each pertinent test execution.

*Applies to:* *Voting system*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

Accuracy is calculated as a system-level metric, not separated by device type.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **5.3.3-D** Error rate pass criteria

When operational testing is complete, the test lab ***SHALL*** calculate the report total error and report total volume accumulated across all pertinent tests. If analysis of the cumulative behavior across all pertinent tests indicates that the probability of the true report total error rate being worse than the benchmark specified in Requirement III.5.3.2-B is greater than 90 %, the verdict on conformity to Requirement III.5.3.2-B ***SHALL*** be Fail. Otherwise, the verdict ***SHALL*** be Pass.

*Applies to:* *Voting system*

*Test Reference:* *Click here to add the Test Reference*

D I S C U S S I O N

The report total volumes below which a given number of errors indicates rejection, for values less than 22, are shown in Table 5-3.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

| REPORT TOTAL ERROR | REPORT TOTAL VOLUME |
|---|---|
| 1 | 13171 |
| 2 | 66477 |
| 3 | 137759 |
| 4 | 218097 |
| 5 | 304074 |

| REPORT TOTAL ERROR | REPORT TOTAL VOLUME |
|---|---|
| 6 | 393988 |
| 7 | 486846 |
| 8 | 582015 |
| 9 | 679059 |
| 10 | 777664 |
| 11 | 877594 |
| 12 | 978668 |
| 13 | 1080743 |
| 14 | 1183703 |
| 15 | 1287453 |
| 16 | 1391913 |
| 17 | 1497016 |
| 18 | 1602707 |
| 19 | 1708935 |
| 20 | 1815658 |
| 21 | 1922839 |

Table 5-3 Error rate cutoff points

### 5.3.4 Probability of misfeed

This benchmark applies only to paper-based tabulators.

Multiple feeds, misfeeds (jams), and rejections of ballots that meet all vendor specifications are all treated collectively as "misfeeds" for benchmarking purposes; i.e., only a single count is maintained.

→ **5.3.4-A** Probability of misfeed, pertinent tests

All test cases executed during conformity assessment ***SHALL*** be considered "pertinent" for assessment of probability of misfeed, with the following exceptions:

1. Tests in which misfeeds are forced.

*Applies to:* *Click here to add the Applies to text*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

Click here and type the discussion about this requirement

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **5.3.4-B** Calculation of misfeed rate

For paper-based tabulators, the observed cumulative misfeed rate ***SHALL*** be calculated as follows.

1. Compute the "misfeed total" as the number of times that unforced multiple feed, misfeed (jam), or rejection of a ballot that meets all vendor specifications has occurred during the execution of test cases. It is possible for a given ballot to misfeed more than once; each misfeed would be counted.
2. Compute the "total ballot volume" as the number of successful feeds of ballot pages or cards during the execution of test cases. (If the pages of a multi-page ballot are fed separately, each page counts; but if both sides of a two-sided ballot are read in one pass through the tabulator, it only counts once.)
3. Compute the observed cumulative misfeed rate as the ratio of the misfeed total to the total ballot volume. Special cases: If both values are zero, the misfeed rate is zero. If the total ballot volume is zero but the misfeed total is not, the misfeed rate is infinite.

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

"During the execution of test cases" deliberately excludes jams that occur during pre-testing setup and calibration of the equipment. Uncalibrated equipment can be expected to jam frequently.

*Source:* *New requirement.*

*Impact:* *Click here to add the Impact*

→ **5.3.4-C** Misfeed rate data collection

The test lab ***SHALL*** record the misfeed total and total ballot volume for each pertinent test execution, for each type of device.

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

"Type of device" refers to the different models of paper-based tabulators produced by the vendor.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

→ **5.3.4-D** Misfeed rate pass criteria

When operational testing is complete, the test lab ***SHALL*** calculate the misfeed total and total ballot volume accumulated across all pertinent tests. If analysis of the cumulative behavior across all pertinent tests indicates that the probability of the true misfeed rate being worse than the benchmark specified in Requirement III.6.8.4-C is greater than 90 % for any type of device, the verdict on conformity to Requirement III.6.8.4-C ***SHALL*** be Fail. Otherwise, the verdict ***SHALL*** be Pass.

