1

Draft VVSG Recommendations to the EAC

March 2007 DRAFT

VOLUME 1:

INTRODUCTION

OVERVIEW TO VOLUMES 2-5

VVSG Draft 20070306

March 6, 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 1: Guidelines Overview

Chapter 1: What Has Changed

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.

1.1 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.

2

Draft VVSG Recommendations to the EAC

March 2007 DRAFT

VOLUME 2:

TERMINOLOGY STANDARD

COMMON DEFINITIONS

Volume 2 Table of Contents

Volume 2: Terminology Standard

Chapter 1: Introduction

1.1 Background

The Voluntary Voting System 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 and protocols that test labs implement; and
- A terminology standard (Volume II) defining terms used in the foregoing.

1.2 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.

1.3 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 EAC national certification process;

- Software repositories designated by the EAC 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.

1.4 Description and Rationale of Significant Changes vs. [6]

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.

Chapter 2: Definitions

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.

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.

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

administrator: Role defined in Volume III Section 7.4.

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.

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.

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])

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 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.

EBM: (Electronically-assisted Ballot Marker) VEBD that produces an executed, human-readable paper ballot as a result. Note: The ballot output by an EBM may or may not include a bar code. 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. Vote-by-telephone systems that are in use at the time of this writing are EBMs. The voter uses an audio interface (remotely) and a paper ballot is produced (centrally).

EBP: (Electronic Ballot Printer) EBM that prints an entire ballot.

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: The EMS produces a printed report of the vote count and may produce a report stored on electronic media.

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.

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 system, 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.

failure rate: Ratio of the number of failures that occur to the number of voters served. "Voter volume" is a placeholder until the data necessary to define a credible benchmark have been collected.

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.

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.

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).

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

March 2007 DRAFT

VOLUME 3:

PRODUCT STANDARD

VOTING EQUIPMENT

Volume 3 Table of Contents

Volume 3: Product Standard

Chapter 1: Introduction

1.1 Background

The Voluntary Voting System 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 and protocols that test labs implement; and
- A terminology standard (Volume II) defining terms used in the foregoing.

1.2 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.

1.3 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 EAC national certification process;
- Software repositories designated by the EAC 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.

1.4 Description and Rationale of Significant Changes vs. [6]

1.4.1 Precision and testability

Throughout the Guidelines, requirements 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.

1.4.2 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.

1.4.3 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 benchmark for reliability has been changed from Mean Time Between Failure to a failure rate based on volume. Note also revision of benchmark based on data collected.

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, minor changes include

- Replaced accuracy requirements referring to specific, low-level operations with a single, general, end-to-end accuracy requirement.
- Made compatible with early voting.
- Lowered the benchmark rate of rejection for paper ballots that conform to all vendor specifications.
- 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 and moved them into supplemental guidance.
- Replaced the term ballot format, which was inherited from [1], with the term used in modern practice, ballot style.

1.4.4 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).

1.4.5 Coding conventions

1.4.5.1 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).

1.4.5.2 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 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).

1.4.6 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.

1.4.7 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 assertions for use in evaluating the correctness of voting system logic. Volume V Section 4.7 describes the verification procedure.

1.4.8 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.

1.5 Options Not Standardized

1.5.1 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.

1.5.2 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.

1.5.3 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.

1.5.4 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.

1.5.5 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.

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 EAC national certification process;
- Software repositories designated by the EAC 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 and protocols that test labs implement; and
- A terminology standard (Volume II) defining terms used in the foregoing.

2.2 Structure of Requirements

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"). Thus, requirements are nested.

Some requirements are directly testable and some are not. The latter tend to be higher-level and are included because (1) they are testable indirectly insofar as their lower-level requirements are testable, and (2) they often provide the structure and rationale for the lower-level requirements.

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* different requirements that apply to each listed class individually.

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*).

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."

Text using these keywords is 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.

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 *Vote-capture device*, *Paper-based device*, *Electronic device*, *Tabulator*, and all device voting variations (*In-person voting device*, etc.).
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 device	Electronic device that includes application logic. *Programmed 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*.
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

TERM	DEFINITION
	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. Note: The ballot output by an EBM may or may not include a bar code. 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. Vote-by-telephone systems that are in use at the time of this writing are EBMs. The voter uses an audio interface (remotely) and a paper ballot is produced (centrally). *EBM* subsumes *EBP*.
EBP	(Electronic Ballot Printer) EBM that prints an entire 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).
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. *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* and *PCOS*.
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.
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: The EMS produces a printed report of the vote count and may produce a report stored on electronic media.

Table 2 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 may not 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 may not 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 3 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.

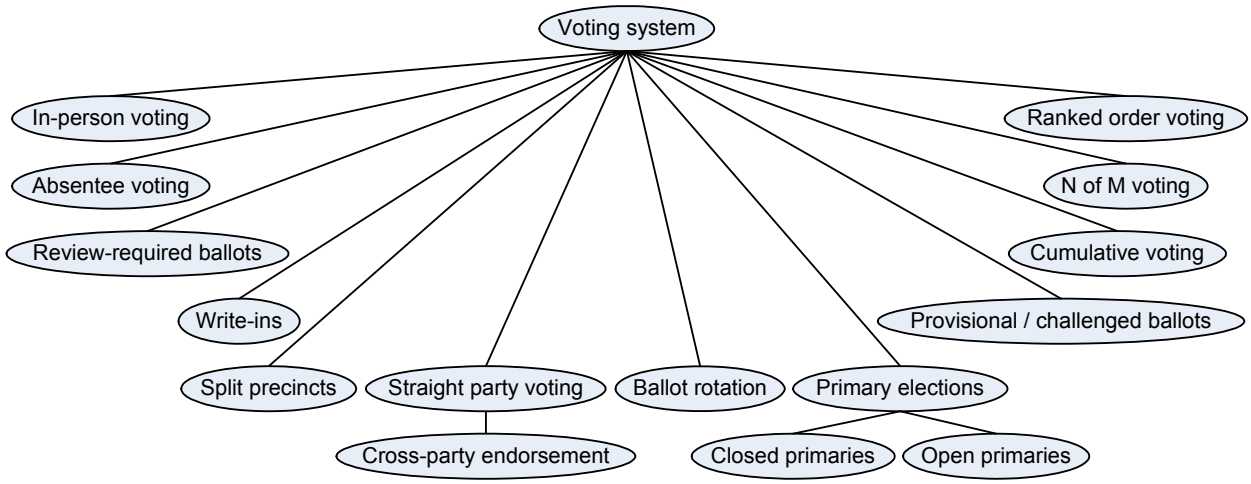

Figure 1 Voting system classes

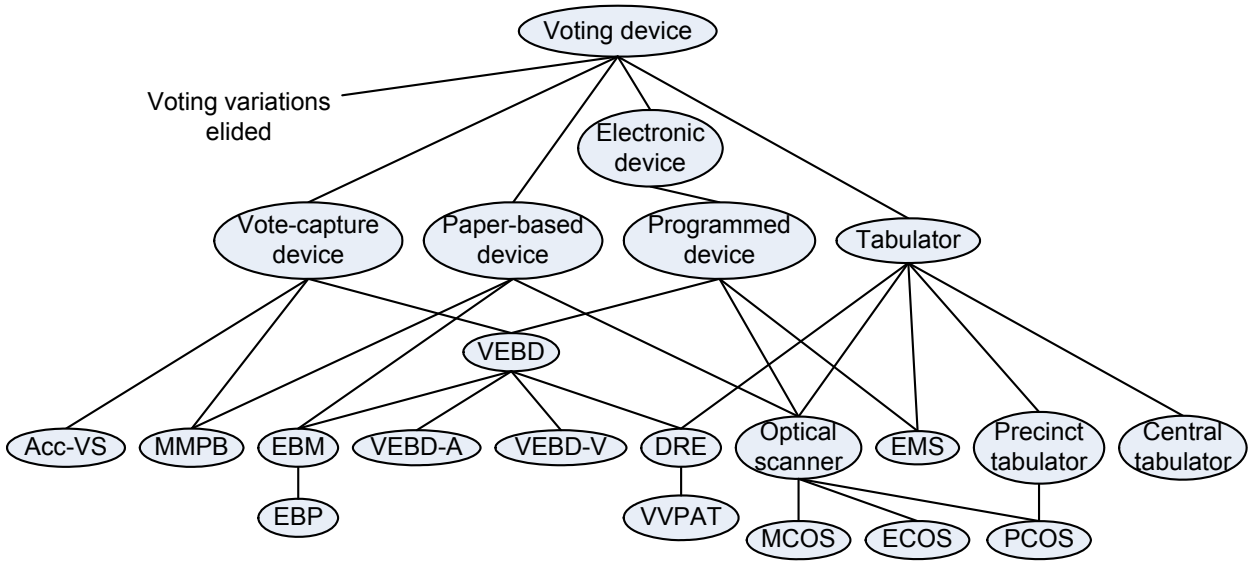

Figure 2 Voting device classes

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*

D I S C U S S I O N

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

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.

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.

- Vote-capture device
- Paper-based device

- Electronic device
  - Programmed device
- Tabulator
  - Precinct tabulator
  - Central tabulator

- 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. 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 may not contradict nor relax requirements that would otherwise apply to the system and its constituent devices.

Chapter 3: Security and Audit Architecture

Chapter 4: Cryptography

4.1 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.

4.1.1 General Cryptographic Implementation

➞ **4.1.1-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.*

➞ **4.1.1-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.*

4.1.2 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.

→ **4.1.2-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*

DISCUSSION

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.*

→ **4.1.2-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.*

↳ **4.1.2-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.*

↳ **4.1.2-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*

4.1.3 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.

4.1.3.1 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.

→ **4.1.3.1-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*

DISCUSSION

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*

→ **4.1.3.1-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*

DISCUSSION

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*

→ **4.1.3-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*

→ **4.1.3-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*

→ **4.1.3-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*

4.1.4 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.

→ **4.1.4-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*

DISCUSSION

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*

→ **4.1.4-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*

→ **4.1.4-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*

→ **4.1.4-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*

→ **4.1.4-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*

→ **4.1.4-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*

→ **4.1.4-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 5: Access Control

5.1 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.

5.2 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

5.2.1 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.

→ **5.2.1-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 System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

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.*

→ **5.2.1-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 System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

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.*

→ **5.2.1-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*

DISCUSSION

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.*

Table 1 Voting System States

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.

→ **5.2.1-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.*

→ **5.2.1-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.*

→ **5.2.1-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.*

→ **5.2.1-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.*

→ **5.2.1-H** Least privilege requirement

The voting system shall implement the least privilege principle for default access control permissions.

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 least privilege access control permissions.*

5.2.2 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.

→ **5.2.2-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*

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.*

→ **5.2.2-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.*

→ **5.2.2-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*

DISCUSSION

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.*

→ **5.2.2-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*

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.*

→ **5.2.2-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*

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.*

→ **5.2.2-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.*

→ **5.2.2-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.

5.2.3 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.

→ **5.2.3-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 System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

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.*

→ **4.2.3-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 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 (a)*

Impact: *This requirement extends VVSG 2005 Volume I, Section 7.2.1.1 (a) by requiring role-based methods to follow ANSI INCITS 359-2005.*

→ **5.2.3-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: *Vote-capture device*

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.*

→ **5.2.3-D** Group member identification requirement

Members within all groups except the voter group shall be identified individually and explicitly.

Applies to: *Vote-capture device*

Test Reference: *Volume V, Section 5.4*

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.*

Table 2 Voting System Groups/Roles and Descriptions

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.

→ **5.2.3-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 System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

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.*

Table 3 Roles and States Access Matrix

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

→ **5.2.3-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.*

5.2.4 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.

→ **5.2.4-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 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.*

→ **5.2.4-B** Multiple authentication mechanism requirement

The voting system shall provide multiple authentication methods to support multi-factor authentication.

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 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.*

→ **5.2.4-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 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 multi-factor authentication for the voting system administrator group or role.*

Table 4 Minimum Authentication Methods for Groups and Roles

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

→ **5.2.4-D** Prohibition of hard coded authentication data requirement

Voting system software shall not contain hard coded authentication data.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.4*

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.*

→ **5.2.4-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 System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

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.*

→ **5.2.4-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 System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

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.

→ **5.2.4-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 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.*

→ **5.2.4-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 5.1*

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.*

→ **5.2.4-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 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.*

→ **5.2.4-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 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.*

→ **5.2.4-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 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.*

→ **5.2.4-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 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.*

↳ **5.2.4-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 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.*

↳ **5.2.4-L.2** Common word usage for password configuration requirement

The voting system shall restrict the use of common words for passwords.

Applies to: *Voting 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.*

↳ **5.2.4-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 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 history.*

↳ **5.2.4-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 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 the use or usernames and related information in passwords.*

↳ **5.2.4-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 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 the expiration of unchanged passwords.*

↳ **5.2.4-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 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 advanced warning or password expiration to users.*

↳ **5.2.4-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 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 configuration of password expiration and warnings.*

→ **5.2.4-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*

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 including the use of security tokens and allowing the administrator group or role flexibility in configuring the security token.*

↳ **5.2.4-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*

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 mutual authentication of the security token and the voting device.*

↳ **5.2.4-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*

DISCUSSION

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.*

↳ **5.2.4-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.*

↳ **5.2.4-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.*

↳ **5.2.4-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: *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 7.2.1.2*

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.*

↳ **5.2.4-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*

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 use of security token functionality to casting or spoiling a vote.*

→ **5.2.4-N** Voter mutual authentication requirement

The voting system shall provide mutual authentication between the voter and the voting device.

Applies to: *Vote-capture device*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

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.*

5.2.5 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.

→ **5.2.5-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 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 restricting access to election data to authorized accounts.*

→ **5.2.5-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 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 separation of duty.*

→ **5.2.5-C** Dual person control requirement

The voting system shall provide dual person control for administrative activities.

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 (a) by requiring dual person control for administrative activities.*

→ **5.2.5-D** Explicit authorization requirement

The voting system shall explicitly authorize subjects' access based on access control lists or policies.

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 (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.*

→ **5.2.5-E** Explicit deny requirement

The voting system shall explicitly deny subjects access based on access control lists or policies.

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 (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.*

→ **5.2.5-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 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.*

→ **5.2.5-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 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.*

5.2.6 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.

→ **5.2.6-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.*

→ **5.2.6-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: *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 7.2.1.2*

Impact: *This requirement extends VVSG 2005 Volume I, Section 7.2.1.2 by restricting the accounts, groups, or roles that are accessed remotely.*

→ **5.2.6-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.*

→ **5.2.6-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: *Vote-capture device*

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.*

Chapter 6: System Event Logging

6.1 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

6.2 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.

6.2.1 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.

→ **6.2.1-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 5.3*

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.*

→ **6.2.1-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 5.4*

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 5.5.2*

Impact: *This requirement extends VVSG 2005 Volume I, Section 5.5.2 by requiring event log encryption and file integrity protection as part of the default settings.*

→ **6.2.1-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:

→ **6.2.1-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.*

↳ **6.2.1-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.*

↳ **6.2.1-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.*

↳ **6.2.1-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.*

↳ **6.2.1-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.*

↳ **6.2.1-D.5** Clock synchronization requirement

The voting system shall provide clock synchronization.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

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.*

↳ **6.2.1-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*

DISCUSSION

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.*

→ **6.2.1-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.

