Jul 18, 2025

Smartmatic Voting System

SMT-2022-TDP-01 Implementation Statement

DISCLAIMER

Smartmatic believes that this document is accurate and reliable. Smartmatic accepts no responsibility, financial or otherwise, for any consequences arising out of the information in or the use of this content. The information contained in this document is subject to change. Updates may be issued from time to time.

This document contains proprietary and confidential information. It was prepared by Smartmatic and is intended for the exclusive use of its clients and licensees.

No part of this document may be photocopied or reproduced in any manner without the prior consent of Smartmatic. Smartmatic does not extend any warranties by this document. All product information and material disclosure contained in this document is furnished subject to the terms and conditions of a purchase or lease agreement. The only warranties made by Smartmatic are contained in such agreements. Users should ensure that the use of this system complies with all legal or other obligations of their governmental jurisdictions.

Table of Contents

1 INTRODUCTION 6

1.1 PURPOSE 6

1.2 SCOPE 6

1.3 AUDIENCE 7

1.4 ACRONYMS 7

2 IMPLEMENTATION STATEMENT 9

2.1 IDENTIFICATION OF THE VOTING SYSTEM 9

2.2 SYSTEM CAPACITIES AND LIMITS 9

2.2.1 General Parameters 9

2.3 LANGUAGES SUPPORTED 14

2.4 ACCESSIBILITY CAPABILITIES 14

2.5 LIST OF VOTING VARIATIONS SUPPORT 15

2.6 DEVICES THAT SUPPORT CORE FUNCTIONS 18

2.6.1 Functionalities and Extensions 20

2.7 LIST OF REQUIREMENTS 27

2.8 SIGNATURES 27

3 REFERENCES 28

4 APPENDIX A. LIST OF REQUIREMENTS 31

Record of Changes

Version	Date	Description of changes
1	03 Feb 2023	Original version
2	20 Feb 2023	Updated *System Limits* section.
3	02 Jun 2023	Updated *System Limits* section. Added a reference to *Appendix A. Materials List.* Updated *References* section.
4	18 Dec 2023	Updated document's outline. Updated *References* section. Updated *Devices that Support Core Functions* section. Updated *Maximum ballots scan per batch* in *System Limits* section. Updated *Functionalities and Extensions* section.
5	07 Jun 2024	Updated *Acronyms* section. Updated *References* section. Updated *Functionalities and Extensions* section. Updated *Voting Variations* sources. Updated *List of Requirements* section.
6	30 Jul 2024	Updated *Functionalities and Extensions* section. Updated *Max. "Vote for" per contest* limit in *System Limits* section.
7	20 Sep 2024	Updated BMD ballot lengths in *System Limits* section.
8	07 Nov 2024	Updated *Devices that Support Core Functions* section. Updated CCOS model from Canon image FORMULA DR-X10C II to Canon imageFORMULA DR-G2140.
9	14 Feb 2025	Updated *System Limits* section. Updated *References* section.
10	21 Feb 2025	Minor format edits.
11	18 Apr 2025	Updated *System Limits* section. Updated parameter name *Max. Choices (candidates + yes/no) per election*.

Version	Date	Description of changes
		Updated *Max. Write-ins per contest* and *Max. "Vote for" per contest* system limits. Added *Max choices per contest*, *Max contests in ballot* and *Max Ballot Styles in EMP* system limits.
12	18 Jul 2025	Updated *Languages Supported* section. Updated *System Capacities and Limits* section.

1 Introduction

This Implementation Statement details the Smartmatic Voting System's capabilities, features, and optional functions as well as any implemented extensions.

1.1 Purpose

This document declares the requirements that have been implemented by the Smartmatic voting system, the features and capabilities supported by the voting system, as well as any extensions (i.e. additional functionalities).