*Applies to:* *Paper-based device ∧ Tabulator*

*Test Reference:* *Click here to add the Test Reference*

DISCUSSION

The total ballot volumes below which a given number of misfeeds indicates rejection, for values less than 22, are shown in Table 5-4.

*Source:* *Click here to add the Source*

*Impact:* *Click here to add the Impact*

| MISFEED TOTAL | TOTAL BALLOT VOLUME |
|---|---|
| 1 | 53 |
| 2 | 266 |
| 3 | 552 |
| 4 | 873 |
| 5 | 1217 |
| 6 | 1576 |
| 7 | 1948 |
| 8 | 2329 |
| 9 | 2717 |
| 10 | 3111 |
| 11 | 3511 |

| MISFEED TOTAL | TOTAL BALLOT VOLUME |
|---|---|
| 12 | 3915 |
| 13 | 4323 |
| 14 | 4735 |
| 15 | 5150 |
| 16 | 5568 |
| 17 | 5989 |
| 18 | 6411 |
| 19 | 6836 |
| 20 | 7263 |
| 21 | 7692 |

Table 5-4 Misfeed rate cutoff points

## 5.4 Usability (Performance-Based Testing)

This section is to be provided by HFP.

## 5.5 Open-Ended Vulnerability Testing

Vulnerability testing is an attempt to bypass or break the security of a system or a device. Like functional testing, vulnerability testing can falsify a general assertion (namely, that the system or device is secure) but it cannot verify the security (show that the system or device is secure in all cases). Vulnerability testing is also referred to as penetration testing. Vulnerability testing can be performed using a test suite or it can be open-ended. Open ended vulnerability testing involves the testing of a system or device using the experience and expertise of the tester; using the knowledge of system or device design and implementation; using the publicly available knowledge base of vulnerabilities in the system or device; using the publicly available knowledge base of vulnerabilities in similar system or device; using the publicly available knowledge base of vulnerabilities in similar and related technologies; and using the publicly available knowledge base of vulnerabilities generally found in hardware and software (e.g., buffer overflow, memory leaks, etc.)

6

# Draft VVSG Recommendations to the EAC

**May 2007 DRAFT**

**VOLUME 6:**

**REFERENCES**

REQUIREMENTS LISTINGS

# Volume 6: Bibliography and Summary of Requirements

**Voting Systems Standards and related publications**

[1] Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems, January 1990 edition with April 1990 revisions, in Voting System Standards, U.S. Government Printing Office, 1990.14 Available at http://josephhall.org/fec_vss_1990_pdf/1990_VSS.pdf.

[2] 2002 Voting Systems Standards, available from http://www.eac.gov/election_resources/vss.html.

[3] IEEE Draft Standard for the Evaluation of Voting Equipment, draft P1583/D5.3.2b, 2005-01-04. Unpublished.

[4] Voluntary Voting System Guidelines Version I Initial Report, 2005-05-09, available from http://vote.nist.gov/VVSGVol1&2.pdf.

[5] California Volume Reliability Testing Protocol rev. 2006-01-31, available from http://www.ss.ca.gov/elections/voting_systems/volume_test_protocol_final.pdf.

[6] 2005 Voluntary Voting System Guidelines, Version 1.0, 2006-03-06, available from http://www.eac.gov/vvsg_intro.htm.

[7] Stephen Berger, "VVSG Test Report Requirements," memorandum, 2006-06-08.

[8] U.S. Election Assistance Commission, Quick Start Management Guide for Ballot Preparation/Printing and Pre-Election Testing, 2006-10. Available at http://www.eac.gov/eac_qs_guides.htm.