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.*

↳ **6.2.1-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
GENERAL VOTING SYSTEM	
Machine generated error and exception messages	Examples of machine generated error and exception messages include but are not limited to: ♦ The source and disposition of system interrupts resulting in entry into exception handling routines. ♦ Messages generated by exception handlers. ♦ The identification code and number of occurrences for each hardware and software error or failure. ♦ Notification of physical violations of security ♦ Other exception events such as power failures, failure of critical hardware components, data transmission errors or other types of operating anomalies.
Critical system status messages	Critical system status messages other than information messages displayed by the system during the course of normal operations. Examples of critical system status messages include but are not

	limited to: ♦ Diagnostic and status messages upon startup. ♦ The “zero totals” check conducted before opening the polling place or counting a precinct centrally. ♦ For paper-based systems, the initiation or termination of card reader and communications equipment operation. ♦ Printer errors.
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.
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.
Operating system shutdown and restarts	Both normal and abnormal operation system shutdowns and restarts.
Changes to system configuration settings	Configuration settings include registry keys, kernel parameters, logging settings, and other voting system parameters.
Integrity checks for executables, configuration files, data, and logs.	Integrity checks alert to possible tampering with files and data.
The addition, modification, and deletion of files.	Files that are added, modified, or deleted from the voting system.
System readiness results	System readiness results include at a minimum the following information: ♦ System pass or fail of hardware and software test for system readiness. ♦ Identification of the software release, identification of the election to be processed, polling place identification, and the results of the software and hardware diagnostic tests. ♦ Pass or fail of ballot style compatibility and integrity test. ♦ Pass or fail of system test data removal. ♦ Zero totals of data paths and memory locations for vote recording.
AUTHENTICATION AND ACCESS CONTROL	
Authentication related events	Authentication related events include, but are not limited to the following: ♦ Login/logoff events (both successful and failed attempts) ♦ Account lockout events

	♦ Password changes
Access control related events	Access Control related events include, but are not limited to the following: ♦ Use of privileges (such as a user running a process as an administrator) ♦ All access attempts to application and underlying system resources ♦ Changes to the access control configuration of the voting system.
User account and role (or groups) management activity	User account and role management activity includes, but is not limited to the following: ♦ Addition and deletion of user accounts and roles. ♦ User account and role suspension and reactivation ♦ Changes to account or role security attributes such as password length, access levels, login restrictions, permissions, etc. ♦ 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: ♦ 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. ♦ Changes to system parameters such as enabling and disabling services ♦ Starting and stopping application processes
Abnormal application exits	All abnormal application exits.
Application installations	All application installation.
Application and operating system patching	All patching to applications and the operating system.
Successful and failed database connection attempts (if a database is utilized).	All database connection attempts.
CRYPTOGRAPHIC FUNCTIONS	
Changes to cryptographic keys	At a minimum critical cryptographic settings include key addition, key removal, and re-keying.
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: ♦ The account name that made the modifications ♦ A description of what was modified including the file name, location, and the content changed ♦ The date and time of the modification.
Voting events	Voting events include: ♦ Canceling a vote during verification ♦ Fled voters ♦ Results of exporting logs to tabulation center.

Table1-5. Minimum Events to Log

6.2.2 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.

→ **6.2.2-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.*

↳ **6.2.2-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.*

↳ **6.2.2-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.*

➞ **6.2.2-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.*

6.2.3 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.

→ **6.2.3-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*

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 a suggested logging policy.*

→ **6.2.3-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.*

→ **6.2.3-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.*

→ **6.2.3-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.*

→ **6.2.3-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*

DISCUSSION

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.*

↳ **6.2.3-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*

DISCUSSION

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.*

→ **6.2.3-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.*

↳ **6.2.3-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.*

➞ **6.2.3-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.*

→ **6.2.3-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.*

→ **6.2.3-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.*

→ **6.2.3-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.*

➞ **6.2.3-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.*

➞ **6.2.3-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.*

➞ **6.2.3-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.*

6.2.4 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.

→ **6.2.4-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.*

→ **6.2.4-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.*

→ **6.2.4-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.*

6.2.5 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 7: Setup Validation

7.1 Introduction

This section provides requirements supporting the capability to verify that voting equipment is setup and configured properly for use in an election. The requirements support the inspection of the voting equipment to determine that: (a) only authorized EAC 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].

7.2 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, a discussion of the effects timing of the inspections has on the assurance provided to voting system equipment is included.

7.2.1 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 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, EAC, or other notary repositories can be used to determine if EAC or jurisdiction approved software has been modified. However, VSTLs, NSRL, EAC, and other notary repositories can only provide software reference information for the voting system software they receive from vendors, VSTLs, and jurisdictions. Election specific and installation dependant software used by jurisdictions could be provided to the VSTLs, NSRL, EAC, 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.

7.2.2 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 are dependant 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 before the voting equipment is used from documentation provided by vendors and jurisdictions. 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 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

[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.

registers or variables. A summation of the register or variable values can be compared to the record of the number of voter that used the voting equipment.

7.2.3 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.

7.2.4 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 worker) 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 have inspections performed 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.

7.3 Voting equipment setup validation requirements

7.3.1 Voting equipment setup validation process requirement

→ **7.3.1-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*

DISCUSSION

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*

→ **7.3.1-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 section7.3.2), registers and variables (See requirements in section7.3.3), 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*

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 (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.*

→ **7.3.1.1-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*

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*

7.3.2 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 election management systems and networked vote capture devices.

7.3.2.1 Software identification verification

→ **7.3.2.1-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 requirement7.**3.2.1-C**.*

DISCUSSION

This requirement provides the ability to identify if the proper software is installed and no other software is present on voting equipment. This requirement covers software stored on voting equipment with or without 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 software installed needs to be documented.*

→ **7.3.2.1-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 election management systems and networked vote capture devices 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.*

→ **7.3.2.1-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 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.*

→ **7.3.2.1-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.*

7.3.2.2 Software integrity verification

→ **7.3.2.2-A** Software integrity verification requirement

Voting equipment **shall** verify the integrity of software installed on storage devices using cryptographic software reference information from the EAC, NSRL, and State designated notary repositories.

Applies to: *Programmed device*

Test Reference: *Volume V, Section 5.2 (Functional Test)*

D I S C U S S I O N

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.*

→ **7.3.2.2-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)*

D I S C U S S I O N

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.*

→ **7.3.2.2-B.1** 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 requirement7.**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)(iii)*

Impact: *This requirement updates VVSG 2005 Volume I, Section 7.4.6 (b)(iii) with some word changes.*

→ **7.3.2.2-B.2** 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***

D I S C U S S I O N

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.*

→ **7.3.2.2-C** 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)*

D I S C U S S I O N

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 requirement7.**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 in7.**3.4**, and focusing the scope of the requirement from voting equipment to election management systems and networked vote capture devices.*

→ **7.3.2.2-C.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 requirement7.**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 to 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.*

→ **7.3.2.2-C.1** 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 to the VVSG 2005 Volume I Section 7.4.6 (e) by explicitly disallowing the 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.*

→ **7.3.2.2-C.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 read 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.*

→ **7.3.2.2-D** 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 requirement7.**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 needs to be documented.*

→ **7.3.2.2-E** Software reference information generation requirement

VSTLs, EAC, 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, EAC, 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*

→ **7.3.2.2-F** 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).*

➞ **7.3.2.2-G** 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.*

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.*

7.3.3 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 section7.2.2 for a discussion of register and variable characteristics and limitations of register and variable inspection.

➞ **7.3.3-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)*

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 (f)(ii)*

Impact: *This requirement updates VVSG 2005 Volume I, Section 7.4.6 (f)(ii) with some word changes*

→ **7.3.3-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)*

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 (f)(ii)*

Impact: *This requirement updates VVSG 2005 Volume I, Section 7.4.6 (f)(ii) with some word changes*

→ **7.3.3-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)*

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 (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*

→ **7.3.3-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 requirement7.**3.3-F***

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 (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 some*

→ **7.3.3-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)*

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: *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*

→ **7.3.3-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*

→ **7.3.3-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*

7.3.4 Voting equipment properties inspection requirements

→ **7.3.4-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*

→ 7.**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*

→ 7.**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)*

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*

→ 7.**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 requirement7.**3.4-B***

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.**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)*

D I S C U S S I O N

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*

→ 7.**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*

→ 7.**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 requirement7.**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*

→ 7.**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*

→ 7.**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*

→ 7.**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 requirement7.**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*

→ 7.**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)*

D I S C U S S I O N

For example, LEDs can also 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*

→ 7.**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)*

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*

→ 7.**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 requirement7.**3.4-K***

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.**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*

→ 7.**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*

→ 7.**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)*

D I S C U S S I O N

Requirement7.**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*

→ 7.**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 requirement7.**3.4-N***

D I S C U S S I O N

Requirement7.**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*

→ 7.**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)*

D I S C U S S I O N

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*

7.**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*

→ 7.**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

Requirement7.**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*

→ 7.**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 requirement7.**3.4-R***

D I S C U S S I O N

Requirement7.**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*

→ 7.**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

Requirement7.**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*

→ 7.**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 requirement7.**3.4-X***

D I S C U S S I O N

Requirement7.**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*

→ 7.**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*

→ 7.**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 is a generalization and extension of 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*

→ 7.**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 requirement7.**3.4-Y***

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.**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)*

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. 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 is a generalization 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*

→ 7.**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 Section7.3.4. This requirement provides a mechanism for the properties not covered in Section7.3.4 to be captured.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ 7.**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 Section7.3.4. This requirement provides a mechanism for the properties not covered in Section7.3.4 to be captured.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **7.3.4-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, name(s) of the individual(s) 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.*

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*

7.3.5 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 8: Software Distribution and Installation

Chapter 9: Physical Security

Chapter 10: System Integrity Management

Chapter 11: CRT General Requirements

11.1 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).

➞ **11.1-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*

➞ **11.1-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*

→ **11.1-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*

→ **11.1-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*

→ **11.1-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.*

→ **11.1-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."*

→ **11.1-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*

→ **11.1-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*

11.2 Voting Variations

The purpose of these formulaic requirements is to clarify that support for a given voting variation may not 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.

→ **11.2-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*

→ **11.2-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*

→ **11.2-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*

→ **11.2-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*

D I S C U S S I O N

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*

→ **11.2-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*

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*

→ **11.2-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*

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*

↳ **11.2-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*

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*

→ **11.2-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*

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*

→ **11.2-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*

↳ **11.2-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*

↳ **11.2-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*

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*

→ **11.2-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*

D I S C U S S I O N

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*

→ **11.2-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*

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*

→ **11.2-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*

→ **11.2-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*

11.3 Hardware and Software Performance, General Requirements

This section contains requirements for hardware and software performance:

1. Reliability;
2. Accuracy/error rate; and
3. Electrical/RF.

11.3.1 Reliability

11.3.1-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*

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.a / [6] I.4.3.1.a*

Impact: *Click here to add the Impact*

11.3.1-B Failure rate benchmark

All devices shall achieve a failure rate of no more than 10^{-4} (1 / 10 000).

Applies to: *Voting device*

Test Reference: *Volume V Section 5.3.2*

D I S C U S S I O N

The critical terms failure rate and failure are defined in Volume II.

Source: *Revised from [2] I.3.4.3 / [6] I.4.3.3*

Impact: *Click here to add the Impact*

11.3.1-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*

→ **11.3.1-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*

11.3.2 Accuracy/error rate

→ **11.3.2-A** Satisfy integrity constraints

All systems shall satisfy the assertions 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*

→ **11.3.2-B** End-to-end accuracy benchmark

All systems shall achieve a report total error rate of no more than 10^{-7} (1 / 10 000 000).

Applies to: *Voting system*

Test Reference: *Volume V Section 5.3.3*

D I S C U S S I O N

See Requirement V.5.3.3-B.

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.

11.3.3 Electrical/RF

To be supplied by AG.

11.4 Workmanship

This section contains requirements for voting system materials, and for good design and construction workmanship for software and hardware:

1. Software engineering practices;
2. Quality assurance and configuration management;
3. General build quality;
4. Durability;
5. Security and audit architectural requirements;
6. Maintainability;
7. Temperature and humidity; and
8. Equipment transportation and storage.

11.4.1 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.

11.4.1.1 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.

11.4.1.2 Selection of programming languages

→ **11.4.1.2-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*

↳ **11.4.1.2-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*

11.4.1.3 Selection of general coding conventions

→ **11.4.1.3-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*

DISCUSSION

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*

↳ **11.4.1.3-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*

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.

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*

↳ **11.4.1.3-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*

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.

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*

11.4.1.4 Software modularity and programming

➞ **11.4.1.4-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.*

↳ **11.4.1.4-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*

➞ **11.4.1.4-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*

↳ **11.4.1.4-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*

DISCUSSION

"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.*

↳ **11.4.1.4-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

11.4.1.5 Structured programming

➞ **11.4.1.5-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*

DISCUSSION

See Volume III Section 1.4.5.2.

Source: *Extension of [6] requirements for structured programming.*

Impact: *Click here to add the Impact*

↳ **11.4.1.5-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*

→ **11.4.1.5-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*

↳ **11.4.1.5-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*

↳ **11.4.1.5-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" may not 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*

↳ **11.4.1.5-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*

➞ **11.4.1.5-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*

11.4.1.6 Comments

➞ **11.4.1.6-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*

DISCUSSION

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.*

11.4.1.7 Executable code and data integrity[4,5]

➞ **11.4.1.7-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*

↳ **11.4.1.7-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.*

↳ **11.4.1.7-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").*

↳ **11.4.1.7-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.*

↳ **11.4.1.7-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*

↳ **11.4.1.7-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).

→ **11.4.1.7-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*

→ **11.4.1.7-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*

➞ **11.4.1.7-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*

11.4.1.8 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].

➞ **11.4.1.8-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*

↳ **11.4.1.8-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*

➞ **11.4.1.8-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. 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).*

↳ **11.4.1.8-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."*

↳ **11.4.1.8-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*

D I S C U S S I O N

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*

↳ **11.4.1.8-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*

D I S C U S S I O N

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*

↳ **11.4.1.8-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*

D I S C U S S I O N

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*

➞ **11.4.1.8-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*

↳ **11.4.1.8-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.*

↳ **11.4.1.8-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.*

→ **11.4.1.8-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*

➞ **11.4.1.8-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*

➞ **11.4.1.8-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*

→ **11.4.1.8-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*

→ **11.4.1.8-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*

→ **11.4.1.8-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.*

→ **11.4.1.8-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*

DISCUSSION

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*

11.4.1.9 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.

→ **11.4.1.9-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Extrapolated from [2] I.2.2.3.*

Impact: *Click here to add the Impact*

→ **11.4.1.9-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*

→ **11.4.1.9-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*

→ **11.4.1.9-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*

↳ **11.4.1.9-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.*

↳ **11.4.1.9-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*

→ **11.4.1.9-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*

11.4.2 Quality assurance and configuration management

This section is to be provided by AG. See Max Etschmaier, "Voting Machines: Draft Requirements for Quality and Configuration Management."