1.2 Scope

The implementation statement serves to provide a high-level understanding of the solution's components and capabilities. It includes:

- Identification of the Voting System
- Device Capacities and Limits
- Languages Supported
- Accessibility Capabilities
- List of Voting Variations Supported
- Devices that Support Core Functions
- List of Requirements
- Extensions
- Signatures

1.3 Audience

This overview is intended for VSTL technicians testing Smartmatic election products, EAC personnel authorized to certify Smartmatic election products, and Smartmatic personnel identifying the conformity assessment activities that are applicable.

1.4 Acronyms

Terms	Definition
AHCI	Advanced Host Controller Interface
BMD	Ballot Marking Device
BIOS	Basic Input Output System
CCOS	Central Count Optical Scanner
CIF	Common Industry Format
COTS	Commercial off the Shelf
CVR	Cast Vote Record
EAC	Election Assistance Commission
EBM	Electronically-assisted Ballot Marker
ECS	Electoral Configuration System
EEM	Election Event Manager
EMP	Election Management Platform
ENR	Election Night Reporting
FEC	Federal Election Commission. Home page at *http://www.fec.gov*
IEEE	Institute of Electrical and Electronics Engineers. Home page at *http://www.ieee.org*
ISO	International Organization for Standardization. Home page at *http://www.iso.org*
JIRA	Issue Tracking software
JM	Jurisdiction Manager
LCD	Liquid Crystal Display
NIST	National Institute of Standards and Technology
NPE	New Product Evaluation
NVLAP	The National Voluntary Laboratory Accreditation Program operated by NIST

Terms	Definition
PCOS	Precinct Count Optical Scanner
RLA	Risk-Limiting Audit
RMS	Results Management System
SMTT	Smartmatic
SVS	Smartmatic Voting System
TDP	Technical Data Package
TGDC	Technical Guidelines Development Committee
UOCAVA	Uniformed and Overseas Citizens Absentee Voting Act
USB	Universal Serial Bus
VSR1	Voting System Release 1
VSTL	Voting System Test Laboratory
VVSG	Voluntary Voting Standards Guide

2 Implementation Statement

2.1 Identification of the Voting System

See full product identification in *Appendix A. Material List in System Overview.*

2.2 System Capacities and Limits

The system limits provide recommendations regarding the behavior of the system under a specific configuration.

2.2.1 General Parameters

#	Parameter	Definition	Component Affected	System Limit
1	Max. Subdivisions levels	The subdivisions represent the jurisdiction configuration of the system, such as State, county, etc.	EMP	47
2	Max. Precincts per election	Subdivision of an electoral district, typically a contiguous area within which all electors go to a single polling place to cast their ballots.	Performance* Reports (EMP)	1000
3	Max. Splits Precincts per election	A subdivision of a precinct that arises when a precinct is split by two or more election districts that may require different ballot styles. Synonyms: split, split precinct, sub-precinct	Performance* Reports (EMP)	400
4	Max. Districts per election	A territorial subdivision for electing members to a legislative body. Generally, only voters	Reports (EMP)	1500

#	Parameter	Definition	Component Affected	System Limit
		(constituents) who reside within the district are permitted to vote in an election held there.		
5	Max. Polling places per election	Location at which voters may cast in-person ballots under the supervision of election workers during one or more specific time periods. Synonyms: poll, polling station 22	Reports (EMP)	220
6	Max. Parties (General Election)	Number of parties defined for a General Election	Ballot size EMP Performance Reports Voting experience	20
7	Max. Contests per election	Number of contests in the election. The contests depend on the voting variations.	Ballot size EMP Performance Reports Voting experience	200
8	Max. Choices (candidates + yes/no) per election	Number of candidates defined for an election	Ballot size EMP Performance Reports Voting experience	2140