[9] U.S. Election Assistance Commission, Quick Start Management Guide for Voting System Security, 2006-10. Available at http://www.eac.gov/eac_qs_guides.htm.

[10] U.S. Election Assistance Commission, Testing and Certification Program Manual, Version 1.0, 2006-12-05. Available at http://www.eac.gov/docs/Voting%20System%20Testing%20and%20Certification%20Program%20Manual--Final%20--120506.pdf.

**Modelling**

[11] UML 2.0 Superstructure Specification, 2004-10-08, http://doc.omg.org/ptc/2004-10-02.

[12] Philippe A. Martin, Petri Net Linear Form (PNLF), in "Using PIPE and Woflan (and the Petri Net Linear Form)," http://www.cit.gu.edu.au/~phmartin/wf/PIPE/, 2007-05-09.

**Development and testing**

[13] Abraham Wald, Sequential Analysis, John Wiley & Sons, 1947.

[14] Benjamin Epstein and Milton Sobel, "Sequential Life Tests in the Exponential Case," Annals of Mathematical Statistics, v. 26, n. 1, 1955-03, pp. 82-93.

[15] C. A. R. Hoare, "An Axiomatic Basis for Computer Programming," Communications of the ACM, v. 12, n. 10, 1969-10, pp. 576-580, 583.

[16] Boris Beizer, Software System Testing and Quality Assurance, Van Nostrand Reinhold Company, 1984.

[17] F. L. Morris and C. B. Jones, "An Early Program Proof by Alan Turing," IEEE Annals of the History of Computing, v. 6, n. 2, 1984-04, pp. 139-143.

[18] F. J. Redmill, Ed., Dependability of Critical Computer Systems 1, Elsevier Applied Science, London and New York, 1988.

[19] M. R. Moulding, "Designing for high integrity: the software fault tolerance approach," Section 3.4. In C. T. Sennett, ed., High-Integrity Software, Plenum Press, New York and London, 1989.

[20] Capability Maturity Model Integration, http://www.sei.cmu.edu/cmmi/, 2006-07.

[21] CERT® Coordination Center, Secure Coding homepage, http://www.cert.org/secure-coding/, 2006-07.

[22] Department of Homeland Security, Build Security In homepage, https://buildsecurityin.us-cert.gov/, 2006-07.

[23] Valgrind home page, http://valgrind.org/, 2006-07.

**NIST Special Publications**

[24] Fred R. Byers, Care and Handling of CDs and DVDs—A Guide for Librarians and Archivists, National Institute of Standards and Technology Special Publication 500-252, 2003-10, available from http://www.itl.nist.gov/div895/carefordisc/index.html.

[25] Recommended Security Controls for Federal Information Systems, National Institute of Standards and Technology Special Publication 800-53, 2005-02, available from http://csrc.nist.gov/publications/nistpubs/.

**ISO Standards and Technical Reports**

[QACM1] ISO 9000:2005 Quality management systems – Fundamentals and vocabulary. Available from ISO, http://www.iso.org/

[QACM2] ISO 9001:2000 Quality management systems – Requirements. Available from ISO, http://www.iso.org/

[QACM3] ISO 10007:2003 Quality management systems – Guidelines for configuration management. Available from ISO, http://www.iso.org/

[26] ISO/IEC 8652:1987, Programming languages—Ada. Superseded by [29].

[27] ISO/IEC 9899:1990, Programming languages—C. Superseded by [31].

[28] ISO 9706:1994, Information and documentation—Paper for documents—Requirements for permanence. Available from ISO, http://www.iso.org/.

[29] ISO/IEC 8652:1995, Information technology—Programming languages—Ada. Available from ISO, http://www.iso.org/.

[30] ISO/IEC 14882:1998, Programming languages—C++. Superseded by [34].

[31] ISO/IEC 9899:1999, Programming languages—C. Available from ISO, http://www.iso.org/.