11.4.3 General build quality

→ **11.4.3-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*

↳ **11.4.3-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*

D I S C U S S I O N

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*

↳ **11.4.3-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*

D I S C U S S I O N

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*

➞ **11.4.3-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*

D I S C U S S I O N

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*

11.4.4 Durability

→ **11.4.4-A** Durability

Voting systems shall be designed to withstand normal use without deterioration and without excessive maintenance cost 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

AG action item: Is the ten years benchmark still appropriate? If so, is it testable (with accelerated aging) or verifiable with an expert design review? If so, still need testable language for "excessive maintenance cost" or informative text addressing the issue.

Source: *[2] I.3.4.2 / [6] I.4.3.2*

Impact: *Click here to add the Impact*

11.4.5 Security and audit architectural requirements

This section is to be provided by STS.

11.4.6 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.

→ **11.4.6-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*

→ **11.4.6-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. A non-technician to easily perform database updates;
4. Easy access to components for replacement;
5. Easy adjustment, alignment, and tuning of components; and
6. 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

AG action item: fix database updates; need performance measures and appropriate usability tests to assess "easy" and "easily;" need input from HFP; need a quantification of "low" in f), or informative text addressing the issue.

Source: *[2] I.3.4.4.2 / [6] I.4.3.4.2*

Impact: *Click here to add the Impact*

→ **11.4.6-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.*

11.4.7 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.

→ **11.4.7-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.

11.4.8 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.

→ **11.4.8-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*

D I S C U S S I O N

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*

→ **11.4.8-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*

D I S C U S S I O N

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*

→ **11.4.8-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*

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*

↳ **11.4.8-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*

→ **11.4.8-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*

↳ **11.4.8-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."*

↳ **11.4.8-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*

↳ **11.4.8-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*

↳ **11.4.8-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*

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.d*

Impact: *Click here to add the Impact*

11.5 Archival Requirements

11.5.1 Archivalness of media

→ **11.5.1-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*

D I S C U S S I O N

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*

11.5.2 Procedures required for correct system functioning

→ **11.5.2-A** Statutory period of retention

All printed copy records produced by the election database and ballot processing systems shall be labeled and archived for a period of at least 22 months after the 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

See also Requirement III.5.5.1-A and Volume III Section 5.5.3.

Source: *Reworded from [2] I.2.2.11.*

Impact: *Click here to add the Impact*

11.5.3 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.

11.6 Interoperability

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.

The ability to export voting data in a transparent format increases the chances that integration with another system is possible, but in and of itself it guarantees neither interoperability nor integratability with any particular system.

See also [6] I.C.3.2 (data formats for token objects) and Resolution #23-05 (Common Ballot Format Specifications).

→ **11.6-A** Interoperability

All systems shall maximize interoperability and 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*

↳ **11.6-A.1** Interoperability of election programming data and report data

All Election Management Systems shall maximize interoperability and 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*

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*

↳ **11.6-A.2** Interoperability of ballot image data

All DREs shall maximize interoperability and integratability with respect to ballot image data.

Applies to: *DRE*

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*

↳ **11.6-A.3** Interoperability through open export

The interoperability and 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*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Generalized from [2] II.6.3.b and TGDC Resolution #23-05.*

Impact: *Click here to add the Impact*

↳ **11.6-A.4** Interoperability through open database

The interoperability and 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 12: Usability and Accessibility Requirements

12.1 Overview

[[Convention for embedded comments: they are enclosed in double brackets. These remarks and questions are directed to the TGDC and its HFP subcommittee.]]

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.

12.1.1 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 is to 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.

12.1.2 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".
- **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.

12.1.3 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.

12.2 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.

12.2.1 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.

12.2.1.1 Overall Performance Metrics

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

→ **12.2.1.1-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 device*

Test Reference: *Performance*

DISCUSSION

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

→ **12.2.1.1-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 device*

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.

➞ **12.2.1.1-C** Overall Satisfaction

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

Applies to: *Voting device*

Test Reference: *Performance*

D I S C U S S I O N

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

[[Are we keeping this or dropping it? – Question is whether it's worth the trouble of separate testing.]]

➞ **12.2.1.1-D** Support for Independent Voting

No more than XXX% of subjects shall request external assistance in the process of executing and casting their ballots, as measured by the NIST VPP.

Applies to: *Voting device*

Test Reference: *Performance*

D I S C U S S I O N

The voting system should provide clear instructions and assistance so as to allow voters to successfully execute and cast their ballots independently. Voters should not routinely need to ask for human assistance.

12.2.1.2 Vendor Testing

➞ **12.2.1.2-A** Usability Testing by Vendor

The vendor shall conduct summative usability tests on the voting system using individuals representative of the general population. The vendor shall document the testing performed and report the test results using the Common Industry Format. [[There are plans for a more specific version of the CIF targeted towards voting. If this comes about, it will be referred to here.]] This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

Applies to: *Voting device*

Test Reference: *Inspection*

D I S C U S S I O N

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.

12.2.2 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).

→ **12.2.2-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.

→ **12.2.2-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 device*

Test Reference: *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

→ **12.2.2-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 device*

Test Reference: *Functional*

DISCUSSION

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.

12.2.2.1 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.

→ **12.2.2.1-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*

DISCUSSION

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.

→ **12.2.2.1-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 (e.g., undervotes).

Applies to: *VEBD*

Test Reference: *Functional*

D I S C U S S I O N

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

→ **12.2.2.1-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

→ **12.2.2.1-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*

D I S C U S S I O N

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.

→ **12.2.2.1-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*

D I S C U S S I O N

For example, the voter should not be forced to proceed sequentially through all the contests before going back to check his or her selection for a previous contest.

12.2.2.2 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.

➞ **12.2.2.2-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

➞ **12.2.2.2-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

➞ **12.2.2.2-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*

D I S C U S S I O N

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.

[[Here is the new clarifying requirement - I believe this is what was intended all along, but needed to be more explicit.]]

→ **12.2.2.2-D** Ballot Correction or Submission Following Notification

After the voting system has notified the voter that an anomalous 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*

D I S C U S S I O N

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).

→ **12.2.2.2-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*

D I S C U S S I O N

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.

12.2.3 Cognitive Issues

The features specified in this section are intended to minimize cognitive difficulties for the voter. The voter should always be able to operate the voting system and understand the effect of his/her actions.

→ **12.2.3-A** Completeness of Instructions

The voting system shall provide instructions for all its valid operations.

Applies to: *Voting device*

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.

→ **12.2.3-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 device*

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.

→ **12.2.3-C** Plain Language

All instructional material for the voter shall conform to certain accepted norms and best practices for plain language.

Applies to: *Voting device*

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.

↳ **12.2.3-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 device*

Test Reference: *Functional*

DISCUSSION

In case of an equipment failure, the only action available to the voter might be to get assistance from a poll worker.

↳ **12.2.3-C.2** Context before Action

Within conditional instructions, the conditions should be stated first, and then the action to be performed.

Applies to: *Voting device*

Test Reference: *Functional*

DISCUSSION

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

↳ **12.2.3-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 device*

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 ..."

↳ **12.2.3-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 device*

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.

↳ **12.2.3-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 device*

Test Reference: *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

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

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

Applies to: *Voting device*

Test Reference: *Functional*

D I S C U S S I O N

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

↳ **12.2.3-C.7** Gender-based Pronouns

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

Applies to: *Voting device*

Test Reference: *Functional*

D I S C U S S I O N

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

➞ **12.2.3-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 device*

Test Reference: *Inspection*

D I S C U S S I O N

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.

➞ **12.2.3-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 device*

Test Reference: *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

↳ **12.2.3-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 device*

Test Reference: *Functional*

D I S C U S S I O N

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.

↳ **12.2.3-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 device*

Test Reference: *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

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

There shall be a consistent relationship between the name of a candidate and the mechanism used to vote for that candidate.

Applies to: *Voting device*

Test Reference: *Functional*

D I S C U S S I O N

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'.

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

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

Applies to: *Voting device*

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. This is especially important for VEBD type systems.

→ **12.2.3-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 device*

Test Reference: *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

→ **12.2.3-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.

12.2.4 Perceptual Issues

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

→ **12.2.4-A** Screen Flicker

No voting machine display screen shall flicker with a frequency between 2 Hz and 55 Hz.

Applies to: *VEBD-V*

Test Reference: *Inspection*

DISCUSSION

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

→ **12.2.4-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.

Applies to: *Voting device*

Test Reference: *Functional*

DISCUSSION

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

→ **12.2.4-C** Ability to Reset to Default Values

If any aspect of a voting machine 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 device*

Test Reference: *Functional*

DISCUSSION

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

→ **12.2.4-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 the voter.

Applies to: *Voting device*

Test Reference: *Functional*

DISCUSSION

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

[[Two issues: 1) what about the wording for "continuous adjustability"? 2) now that this is mandatory for all screen-based systems, should we drop the Acc-VS req as redundant?]]

→ **12.2.4-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

[[dropping: Note that the corresponding requirement for the accessible voting station is mandatory.]] All millimeters will be calculated using Hard Metric Conversion. (See Glossary for definition.)

→ **12.2.4-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

Experimentation has shown that users prefer such fonts.

→ **12.2.4-G** Legibility of Paper Ballots

All voting machines using paper ballots should make provisions for voters with poor reading vision.

Applies to: *Paper-based device*

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 a magnifying device.

[[No consensus yet on whether or how to change this.]]

→ **12.2.4-H** Visual Access to VVPAT

When the voting system asks a voter to compare two distinct records of his/her vote (as in VVPAT systems), both records shall be positioned so as to be easily viewable and legible from the same posture.

Applies to: *VVPAT*

Test Reference: *Functional*

D I S C U S S I O N

For instance, the voter should not have to swivel from side to side as he/she compares records.

→ **12.2.4-I** Contrast Ratio

The minimum figure-to-ground ambient contrast ratio for all text and informational graphics (including icons) intended for the voter 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

→ **12.2.4-J** 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

[[Dropped: Note that the corresponding requirement for the accessible voting station is mandatory.]]

➞ **12.2.4-K** Accommodation for Color Blindness

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

Applies to: *Voting device*

Test Reference: *Inspection*

D I S C U S S I O N

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.

➞ **12.2.4-L** 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 device*

Test Reference: *Functional*

D I S C U S S I O N

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.

12.2.5 Interaction Issues

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

➞ **12.2.5-A** No Page Scrolling

Voting machines 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."

→ **12.2.5-B** Unambiguous Feedback for Voter's Selection

The voting machine 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 device*

Test Reference: *Functional*

DISCUSSION

Click here and type the discussion about this requirement

→ **12.2.5-C** Accidental Activation

Input mechanisms shall be designed to minimize accidental activation.

Applies to: *Voting device*

Test Reference: *Functional*

DISCUSSION

Click here and type the discussion about this requirement

↳ **12.2.5-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*

DISCUSSION

Click here and type the discussion about this requirement

↳ **12.2.5-C.2** No Repeating Keys

No key or control on a voting machine 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.

12.2.5.1 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.

→ **12.2.5.1-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 apprehend 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.

→ **12.2.5.1-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 paint an "X" next to the candidate's name, and an audio system might announce "You have voted for Smith for Governor".

→ **12.2.5.1-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 shall never take more than 10 seconds. In the case of audio systems, no upper limit is specified, since certain operations, such as reading out all the candidates running in a contest, may take a long time.

→ **12.2.5.1-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*

DISCUSSION

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).

→ **12.2.5.1-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 2 and 5 minutes.

Applies to: *VEBD*

Test Reference: *Functional*

DISCUSSION

Each type of system must have a given inactivity time that is consistent for all voting sessions.

→ **12.2.5.1-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

12.2.6 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 expected that jurisdictions will apply additional requirements appropriate for their particular circumstances for procurement and deployment.

➞ **12.2.6-A** General Support for Alternative Languages

The voting system shall be capable of presenting the ballot, ballot selections, review screens and instructions in any language declared by the vendor to be supported by the system.

Applies to: *Voting device*

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.

[[NEW:]]

↳ **12.2.6-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.

↳ **12.2.6-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 VVPAT information) shall also be presented when an alternative language is being used, whether the language is written or spoken.

Applies to: *Voting device*

Test Reference: *Functional*

DISCUSSION

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.

↳ **12.2.6-A.3** Usability Testing for Alternative Language

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. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

Applies to: *Voting device*

Test Reference: *Inspection*

DISCUSSION

Click here and type the discussion about this requirement

12.2.7 Privacy

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.

12.2.7.1 Privacy at the Polls

→ **12.2.7.1-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 device*

Test Reference: *Functional*

DISCUSSION

Click here and type the discussion about this requirement

↳ **12.2.7.1-A.1** Visual Privacy

The ballot and any input controls shall be visible only to the voter during the voting session and ballot submission.

Applies to: *Voting device*

Test Reference: *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

↳ **12.2.7.1-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.

↳ **12.2.7.1-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 device*

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.

↳ **12.2.7.1-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 device*

Test Reference: *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

12.2.7.2 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.

→ **12.2.7.2-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 device*

Test Reference: *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

→ **12.2.7.2-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 device*

Test Reference: *Functional*

D I S C U S S I O N

Click here and type the discussion about this requirement

12.2.8 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.

12.2.8.1 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.

→ **12.2.8.1-A** Ease of Normal Operation

Procedures for system setup, polling, and shutdown shall be reasonably easy for the typical poll worker to learn, understand, and perform.

Applies to: *Voting device*

Test Reference: *Functional*

DISCUSSION

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.

→ **12.2.8.1-B** Usability Testing by Vendor

The vendor shall conduct summative usability tests on the voting system using individuals representative of the general population. The tasks to be covered in the test shall include setup, operation, and shutdown. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

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

12.2.8.2 Maintenance

Maintainability represents the ease with which maintenance actions can be performed based on the design characteristics of equipment and software and 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 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 shall 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.

→ **12.2.8.2-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

→ **12.2.8.2-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 device*

Test Reference: *Inspection*

D I S C U S S I O N

Click here and type the discussion about this requirement

12.2.8.3 Safety

[[This section has been somewhat updated. The listing of specific hazards has been moved from a supplementary requirement to the following introductory section and the basic safety requirement now refers to the underlying technical UL standard, instead of to the broader OSHA standard, which governs workplace inspections.]]

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

→ **12.2.8.3-A** Compliance with Federal Regulations

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 device*

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.

12.3 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 whose disabilities are so severe that they will need personal assistance. Nonetheless, these requirements are meant to make the voting system independently accessible to as many voters as possible. These requirements are *in addition* to those described in Subsection 3.2 XREF which generally apply to the Acc-VS.

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.

12.3.1 General

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

→ **12.3.1-A** 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*

D I S C U S S I O N

Click here and type the discussion about this requirement

→ **12.3.1-B** No Dependence on 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*

D I S C U S S I O N

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 obviate the need for a voter's ordinary non-interfacing devices, such as eyeglasses or canes.

→ **12.3.1-C** 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*

D I S C U S S I O N

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

[[JC: The following is the draft of a new proposed requirement to address accessibility and verification.]]

→ **12.3.1-D** 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 should provide a mechanism that can read that record and generate an audio representation of its contents. The use of this mechanism should be accessible to voters with dexterity disabilities.

Applies to: *Acc-VS*

Test Reference: *Functional*

DISCUSSION

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.

12.3.2 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 selection of color combinations that are 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.

→ **12.3.2-A** Usability Testing by Vendor

The vendor shall conduct summative usability tests on the voting system using partially sighted individuals. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

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

[[Redundant, given the new general req?]]

→ **12.3.2-B** Available Font Sizes for Accessible Display

Accessible voting stations that use 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: *Acc-VS*

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.

[[Redundant, given the new general req?]]

→ **12.3.2-C** High Contrast for Accessible Display

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

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

→ **12.3.2-D** 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*

D I S C U S S I O N

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.

→ **12.3.2-E** 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*

D I S C U S S I O N

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

→ **12.3.2-F** 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. [[Here is the "continuous adjustability" option:]] 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.

12.3.3 Blindness

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

→ **12.3.3-A** Usability Testing by Vendor

The vendor shall conduct summative usability tests on the voting system using individuals who are blind. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

Applies to: *Acc-VS*

Test Reference: *Inspection*

DISCUSSION

Click here and type the discussion about this requirement

→ **12.3.3-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

↳ **12.3.3-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.

↳ **12.3.3-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.

↳ **12.3.3-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.

↳ **12.3.3-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.

↳ **12.3.3-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").

→ **12.3.3-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 machine audio output, not just to the ATI of an accessible voting station.

↳ **12.3.3-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

↳ **12.3.3-C.2** T-coil Coupling

When a voting machine 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*

D I S C U S S I O N

Click here and type the discussion about this requirement

↳ **12.3.3-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*

D I S C U S S I O N

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

↳ **12.3.3-C.4** Initial Volume

The voting machine shall set the initial volume for each voting session between 40 and 50 dB SPL.

Applies to: *VEBD-A*

Test Reference: *Functional*

D I S C U S S I O N

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".

↳ **12.3.3-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

↳ **12.3.3-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

Click here and type the discussion about this requirement

↳ **12.3.3-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*

DISCUSSION

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.

↳ **12.3.3-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*

DISCUSSION

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

→ **12.3.3-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*

DISCUSSION

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

→ **12.3.3-E** Ballot Submission

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

Applies to: *Acc-VS*

Test Reference: *Functional*

DISCUSSION

For example, if voters using this station normally feed their own optical scan ballots into a reader, blind voters should also be able to do so.

→ **12.3.3-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*

DISCUSSION

Click here and type the discussion about this requirement

→ **12.3.3-G** Discernability of Key Status

On an accessible voting station, the status of all locking or toggle controls or keys (such as the "shift" key) shall be visually discernible, and discernible either through touch or sound.

Applies to: *Acc-VS*

Test Reference: *Functional*

DISCUSSION

Click here and type the discussion about this requirement

12.3.4 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.

→ **12.3.4-A** Usability Testing by Vendor

The vendor shall conduct summative usability tests on the voting system using individuals lacking fine motor control. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

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

→ **12.3.4-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*

D I S C U S S I O N

This requirement ensures that the accessible voting station is operable by individuals who do not have the use of their hands. An example of non-manual control would be a "sip and puff" switch. 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.

→ **12.3.4-C** Ballot Submission

If the voting station supports ballot submission 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 this submission.

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

→ **12.3.4-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*

D I S C U S S I O N

Controls are to be operable without excessive force.

→ **12.3.4-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*

D I S C U S S I O N

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

12.3.5 Mobility

These requirements specify the features of the accessible voting station designed to assist voters who use mobility aids, including wheelchairs.

→ **12.3.5-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*

D I S C U S S I O N

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.

→ **12.3.5-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*

D I S C U S S I O N

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

→ **12.3.5-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 machine 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*

D I S C U S S I O N

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.

12.3.5.1 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.

→ **12.3.5.1-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

➞ **12.3.5.1-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

↳ **12.3.5.1-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

↳ **12.3.5.1-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

↳ **12.3.5.1-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

↳ **12.3.5.1-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

→ **12.3.5.1-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

→ **12.3.5.1-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.

↳ **12.3.5.1-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

↳ **12.3.5.1-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.]]

12.3.6 Hearing

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

➞ **12.3.6-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.

➞ **12.3.6-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*

D I S C U S S I O N

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.

→ **12.3.6-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.

12.3.7 Cognition

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

→ **12.3.7-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.

12.3.8 English Proficiency

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

→ **12.3.8-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

12.3.9 Speech

→ **12.3.9-A** Speech not to be Required by Equipment

No voting equipment shall require voter speech for its operation.

Applies to: *Voting device*

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 13: Requirements by Voting Activity

13.1 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.

→ **13.1-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*

↳ **13.1-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*

→ **13.1-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*

→ **13.1-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*

→ **13.1-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*

↳ **13.1-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*

↳ **13.1-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*

↳ **13.1-D.3** EMS, indicate party endorsements

In all systems, the Election Management System shall allow the definition of political parties and the indication of the political parties (if any) that endorsed 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*

↳ **13.1-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*

↳ **13.1-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.*

↳ **13.1-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*

↳ **13.1-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*

↳ **13.1-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*

↳ **13.1-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*

↳ **13.1-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*

↳ **13.1-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*

→ **13.1-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."*

→ **13.1-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*

→ **13.1-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*

➞ **13.1-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*

13.2 Ballot Preparation, Formatting, and Production

➞ **13.2-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*

↳ **13.2-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*

↳ **13.2-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*

↳ **13.2-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*

↳ **13.2-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*

↳ **13.2-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*

↳ **13.2-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*

↳ **13.2-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*

↳ **13.2-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*

13.2-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*

13.2-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*

13.2-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*

➞ **13.2-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*

13.2.1 Procedures required for correct system functioning

See [8] for details.

➞ **13.2.1-A** Paper ballot production

Central election officials shall verify that paper ballots are produced in accordance with vendor specifications.

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*

↳ **13.2-A.1** Paper ballot production quality

Central election officials shall 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.

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.2.3.1.3.1.c.*

Impact: *Click here to add the Impact*

↳ **13.2-A.2** Paper ballot field alignment

Central election officials shall ensure that the vote response fields can be properly aligned with respect to any ballot marking devices 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: *[2] I.2.3.1.1.2.b.*

Impact: *Click here to add the Impact*

↳ **13.2-A.3** Paper ballot timing mark alignment

Central election officials shall ensure that timing marks align properly with the vote response fields.

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.2.3.1.1.2.c.*

Impact: *Click here to add the Impact*

13.3 Equipment Preparation

This section is to be provided by STS.

13.4 Equipment Setup for Security and Integrity

13.4.1 Setup for end-to-end cryptographic systems

This section is to be provided by STS.

13.4.2 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.

→ **13.4.2-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.

→ **13.4-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*

→ **13.4.2-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*

→ **13.4.2-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*

DISCUSSION

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*

→ **13.4.2-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*

DISCUSSION

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*

→ **13.4.2-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*

DISCUSSION

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*

→ **13.4.2-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*

→ **13.4.2-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.*

→ **13.4.2-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*

→ **13.4.2-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.*

↳ **13.4.2-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*

13.4.3 Setup validation

This section is to be provided by STS.

13.4.4 Procedures required for correct system functioning

See [8] and [9].

13.5 Opening Polls

13.5-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*

13.5-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*

13.5-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*

→ **13.5-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*

→ **13.5-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*

↳ **13.5-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*

↳ **13.5-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*

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.b.*

Impact: *Click here to add the Impact*

↳ **13.5-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*

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.c.*

Impact: *Click here to add the Impact*

13.6 Casting

These functional capabilities include all operations conducted at the polling place by voters and officials while polls are open.

13.6.1 Ballot activation

→ **13.6.1-A** DRE and EBP, ballot activation

DREs and EBPs shall support ballot activation.

Applies to: *DRE, EBP*

Test Reference: *Volume V Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *[2] I.2.4.*

Impact: *Click here to add the Impact*

↳ **13.6.1-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*

→ **13.6.1-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.6.7-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*

↳ **13.6.1-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *[2] I.2.4.2.g.*

Impact: *Click here to add the Impact*

↳ **13.6.1-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *[2] I.2.4.2.h.*

Impact: *Click here to add the Impact*

↳ **13.6.1-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*

↳ **13.6.1-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *New requirement.*

Impact: *Click here to add the Impact*

13.6.2 General voting functionality

➞ **13.6.2-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*

→ **13.6.2-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*

13.6.3 Voting variations

→ **13.6.3-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*

↳ **13.6.3-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*

↳ **13.6.3-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*

↳ **13.6.3-A.3** Vote-capture device, indicate party endorsements

All vote-capture devices shall be capable of indicating the political parties (if any) that endorsed 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*

↳ **13.6.3-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*

↳ **13.6.3-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*

↳ **13.6.3-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.*

↳ **13.6.3-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*

↳ **13.6.3-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*

↳ **13.6.3-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*

↳ **13.6.3-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*

↳ **13.6.3-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*

↳ **13.6.3-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*

↳ **13.6.3-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*

↳ **13.6.3-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*

↳ **13.6.3-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*

↳ **13.6.3-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*

↳ **13.6.3-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*

↳ **13.6.3-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*

13.6.4 Recording votes

→ **13.6.4-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*

➞ **13.6.4-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*

➞ **13.6.4-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*

↳ **13.6.4-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*

↳ **13.6.4-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*

→ **13.6.4-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*

13.6.5 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.

➞ **13.6.5-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*

↳ **13.6.5-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.

13.6.6 Respecting limits

➞ **13.6.6-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*

↳ **13.6.6-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*

D I S C U S S I O N

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*

13.6.7 Procedures required for correct system functioning

13.6.7-A Process allows each eligible voter to vote

The voting process shall allow each eligible voter to cast a ballot.

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 also Requirement III.6.6.4-C.1.

Source: *[2] I.2.4.2.b, generalized from DRE systems to the voting process.*

Impact: *Click here to add the Impact*

13.6.7-B At most one cast ballot per voter

The voting process shall prevent a voter from casting more than one ballot in the same 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

See also Requirement III.6.6.1-A.1.

Source: *[2] I.2.4.2.d, generalized from DRE systems to the voting process.*

Impact: *Click here to add the Impact*

13.6.7-C Process ensures correct ballot style

The voting process shall prevent a voter from voting a ballot style to which he or she is not entitled.

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 also Requirement III.6.2-A.2, Requirement III.6.2-A.3 and Requirement III.6.6.1-B.

Source: *[2] I.2.4.2.c, generalized from DRE systems to the voting process.*

Impact: *Click here to add the Impact*

→ **13.6.7-D** Process prevents vote tampering

The voting process shall prevent modification of the voter's vote after the ballot is cast.

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 also Requirement III.6.6.4-D, cast ballot.

Source: *[2] I.2.4.3.3.n, generalized.*

Impact: *Click here to add the Impact*

→ **13.6.7-E** Early voting, ballot accounting

In the presence of a witness, election judges shall record the value of the ballot counter from each tabulator at the end of each active period.

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 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).

Source: *Issue #1366, Issue #2143.*

Impact: *Click here to add the Impact*

→ **13.6.7-F** Early voting, resumption practices

Election judges returning equipment to the ready state after it has been placed in the suspended state shall 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.

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

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

DISCUSSION

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).

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

13.7 Closing Polls

→ **13.7-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*

DISCUSSION

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*

→ **13.7-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Reworded from [2] I.2.5.*

Impact: *Click here to add the Impact*

↳ **13.7-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*

D I S C U S S I O N

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*

↳ **13.7-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*

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.a.*

Impact: *Click here to add the Impact*

↳ **13.7-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*

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.b.*

Impact: *Click here to add the Impact*

↳ **13.7-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*

↳ **13.7-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."*

→ **13.7-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*

13.7.1 Procedures required for correct system functioning

➞ **13.7.1-A** Process, no early reporting

The voting process shall prevent access to voted ballots until after the close of polls.

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 also Requirement III.6.7-A.

Source: *[2] I.2.4.3.3.r, generalized.*

Impact: *Click here to add the Impact*

13.8 Counting

13.8.1 Integrity

➞ **13.8.1-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*

→ **13.8.1-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*

13.8.2 Voting variations

→ **13.8.2-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*

↳ **13.8.2-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*

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*

↳ **13.8.2-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*

↳ **13.8.2-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*

↳ **13.8.2-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*

↳ **13.8.2-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*

↳ **13.8.2-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*

↳ **13.8.2-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*

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 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*

↳ **13.8.2-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*

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*

↳ **13.8.2-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*

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*

↳ **13.8.2-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*

D I S C U S S I O N

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*

↳ **13.8.2-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*

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*

↳ **13.8.2-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*

↳ **13.8.2-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*

↳ **13.8.2-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*

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*

↳ **13.8.2-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*

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*

↳ **13.8.2-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*

↳ **13.8.2-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*

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, 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*

13.8.3 Ballot separation

See also Dangling ref: PleaseAddReference_HFP_Rejection and Requirement III.6.8.4-C.

→ **13.8.3-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*

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*

↳ **13.8.3-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*

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*

↳ **13.8.3-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*

↳ **13.8.3-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*

→ **13.8.3-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*

→ **13.8.3-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*

13.8.4 Misfed ballots

→ **13.8.4-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."*

→ **13.8.4-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*

→ **13.8.4-C** Paper-based tabulators, misfeed rate benchmark

The misfeed rate shall not exceed 10^{-4} (1 / 10 000).

Applies to: *Paper-based device ∧ Tabulator*

Test Reference: *Volume V Section 5.3.4*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Merge of [2] I.3.2.5.1.4.b and I.3.2.5.2.c, harmonized to 1 in 10 000 benchmark.*

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 %.*

13.8.5 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.

→ **13.8.5-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*

DISCUSSION

"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*

→ **13.8.5-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*

→ **13.8.5-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*

→ **13.8.5-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*

→ **13.8.5-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*

→ **13.8.5-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*

→ **13.8.5-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*

→ **13.8.5-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*

→ **13.8.5-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*

DISCUSSION

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*

13.8.6 Consolidation

→ **13.8.6-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*

DISCUSSION

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*

↳ **13.8.6-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*

DISCUSSION

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*

13.8.7 Procedures required for correct system functioning

→ **13.8.7-A** 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 shall perform this task in the presence of a witness.

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

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

DISCUSSION

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.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

13.9 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.

13.9.1 General reporting functionality

→ **13.9.1-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*

→ **13.9.1-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*

→ **13.9.1-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*

13.9.2 Audit, status, and readiness reports

→ **13.9.2-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*

DISCUSSION

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*

→ **13.9.2-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*

DISCUSSION

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*

→ **13.9.2-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*

→ **13.9.2-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*

→ **13.9.2-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*

→ **13.9.2-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*

→ **13.9.2-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*

13.9.3 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.