[32] ISO/IEC TR 15942:2000, Information technology—Programming languages—Guide for the use of the Ada programming language in high integrity systems. Available from ISO, http://www.iso.org/.

[33] ISO 18921:2002, Imaging materials—Compact discs (CD-ROM)—Method for estimating the life expectancy based on the effects of temperature and relative humidity. Available from ISO, http://www.iso.org/.

[34] ISO/IEC 14882:2003, Programming languages—C++. Available from ISO, http://www.iso.org/.

[35] ISO/IEC 23270:2003, Information technology—C# language specification. Superseded by [38].

[36] ISO 8601:2004, Data elements and interchange formats—Information interchange—Representation of dates and times. Available from ISO, http://www.iso.org/.

[37] ISO 17000:2004, Conformity assessment—Vocabulary and general principles. Available from ISO, http://www.iso.org/.

[38] ISO/IEC 23270:2006, Information technology—Programming languages—C#. Available from ISO, http://www.iso.org/.

**IEEE Standards**

[39] IEEE/EIA 12207.1-1997, Industry implementation of International Standard ISO/IEC 12207:1995—(ISO/IEC 12207) standard for information technology—software life cycle processes—life cycle data. Available from IEEE, http://www.ieee.org/.

[40] IEEE Std 829-1998, IEEE standard for software test documentation. Available from IEEE, http://www.ieee.org/.

**MIL Standards and Handbooks**

[41] MIL-STD-1521B (USAF) Technical Reviews and Audits for Systems, Equipments [sic], and Computer Software, rev. 1985-12-19.

[42] MIL-HDBK-781A, Handbook for Reliability Test Methods, Plans, and Environments for Engineering, Development, Qualification, and Production, 1996-04-01.

**Requests for Proposals**

[43] Request for Proposals #108.6-03-001, North Dakota, 2003-10-31. Available from http://www.state.nd.us/hava/documents/docs/vsp-rfp-official.pdf, 2006-01-26.

[44] Solicitation #DG5502, Utah, 2004-07-09, available from http://purchasing.utah.gov/BidHeaders/8750.pdf, 2006-01-27.

[45] Request For Proposal #3443, Mississippi, 2005-04-28. Available from http://www.its.state.ms.us/rfps/3443.htm, 2006-07.

[46] Request For Proposal #08455, Kansas, 2005-05-16. Available from http://www.kssos.org/elections/05elec/Voting_Equipment_RFP.pdf, 2006-07.

**Miscellaneous**

[47] New Shorter Oxford English Dictionary, Clarendon Press, Oxford, 1993.

[48] Matt Pietrek, "A Crash Course on the Depths of Win32™ Structured Exception Handling," Microsoft Systems Journal, 1997-01. Available at http://www.microsoft.com/msj/0197/exception/exception.aspx.

[49] CEXCEPT (exception handling in C), software package, 2000. Available at http://cexcept.sourceforge.net/.

[50] 2004 Presidential General Election Review Lessons Learned, http://www.truevotemd.org/Resources/Lessons_Learned.pdf.

[51] MISRA-C:2004: Guidelines for the use of the C language in critical systems, MIRA Limited, U.K., 2004-10.

[52] The Java Language Specification, Third Edition, 2005. Available at http://java.sun.com/docs/books/jls/index.html.

[53] Paul Vick, The Microsoft® Visual Basic® Language Specification, Version 8.0, 2005. Available from Microsoft Download Center, http://go.microsoft.com/fwlink/?linkid=62990.

## EMC Bibliography

**Code of Federal Regulations**

[EMC 1] Title 47, Part 15, Rules and Regulations of the Federal Communications Commission, Radio Frequency Devices.