13.9.3.1 General functionality

→ **13.9.3.1-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.*

→ **13.9.3.1-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*

→ **13.9.3.1-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*

→ **13.9.3.1-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.*

↳ **13.9.3.1-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*

↳ **13.9.3.1-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*

→ **13.9.3.1-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*

→ **13.9.3.1-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*

D I S C U S S I O N

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."*

13.9.3.2 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).

→ **13.9.3.2-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*

→ **13.9.3.2-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*

↳ **13.9.3.2-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*

↳ **13.9.3.2-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*

↳ **13.9.3.2-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **13.9.3.2-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*

DISCUSSION

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*

↳ **13.9.3.2-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*

D I S C U S S I O N

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*

↳ **13.9.3.2-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*

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*

↳ **13.9.3.2-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*

D I S C U S S I O N

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*

→ **13.9.3.2-D** Report counted ballots by contest

All systems shall report the number of counted ballots for each 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*

DISCUSSION

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*

13.9.3.3 Vote totals

For the source of these requirements, please see the note in Volume III Section 6.9.3.2.

→ **13.9.3.3-A** Report votes for each candidate or choice

All systems shall report the vote totals for each candidate or choice in each 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*

DISCUSSION

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*

→ **13.9.3.3-B** Report overvotes for each contest

All systems shall report the number of overvotes for each 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*

DISCUSSION

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*

↳ **13.9.3.3-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*

DISCUSSION

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*

➞ **13.9.3.3-C** Report undervotes for each contest

All systems shall report the number of undervotes for each 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

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*

→ **13.9.3.3-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*

→ **13.9.3.3-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*

→ **13.9.3.3-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*

→ **13.9.3.3-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*

→ **13.9.3.3-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*

DISCUSSION

"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*

→ **13.9.3.3-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*

DISCUSSION

"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*

13.9.4 Procedures required for correct system functioning

→ **13.9.4-A** Ballot accounting

All precincts shall account for all ballots pursuant to the current best practices for ballot accounting.

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

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

DISCUSSION

[EAC Best Practice Reference Here]

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **13.9.4-B** Label unofficial reports

Any unofficial reports shall be clearly labelled as unofficial.

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 1.4.8.

Source: *[2] I.2.5.4.c, converted to procedural requirement.*

Impact: *Click here to add the Impact*

Chapter 14: Reference Models

14.1 Process Model (informative)

14.1.1 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.

14.1.2 Diagrams

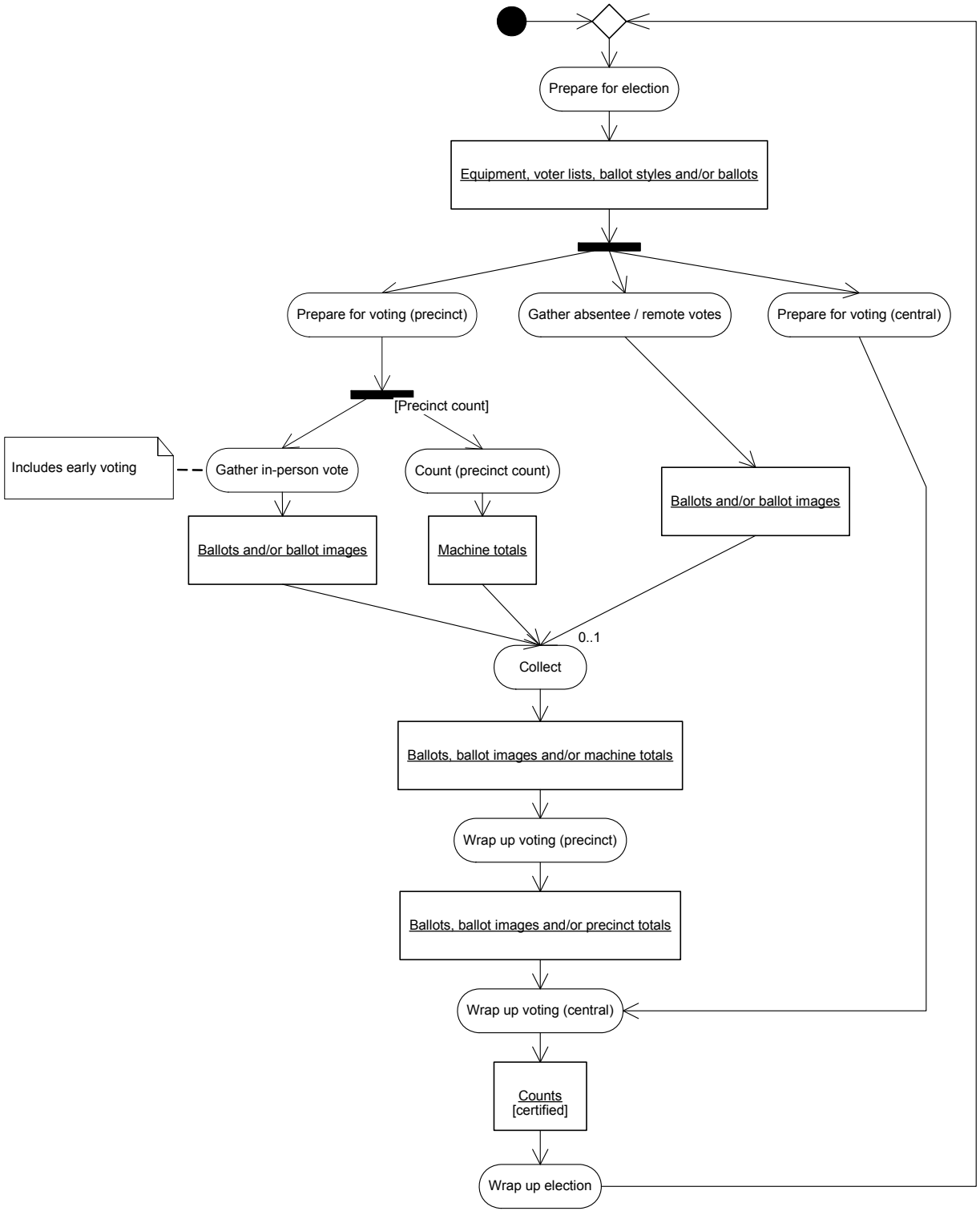

Figure 3 Administer elections

14.1 77BProcess Model (informative)

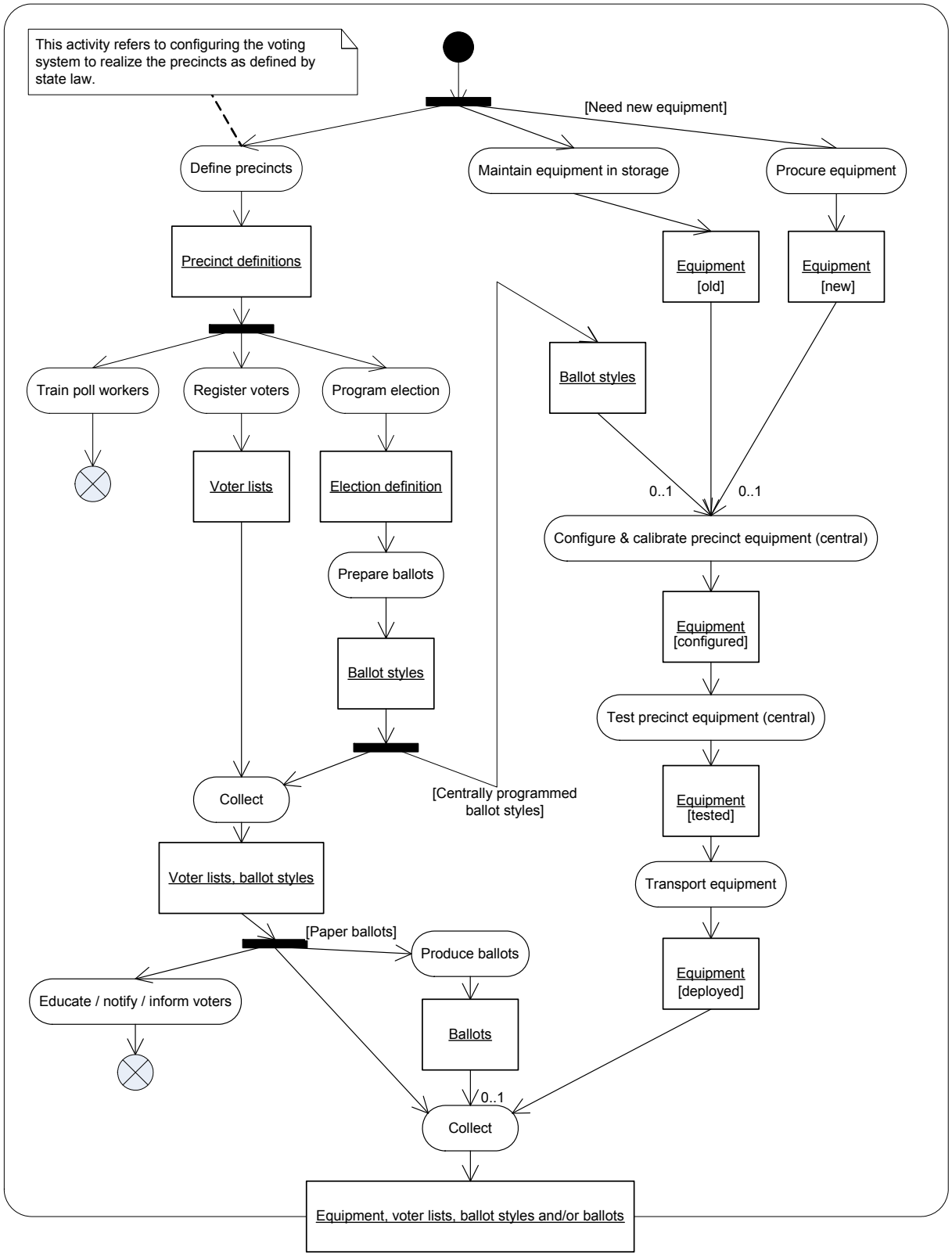

Figure 4 Prepare for election

14.1 77BProcess Model (informative)

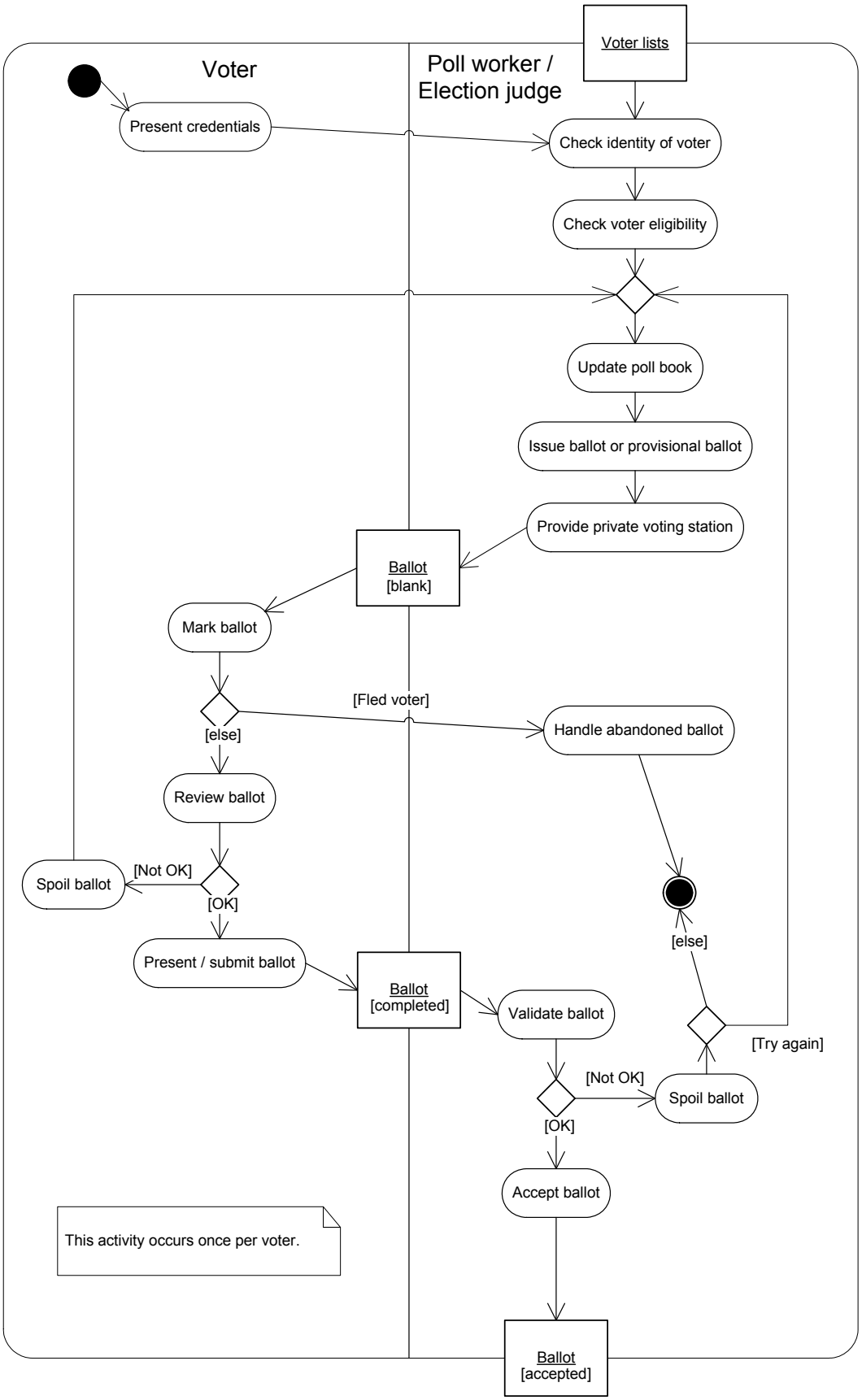

Figure 5 Gather in-person vote (paper-based)

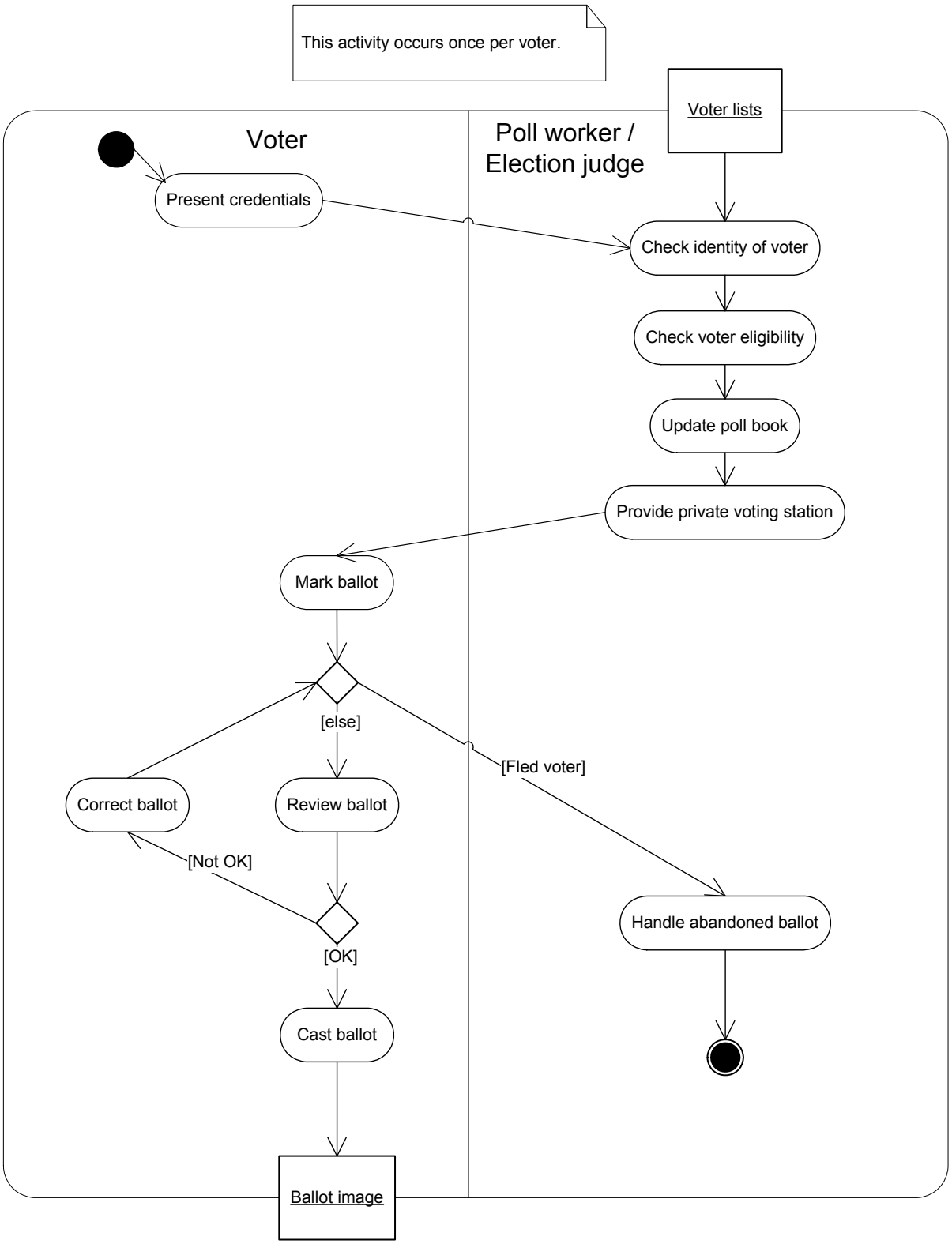

Figure 6 Gather in-person vote (DRE)

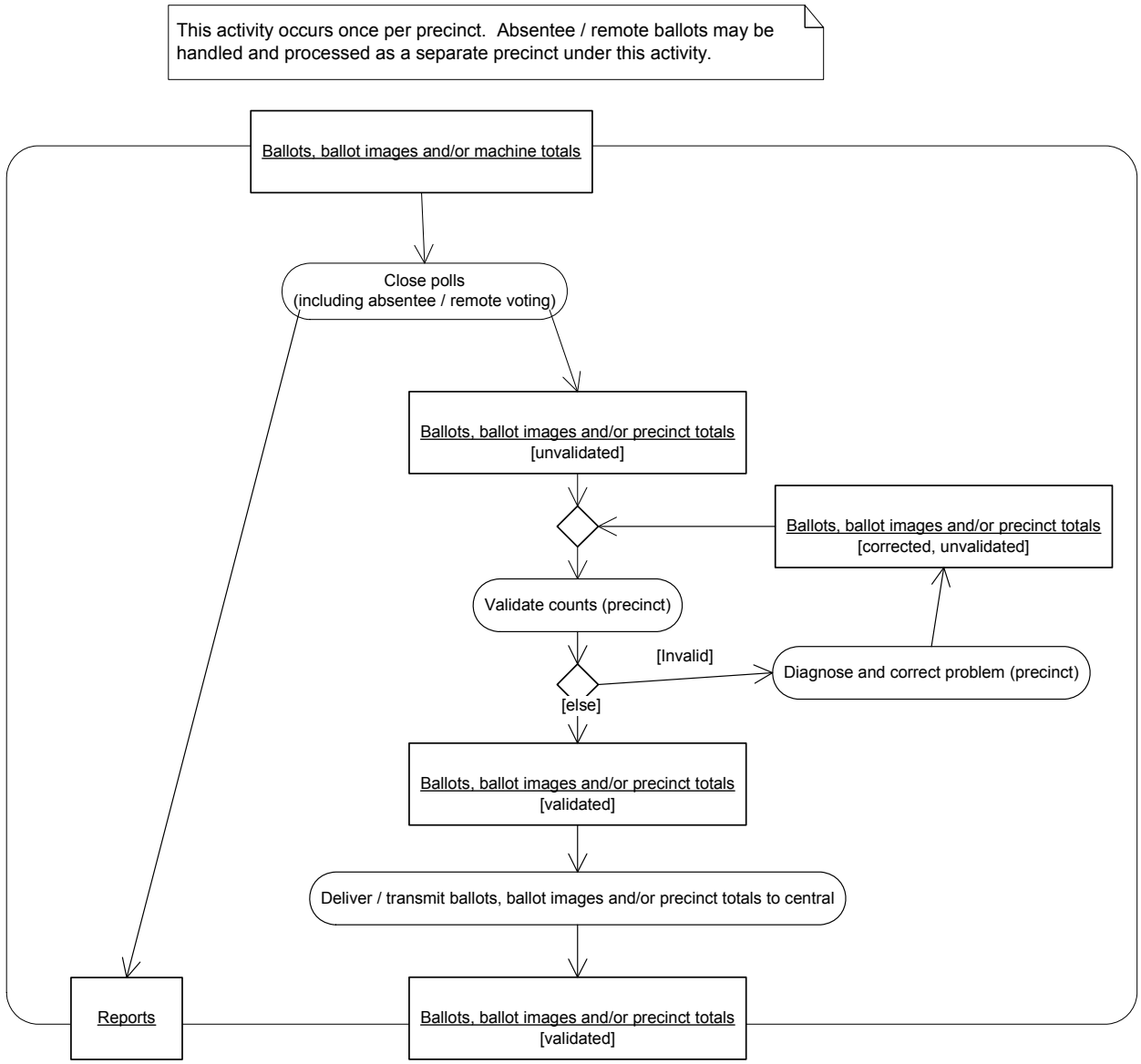

Figure 7 Wrap up voting (precinct)

14.1 77BProcess Model (informative)

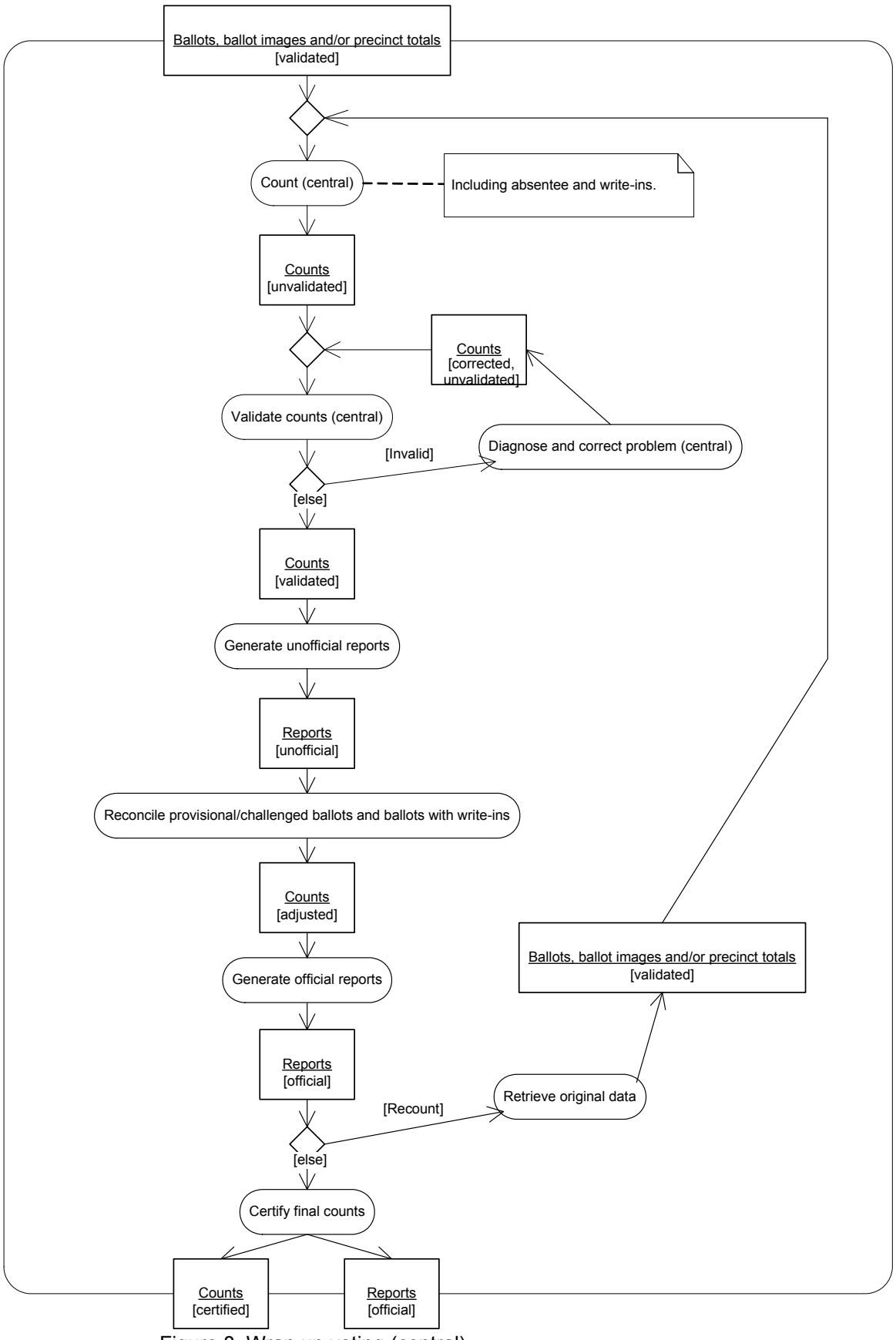

Figure 8 Wrap up voting (central)

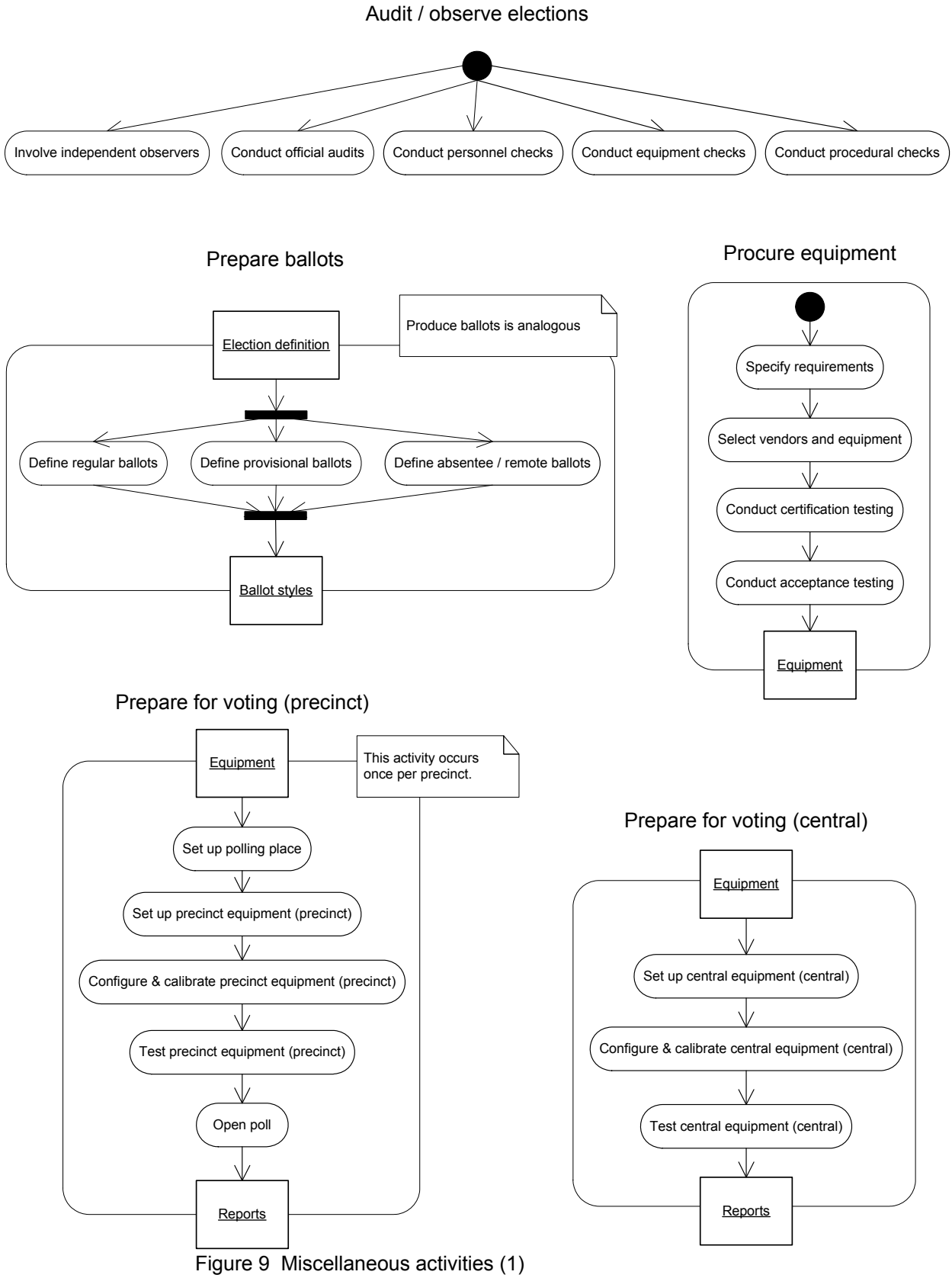

Figure 9 Miscellaneous activities (1)