[EMC 2] Title 47, Part 68, Rules and Regulations of the Federal Communications Commission, Connection of Terminal Equipment to the Telephone Network

**ANSI Standards**

[EMC 3] ANSI C63.16:1993 American National Standard Guide for Electrostatic Discharge Test – Methodology and Criteria for Electronic Equipment. Available from ANSI, http://www.ansi.org/

[EMC 4] ANSI C84.1:2006 Electric Power Systems and Equipment—Voltage Ratings (60 Hertz). Available from ANSI, http://www.ansi.org/

[EMC 5] ANSI/TIA-968-A:2002 Technical Requirements for Connection of Terminal Equipment to the Telephone Network. Available from ANSI, http://www.ansi.org/

[EMC 6] CISPR 22 Ed. 5.2 b:2006 Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement. Available from ANSI, http://www.ansi.org/

[EMC 7] CISPR 24 Ed. 1.0 b:1997 Information technology equipment - Immunity characteristics - Limits and methods of measurement. Available from ANSI, http://www.ansi.org/

**IEEE Standards**

[EMC 8] IEEE Std. C62.41™:1991 Recommended Practice for Surge Voltages in Low-Voltage AC Power Circuits. Available from IEEE. http://www.ieee.org/

[EMC 9] IEEE Std. C62.41.1™:2002 IEEE Guide on the Surge Environment in Low-Voltage (1000 V and less) AC Power Circuits. Available from IEEE. http://www.ieee.org/

[EMC 10] IEEE Std. C62.41.2™:2002 IEEE Recommended Practice on Characterization of Surges in Low-Voltage (1000V and Less) AC Power Circuits. Available from IEEE. http://www.ieee.org/

[EMC 11] IEEE Std. C62.45™:2002 IEEE Recommended Practice on Surge Testing for Equipment Connected to Low-Voltage (1000V and Less) AC Power Circuits

[EMC 12] IEEE 100, The Authoritative Dictionary of IEEE Standard Terms, Seventh Edition. Available from IEEE, http://www.ieee.org/

[EMC 13] IEEE Std. 519™:1992 519-1992 IEEE Recommended Practices and Requirements for Harmonic Control in Electrical Power Systems. Available from IEEE. http://www.ieee.org/

[EMC 14] IEEE Std. 587™:1980 IEEE Guide for Surge Voltages in Low-Voltage AC Power Circuits. Available from IEEE. http://www.ieee.org/

[EMC 15] IEEE Std. 1100™ :2005 IEEE Recommended Practice for Powering and Grounding Electronic Equipment. Available from IEEE. http://www.ieee.org/

**ISO Standards and Technical Reports**

[EMC 16] ISO/IEC 61000-2-5:1995 Electromagnetic compatibility (EMC)- Part 2-5: Environment – Classification of electromagnetic environments . Available from ISO, http://www.iso.org/

[EMC 17] ISO/IEC 61000-4-2:2001 Electromagnetic compatibility (EMC)- Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test. Available from ISO, http://www.iso.org/

[EMC 18] ISO/IEC 61000-4-3:2006 Electromagnetic compatibility (EMC) - Part 4-3. Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test. Available from ISO, http://www.iso.org/

[EMC 19] ISO/IEC 61000-4-4:2004 Electromagnetic compatibility (EMC) - Part 4-3. Testing and measurement techniques – Electrical fast transient/burst immunity test. Available from ISO, http://www.iso.org/

[EMC 20] ISO/IEC 61000-4-6:2006 Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields. Available from ISO, http://www.iso.org/

[EMC 21] ISO/IEC 61000-4-12:2006 Electromagnetic compatibility (EMC) - Part 4-12: Testing and measurement techniques – Ring wave immunity test. Available from ISO, http://www.iso.org/

[EMC 22] ISO/IEC 61000-4-21:2003 Electromagnetic compatibility (EMC) - Part 4-21. Testing and measurement techniques - Reverberation chamber test methods. Available from ISO, http://www.iso.org/

**Miscellaneous**

[EMC 23] ITI (CBEMA) Curve, Information Technology Industry Council (ITI). Available from ITI, http://www.itic.org/

[EMC 24] T.E. Grebe, "Application of Distribution Systems Capacitor Banks and their Impact on Power Quality," IEEE Transactions IA-32, May-June 1996. Available from IEEE. http://www.ieee.org/

[EMC 25] T.S. Key and F.D. Martzloff, “Surging the Upside-Down House: Looking into Upsetting Reference Voltages,” PQA’94 Conference, Amsterdam, Netherlands, 1994. (Accessible on-line at the NIST-hosted SPD Anthology – Part 5, (http://www.eeel.nist.gov/817/pubs/spd-anthology/methods.html).