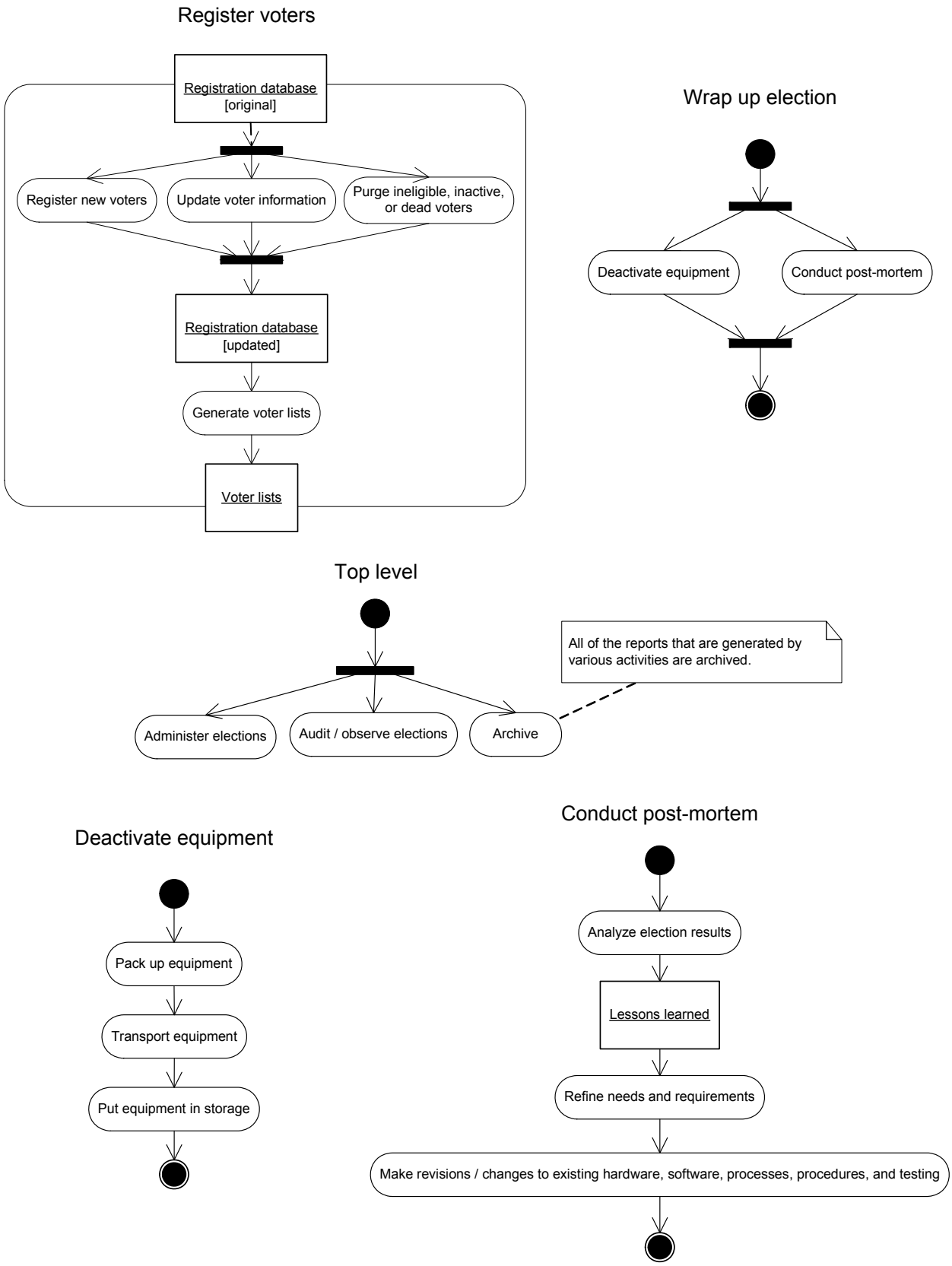

Figure 10 Miscellaneous activities (2)

14.1.3 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.

14.1 77BProcess Model (informative)

```
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).

14.1 77BProcess Model (informative)