**NFPA Standards**

[EMC 26] National Electrical Code (NFPA 70):2005. Available from NFPA, http://www.nfpa.org/

**Telcordia Document**

[EMC 27] Telcordia GR-1089:2006, Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment. Available from Telcordia, http://telecom-info.telcordia.com/

**Underwriters Laboratories Standards**

[EMC 28] UL 943:2006, Standard for Safety for Ground-Fault Circuit-Interrupters. Available from UL, http://www.ul.com/

[EMC 29] UL 60950-1:2005, Information Technology Equipment – Safety – Part 1: General Requirements. Available from UL, http://www.ul.com/

**Notes**

[1] Visual Basic 8 does not support named block exit, but it does support specifying the kind of block (do loop, for loop, while loop, select, subroutine, function, etc.) from which to exit, which need not be the innermost block.

[2] Specific equipment and materials are identified in order to describe certain procedures. In no case does such identification imply recommendation or endorsement, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

[3] A prerequisite for device-level certification would be prescribing a system architecture so that the responsibilities of each device and the interfaces between those devices could be well-specified. Such prescription is undesirable. More importantly, even with a prescribed architecture, a device-level certification would provide no assurance that any particular system that included that component would function as specified. That assurance can only be obtained by evaluating the complete system in the configuration in which it is to be deployed.

[4] Portions of this section are derived from Section 5.6.2.2 of [3].

[5] This material is from an unapproved draft of a proposed IEEE Standard, P1583. As such, the material is subject to change in the final standard. Because this material is from an unapproved draft, the IEEE recommends that it not be utilized for any conformance/compliance purposes. It is used at your own risk.

[6] Portions of this section are derived from Sections 5.6.2.2 and 6.6.4.2 of [3].

[7] In mathematical jargon, the word domain would be more appropriate than range for input variables; however, "range checking" is the common programming jargon.

[8] These values are derived from category 3K3 of IEC 60721-3-3, which is described as, the product operating in a temperature-controlled enclosed location where the humidity is not controlled. Further, the product is not subject to condensed water or water from other sources.

[9] A compromised device could be programmed to give the correct answers during logic and accuracy testing but behave differently after polls are opened. This kind of fraud is detected and prevented through other means, beginning with the design review specified in Volume V Section 4.3 and Requirement III.5.1-A and continuing with setup validation and routine audits.

[10] The reasons that ranked order voting is not handled are discussed in Volume III Section 1.5.5.

[11] A system conforming to the Write-ins class is required to be capable of counting and reporting totals for all candidates that are written in by voters. In some states, write-in votes are not counted unless they exactly match one of a list of registered, accepted write-in candidates. Voting systems may support reporting options that meet the requirements of such states without disruption to the counting logic.

[12] The test lab may rely on media manufacturers' specifications for data retention or life expectancy if accelerated testing results are not available. See also [24], [28] and [33].

[13] Requirement III.5.6-A.3 and Requirement III.5.6-A.4 indicate acceptable designs.

[14] The 1990 Voting System Standards package also included "A Plan for Implementing the FEC Voting System Standards," "System Escrow Plan for the Voting System Standards Program," and "A Process for Evaluating Independent Test Authorities."

# Summary of Requirements

## Volume 1: VVSG Introduction

## Volume 5: Testing Standard

# Table of Figures

# Table of Tables