```
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>.
```


14.2 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.

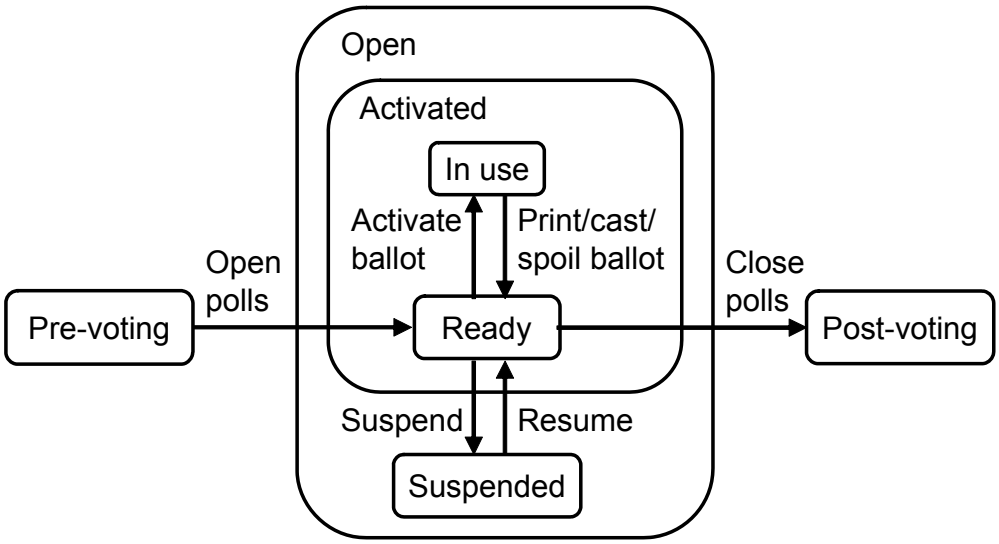

Figure 11 Vote-capture device states

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.

14.3 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]

14.3.1 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. 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. The value of A(*t,v*) may change over time as a result of court decisions, registrar review of voter eligibility, etc. 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

TERM	DEFINITION
	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."
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*).

TERM	DEFINITION
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.
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 4 Terms used in logic verification

14.3.2 General assertions

Invariants:

$$t_O < t_C \leq t_E$$
$$S(c,r,t,v) \geq 0$$
$$S'(c,r,t,v) \geq 0$$

The following assertions formalize several basic integrity constraints. Each textual assertion is intended to elucidate the formal assertion(s) that follow it. In case of discrepancy or confusion, the formal assertions 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.

$$t \geq D(v) \rightarrow S(c,r,t,v) = S(c,r,D(v),v)$$

14.3.3 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 assertions 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).

14.3.4 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).

$$S(c,r,t,v) \leq 1$$

14.4 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

March 2007 DRAFT

VOLUME 4:

DOCUMENTATION STANDARD

DOCUMENTATION REQUIREMENTS
FOR VENDORS AND VSTLS

Volume 4 Table of Contents

test

Volume 4: Standards on data to be provided

Chapter 1: Introduction

1.1 Background

The Voluntary Voting System 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 and protocols that test labs implement; and
- A terminology standard (Volume II) defining terms used in the foregoing.

1.2 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.

1.3 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 EAC national certification process;
- Software repositories designated by the EAC 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.

1.4 Description and Rationale of Significant Changes vs. [6]

1.4.1 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.

1.4.2 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.

1.4.3 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.

1.4.4 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 testing protocols 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.

1.4.5 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 EAC may contain additional, vendor-proprietary information that would not be suitable for publication.

Chapter 2: Technical Data Package (vendor)

2.1 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. If the vendor's developmental test data are incomplete, 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.

2.1.1 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.

2.1.1.1 Required content for initial certification

➞ **2.1.1.1-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*

➞ **2.1.1.1-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.*

➞ **2.1.1.1-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.*

2.1.1.2 Required content for system changes and recertification

→ **2.1.1.2-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*

2.1.1.3 Format

The requirements for formatting the TDP are general in nature; specific format details are of the vendor's choosing.

➞ **2.1.1.3-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*

➞ **2.1.1.3-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*

2.1.2 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.

2.1.3 Protection of proprietary information

→ **2.1.3-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 EAC 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*

→ **2.1.3-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*

2.2 Implementation Statement

➞ **2.2-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*

2.3 System Hardware Specification

➞ **2.3-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*

2.3.1 System hardware characteristics

2.3.1-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*

2.3.2 Design and construction

➞ **2.3.2-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*

↳ **2.3.2-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*

➞ **2.3.2-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*

➞ **2.3.2-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*

2.3.3 Hardwired logic

➞ **2.3.3-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*

→ **2.3.3-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*

2.4 Application Logic Design and Specification

→ **2.4-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*

2.4.1 Purpose and scope

➞ **2.4.1-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*

2.4.2 Applicable documents

➞ **2.4.2-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.*

2.4.3 Application logic overview

➞ **2.4.3-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*

↳ **2.4.3-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*

↳ **2.4.3-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*

↳ **2.4.3-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*

2.4.4 Application logic standards and conventions

→ **2.4.4-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*

→ **2.4.4-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*

➞ **2.4.4-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*

2.4.5 Application logic operating environment

➞ **2.4.5-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*

2.4.5.1 Hardware environment and constraints

→ **2.4.5.1-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*

2.4.5.2 Application logic environment

→ **2.4.5.2-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*

→ **2.4.5.2-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*

→ **2.4.5.2-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*

2.4.6 Application logic functional specification

→ **2.4.6-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*

2.4.6.1 Functions and operating modes

➞ **2.4.6.1-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*

➞ **2.4.6.1-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*

2.4.6.2 Application logic integrity features

➞ **2.4.6.2-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*

2.4.7 Programming specifications

➞ **2.4.7-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*

2.4.7.1 Programming specifications overview

2.4.7.1-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*

2.4.7.1-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*

2.4.7.1-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*

↳ **2.4.7.1-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *[2] II.2.5.7.1.*

Impact: *Click here to add the Impact*

2.4.7.2 Programming specifications details

→ **2.4.7.2-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *[2] II.2.5.7.2.*

Impact: *Click here to add the Impact*

→ **2.4.7.2-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.*

→ **2.4.7.2-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*

→ **2.4.7.2-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.*

→ **2.4.7.2-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.*

→ **2.4.7.2-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

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.*

→ **2.4.7.2-G** TDP, high-level assertions

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 invariants and assertions 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.*

→ **2.4.7.2-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *[2] II.5.4.2.i.*

Impact: *Click here to add the Impact*

2.4.8 System database

→ **2.4.8-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*

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.*

Impact: *Click here to add the Impact*

→ **2.4.8-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*

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.a.*

Impact: *Click here to add the Impact*

➞ **2.4.8-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*

➞ **2.4.8-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*

➞ **2.4.8-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*

→ **2.4.8-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*

2.4.9 Interfaces

→ **2.4.9-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*

2.4.9.1 Interface identification

→ **2.4.9.1-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*

2.4.9.2 Interface description

→ **2.4.9.2-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*

➞ **2.4.9.2-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*

➞ **2.4.9.2-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*

→ **2.4.9.2-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*

→ **2.4.9.2-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*

2.4.10 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.

2.5 System Security Specifications

This section is to be provided by STS.

2.6 System Test and Verification Specification

→ **2.6-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *[2] II.2.7.*

Impact: *Click here to add the Impact*

2.6.1 Development test specifications

➞ **2.6.1-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

The vendor's test cases may help to speed up the open-ended testing portions of certification testing.

Documentation that is already required under the life cycle process adopted by the vendor may satisfy this requirement. AG: relevant to QA/CM standards.

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*

2.6.2 National certification test specifications

➞ **2.6.2-A** TDP, usability test reports

The vendor shall provide usability test reports in 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*

→ **2.6.2-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; and
7. Production of audit trails and statistical data.

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 vendor's test cases may help to speed up the open-ended testing portions of certification testing.

Source: *[2] II.2.7.2.*

Impact: *Deleted "acceptance criteria," which makes no sense here.*

→ **2.6.2-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*

2.7 Configuration Management Plan

This section is to be provided by AG. See Max Etschmaier, "Voting Machines: Draft Requirements for Quality and Configuration Management," [2] I.8.

2.8 Quality Assurance Program

This section is to be provided by AG. See Max Etschmaier, "Voting Machines: Draft Requirements for Quality and Configuration Management," [2] I.7.

2.9 System Change Notes

→ **2.9-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*

→ **2.9-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *[2] II.2.13.*

Impact: *Click here to add the Impact*

2.10 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.

→ **2.10-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *[7] as clarified 2006-07-20.*

Impact: *Click here to add the Impact*

→ **2.10-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*

DISCUSSION

Screen shots showing the installation actions may be helpful.

Source: *[2] I.4.1.1.*

Impact: *Click here to add the Impact*

➞ **2.10-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*

➞ **2.10-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 3: 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.

3.1 System Overview

→ **3.1-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*

↳ **3.1-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *[10] 4.3.2.3*

Impact: *Click here to add the Impact*

3.1.1 System description

➞ **3.1.1-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *[2] II.2.2.1.*

Impact: *Click here to add the Impact*

➞ **3.1.1-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*

➞ **3.1.1-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*

3.1.2 System performance

➞ **3.1.2-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*

↳ **3.1.2-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*

↳ **3.1.2-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*

3.2 System Functionality Description

→ **3.2-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.*

3.3 System Security Specification

This section to be provided by STS. Resolution #18-05.

3.4 System Operations Manual

→ **3.4-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*

→ **3.4-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*

3.4.1 Introduction

3.4.1-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*

3.4.1-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*

3.4.1-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*

→ **3.4.1-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*

3.4.2 Operational environment

→ **3.4.2-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*

→ **3.4.2-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*

➞ **3.4.2-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*

3.4.3 System installation and test specification

➞ **3.4.3-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*

↳ **3.4.3-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).*

3.4.4 Operational features

➞ **3.4.4-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*

→ **3.4.4-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*

→ **3.4.4-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*

3.4.5 Operating procedures

→ **3.4.5-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*

3.4.6 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?

→ **3.4.6-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*

↳ **3.4.6-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*

↳ **3.4.6-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*

↳ **3.4.6-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*

3.4.7 Operations support

→ **3.4.7-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*

3.4.8 Transportation and storage

→ **3.4.8-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*

→ **3.4.8-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*

→ **3.4.8-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*

3.4.9 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:

1. Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer operations;
2. References: A list of references to all vendor documents and to other sources related to operation of the system;
3. Detailed Examples: Detailed scenarios that outline correct system responses to faulty operator input. Alternative procedures may be specified depending on the system state; and
4. Manufacturer's Recommended Security Procedures: Security procedures that are to be executed by the system operator.

3.5 System Maintenance Manual

➞ **3.5-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*

➞ **3.5-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *[2] II.2.9.*

Impact: *Click here to add the Impact*

3.5.1 Introduction

→ **3.5.1-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*

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*

↳ **3.5.1-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*

3.5.2 Maintenance procedures

➞ **3.5.2-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*

3.5.2.1 Preventive maintenance procedures

➞ **3.5.2.1-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*

3.5.2.2 Corrective maintenance procedures

→ **3.5.2.2-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*

→ **3.5.2.2-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*

3.5.3 Maintenance equipment

3.5.3-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*

3.5.4 Parts and materials

3.5.4-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*

3.5.4.1 Common standards

3.5.4.1-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*

3.5.4.2 Paper-based systems

→ **3.5.4.2-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.*

↳ **3.5.4.2-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *[2] I.3.2.4.2.3.c and II.2.9.4.2.*

Impact: *Click here to add the Impact*

→ **3.5.4.2-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *[2] I.2.3.1.3.1.c, I.3.2.4.2.1.c, II.2.9.4.2.*

Impact: *Click here to add the Impact*

→ **3.5.4.2-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*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *[2] I.2.3.1.3.2, revised.*

Impact: *Click here to add the Impact*

→ **3.5.4.2-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.5.5.1-A.

Applies to: *Voting system*

Test Reference: *Volume V Section 4.1*

DISCUSSION

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*

3.5.5 Maintenance facilities and support

→ **3.5.5-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *[2] II.2.9.5.*

Impact: *Click here to add the Impact*

→ **3.5.5-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.*

3.5.6 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:

1. **Glossary:** A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer maintenance;
2. **References:** A list of references to all vendor documents and other sources related to maintenance of the system;
3. **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
4. **Maintenance and Security Procedures:** Technical illustrations and schematic representations of electronic circuits unique to the system.

3.6 Personnel Deployment and Training Requirements

→ **3.6-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*

3.6.1 Personnel

➞ **3.6.1-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*

➞ **3.6.1-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*

3.6.2 Training

→ **3.6.2-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 4: 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.

4.1 Requirements

➞ **4.1-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *[6] II.A.1.1*

Impact: *Click here to add the Impact*

➞ **4.1-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.*

↳ **4.1-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*

→ **4.1-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*

↳ **4.1-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*

➞ **4.1-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:

1. All functionality performed by new devices;
2. All functionality performed by modified devices;

3. Functionality that is accomplished using any interfaces to new devices, or that shares inputs or outputs from new devices;
4. All functionality related to vote tabulation and election results reporting; and
5. 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*

→ **4.1-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*

DISCUSSION

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*

↳ **4.1-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *New requirement.*

Impact: *Click here to add the Impact*

↳ **4.1-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *New requirement.*

Impact: *Click here to add the Impact*

↳ **4.1-E.3** Test plan, other test suites

For all other test cases, including those adopted from vendor-provided test plans and those developed by the test lab, 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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *New requirement.*

Impact: *Click here to add the Impact*

➞ **4.1-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*

DISCUSSION

Click here and type the discussion about this requirement

Source: *[7]*

Impact: *Click here to add the Impact*

Chapter 5: Test Report for EAC Certification (test lab)

5.1 Requirements

➞ **5.1-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*

D I S C U S S I O N

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*

➞ **5.1-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*

D I S C U S S I O N

[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*

→ **5.1-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*

→ **5.1-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*

→ **5.1-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*

D I S C U S S I O N

See Ch. 5 of [10].

Source: *[7]*

Impact: *Click here to add the Impact*

➞ **5.1-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*

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-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*

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-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*

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-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*

DISCUSSION

[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*

↳ **5.1-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*

➞ **5.1-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*

↳ **5.1-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.

Applies to: *Voting device*

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

D I S C U S S I O N

See Volume V Section 5.3.2.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

↳ **5.1-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*

↳ **5.1-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*

➞ **5.1-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*

➞ **5.1-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 "shalls" 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*

➞ **5.1-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*

➞ **5.1-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*

→ **5.1-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*

→ **5.1-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*

→ **5.1-Q** Test report, issues list

The test lab shall list and explain any concerns that should be brought to the attention of the Election Assistance Commission.

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 Election Assistance Commission.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

Chapter 6: Public Information Package (test lab)

6.1 Requirements

→ **6.1-A** Public Information Package (PIP)

The test lab shall provide the EAC 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*

↳ **6.1-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*

↳ **6.1-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 EAC 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

March 2007 DRAFT

VOLUME 5:

TESTING STANDARD

TESTING METHODS OVERVIEWS

Volume 5 Table of Contents

Volume 5: Testing Standard

Chapter 1: Introduction

1.1 Background

The Voluntary Voting System 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 and protocols that test labs implement; and
- A terminology standard (Volume II) defining terms used in the foregoing.

The purpose of national voting system testing is to provide the states and other affected stakeholders with some level of assurance that a voting system is fit for use. States have the option to subject a voting system to additional scrutiny before purchasing and deploying it; however, most states require EAC certification as an entry condition.

1.2 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.

1.3 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 EAC national certification process;
- Software repositories designated by the EAC 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.

1.4 Description and Rationale of Significant Changes vs. [6]

1.4.1 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 EAC on the conformity of the system as a whole.

1.4.2 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 5 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).

1.4.3 New and revised inspections

1.4.3.1 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.

1.4.3.2 Source code review for security

This section is to be provided by STS.

1.4.3.3 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 assertions. 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.

1.4.4 New and revised test protocols

1.4.4.1 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).

1.4.4.2 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 protocol for 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.

1.4.4.3 Performance-based usability testing

This section is to be provided by HFP.

1.4.4.4 Open-ended vulnerability testing

This section is to be provided by STS.

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 EAC.

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 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*

DISCUSSION

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.

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.

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*

D I S C U S S I O N

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*

D I S C U S S I O N

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*

D I S C U S S I O N

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 EAC.

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 Test Methods

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 by a lab technician or an accredited specialist to bypass or break the access or integrity controls of a system or device.

Like functional testing, vulnerability testing can falsify a general assertion (namely, that the system or device is secure) but it cannot verify it (show it to be true in all cases).

Vulnerability testing can be performed using a test suite or it can be open-ended.

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 (if applicable) and design of the voting system 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.

1. Requirement III.5.1-A
2. Requirement III.5.1-D
3. Requirement III.5.1-E
4. Requirement III.5.1-F
5. Requirement III.5.1-G
6. Requirement III.5.1-H
7. Requirement III.5.3.1-A
8. Requirement III.5.3.1-C
9. Requirement III.5.3.1-D
10. Requirement III.5.4.4-A
11. Requirement III.5.4.6-A
12. Requirement III.5.4.6-B
13. Requirement III.5.4.6-C
14. Requirement III.5.4.8-C

15. Requirement III.5.5.1-A12
16. Requirement III.5.6-A13
17. Requirement III.6.1-G
18. Requirement III.6.6.4-B
19. Requirement III.6.6.5-A
20. Requirement III.6.9.1-C

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

4.4 Examination of Vendor Practices for Configuration Management and Quality Assurance

This section is to be provided by AG.

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.

After reviewing the materials submitted, test labs are entitled to additional proof if the correctness of a callable unit is insufficiently verifiable.

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*

DISCUSSION

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 assertions

For the core logic as a whole, and for each invariant and assertion indicated in Volume III Section 7.3, the test lab shall verify that the assertion 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*

Chapter 5: Test Protocols

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 may replicate testing performed by the vendor and documented in the vendor's TDP, but must not rely on vendor testing as a substitute for independent testing.

5.1 Hardware

This section is to be provided by AG.

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*

DISCUSSION

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 instruction and every 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*

DISCUSSION

[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.

Inaccessible code in application logic and border logic should be purged.

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*

D I S C U S S I O N

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** Test lab may reuse vendor's structural test cases

The test lab may use test cases supplied by the vendor in compliance with Requirement IV.2.6.1-A.

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.4.3.3*

Impact: *Click here to add the Impact*

↳ **5.2.2-C.1** Validate vendor's structural test cases

If the test lab elects to use test cases supplied by the vendor, the test lab shall

1. Review the vendor's logic analysis, documentation, and, if available, callable unit test case design;
2. Evaluate the test cases for each callable unit with respect to flow control parameters and data on both entry and exit; and
3. Correct all discrepancies between the specifications and the test cases prior to the initiation of 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: *[2]/[6] II.A.4.3.3*

Impact: *Click here to add the Impact*

↳ **5.2.2-C.2** Complete vendor's structural test cases

If the test lab elects to use test cases supplied by the vendor, but the vendor's test cases do not satisfy Requirement V.5.2.2-A and Requirement V.5.2.2-B, then the test lab shall define and execute additional test cases as required to provide that coverage.

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.4.3.3*

Impact: *Click here to add the Impact*

→ **5.2.2-D** 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*

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.4.3.3*

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.

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 of final results.

Applies to: *Voting system*

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

D I S C U S S I O N

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*

D I S C U S S I O N

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*

D I S C U S S I O N

[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-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** Test lab may reuse vendor's functional test cases

The test lab may use test cases supplied by the vendor in compliance with Requirement IV.2.6.2-B.

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.1** Validate vendor's functional test cases

If the test lab elects to use test cases supplied by the vendor, the test lab shall

1. Review the vendor's test matrix, documentation, and, if available, functional test case design;
2. Evaluate the test cases for each function with respect to input data and expected output; and
3. Correct all discrepancies between the specifications and the test cases prior to the initiation of 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: *Clarification of [2]/[6] II.A.4.3.4, harmonized with structural testing.*

Impact: *Click here to add the Impact*

↳ **5.2.3-I.2** Complete vendor's functional test cases

If the test lab elects to use test cases supplied by the vendor, but the vendor's test cases do not satisfy Requirement V.5.2.3-A, Requirement V.5.2.3-B, Requirement V.5.2.3-C, Requirement V.5.2.3-D, Requirement V.5.2.3-E, Requirement V.5.2.3-F and Requirement V.5.2.3-G, then the test lab shall define and execute additional test cases as required to provide that coverage.

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: *Clarification of [2]/[6] II.A.4.3.4, harmonized with structural testing.*

Impact: *Click here to add the Impact*

→ **5.2.3-J** 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 for the protocol 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 6 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 3.8376×10^{-3}.

The minimum volume required for the protocol 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

N	RV FOR P(N,RV) = 0.1	RV FOR P(N,RV) = 0.9
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 6 Factors for calculation of volume cutoff and demonstrated event rate

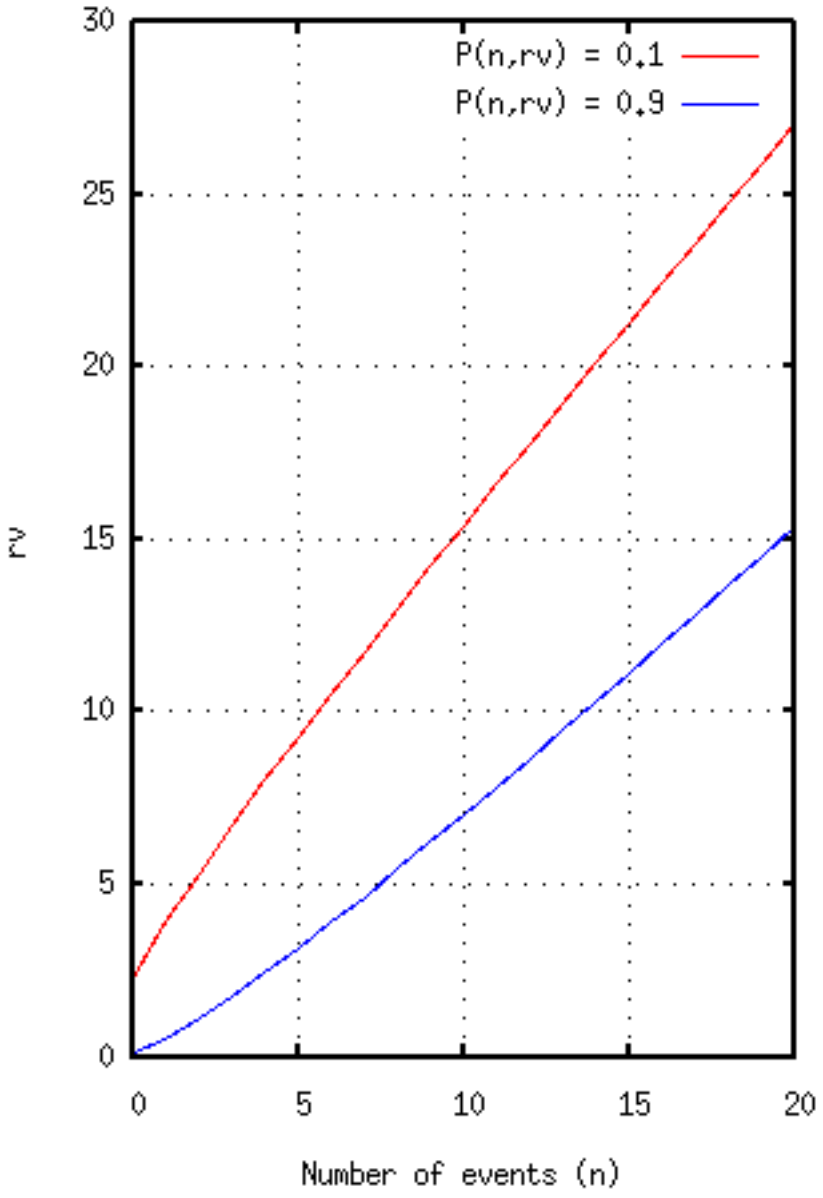

Figure 12 Plot of values from Table 6

Table 6 can be reproduced by Octave[2] version 2.1.73 using the following script.

```
# fsolve won't pass extra parameters to the function being solved, so we must use globals.
global nGlobal # Number of events
global pGlobal # Probability

# Function for the root finder to zero.
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 a and
# b such that an+b is greater than zero and approximates the answer.
function rvFn = rv (n, p, a, b)
  global nGlobal pGlobal
  nGlobal = n
  pGlobal = p
  startingGuess = a*n + b
  [rvFn, info] = fsolve ("rvRoot", startingGuess)
  if (info != 1)
    perror ("fsolve", info)
  endif
endfunction

silent_functions=1
fsolve_options ("tolerance", 1e-12)
printf (" n     P=0.1        P=0.9\n")
for n = 0:20
  printf ("%2u %12.9f %12.9f\n", n, rv(n,0.1,1.3866,2.4441), rv(n,0.9,0.6165,1e-7))
endfor
```

5.3.2 Reliability

"Voter volume" is a placeholder until the data necessary to define a credible benchmark have been collected.

→ **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 number of voters served for each pertinent test execution, for each type of device.

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 do not map 1:1 onto device classes because a given model will belong to several classes.

E.g., The statistics for any number of DREs of the same model are combined, but the statistics for an optical scanner that is also part of the system are kept separate from the DRE statistics.

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 voter volume accumulated across all pertinent tests, for each type of device. If analysis of the cumulative behavior across all pertinent tests indicates that the probability of the true failure rate being worse than the benchmark specified in Requirement III.5.3.1-B is greater than 90 % for any type of device, the verdict on conformity to Requirement III.5.3.1-B shall be Fail. Otherwise, the verdict shall be Pass.

Applies to: *Voting device*

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

DISCUSSION

The total voter volumes below which a given number of failures indicates rejection, for values less than 10, are shown in Table 7.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

FAILURE TOTAL	VOTERS SERVED
1	1054
2	5319

FAILURE TOTAL	VOTERS SERVED
3	11021
4	17448
5	24326
6	31519
7	38948
8	46562
9	54325

Table 7 Failure rate cutoff points

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*

DISCUSSION

The report total volumes below which a given number of errors indicates rejection, for values less than 10, are shown in Table 8.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

REPORT TOTAL ERROR	REPORT TOTAL VOLUME
1	1053606
2	5318117
3	11020654
4	17447696
5	24325911
6	31518981
7	38947669
8	46561182
9	54324681

Table 8 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*

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*

→ **5.3.4-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*

D I S C U S S I O N

"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 10, are shown in Table 9.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

MISFEED TOTAL	TOTAL BALLOT VOLUME
1	1054
2	5319
3	11021
4	17448
5	24326

MISFEED TOTAL	TOTAL BALLOT VOLUME
6	31519
7	38948
8	46562
9	54325

Table 9 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

March 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," http://meganesia.int.gu.edu.au/~phmartin/workflow/PIPE/, 2005-07-22.

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

[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.

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