#	Parameter	Definition	Component Affected	System Limit
9	Max Offices per election	A position established by law with certain associated rights and duties.	Ballot size EMP Performance Reports Voting experience	200
10	Max. Devices per election	Number of devices associated in a polling place	-	821
11	Max. Devices per election Election day	Number of devices associated in a polling place	-	PCOS: 400 BMD: 400
12	Max. Devices per election Early Voting/Voting Center	Number of devices associated in a polling place	-	PCOS: 8 BMD: 8
13	Max. Devices per election Absentee	Number of devices associated in a polling place	-	CCOS: 4
14	Max. Write-ins per contest	Number of write-ins options defined for a single contest	Ballot Reports	22 certified write-ins
15	Min. "Vote for" per contest	Definition of N - M values for a specific contest	Ballot	1
16	Max. "Vote for" per contest	Definition of N - M values for a specific contest	Ballot	22
17	Max. Languages per election	Languages that can be used in the election, including text and audio	Performance (EMP) Ballot	4

#	Parameter	Definition	Component Affected	System Limit
			Device Idle Screen (BMD, PCOS)	
18	Max. Events per election (Pre-LAT, Official)	Events supported in a specific election.	-	2
19	Central Count max cards per batch	Ballots scanned per batch	-	1700 ballots
20	Ballot width	Ballot widths that can be used in the election.	-	8.5''
21	Ballot lengths	Ballot lengths that can be used in the election.	-	PCOS and CCOS: • Minimum: 11'' • Maximum: 21'' BMD: • Minimum: 11'' • Maximum: 13''
22	Scanner Document Feeder Maximum Capacity	Maximum number of ballots that should be stacked on the scanner document feeder.	-	**11" ballots:** 200 ballots. **14" and 17" ballots:** 120 ballots. **19" and 21" ballots:** 100 ballots.

#	Parameter	Definition	Component Affected	System Limit
23	Max choices per contest	Number of choices available per contest.	Hand-marked ballots BMD reports Voter experience	208
24	Max contests in a ballot	Number of contests in a ballot.	Ballots Reports	56
25	Max Ballot Styles supported by EMP	Ballot styles managed by the EMP.	-	1000

2.3 Languages Supported

The Smartmatic Voting System voting machines support the following languages:

- English
- Spanish
- Chinese
- Russian

The voting machines can display and print the ballot, contest options, review screens, ballots, and voting instructions in all supported languages, in both visual and audio formats where applicable.

EMP's base language is English, however, ballots and election configuration files can be generated in the supported languages.

The Smartmatic Voting System does not support non-written languages.

2.4 Accessibility Capabilities

This section describes the accessibility capabilities supported by the Smartmatic Voting System:

- **Visual voting experience:** within this experience, the voter interacts with the software by tapping the touchscreen of the voting machines without any audio support.
- **Audio voting experience:** within this experience, the voter interacts with the software by using the ATI or Dual switches devices (such as Buddy buttons and Sip & Puffs) to move through the ballot (contests and choices), make selections, and review the selections. In this scenario, the voter uses a stereo headphone connected to the ATI device to hear the audio files (instructions, choices, and contest names) played by the software. As soon as the audio voting experience starts, the voter may select the option to turn off the screen (screen goes black) which provides total privacy.

- **Audiovisual voting experience:** together with the audio voting experience, the voting screen is available to provide feedback to the voter by displaying the current contest, options selected, and other information.

Caution

Any accessibility or communication devices that connect via Bluetooth, RFID or any other wireless technology cannot be used with Smartmatic´s voting machines.

2.5 List of Voting Variations Support

The Electoral Event Types affect the behavior of the Voting Machines at the Polling Place; for example, in a Closed Primary Electoral Event, the machine restricts the voter to a single party. Although the way in which the contest data is presented to the voter in the Voting Machines is configurable, the Tabulation Logic in the Voting Machines is not; it always works the same way and there is no way to customize it.

The following table lists the voting variations supported by the Smartmatic Voting System:

Voting Variation	Description	Supported?
General Election	A general election is an election in which candidates are elected to offices. This is in contrast to a primary election, which is used either to narrow the field of candidates for a given elective office or to determine the nominees for political parties in advance of a general election. Generally, candidates for a general election are chosen via a primary election, but this is not always the case. General elections occur at local, state, and federal levels, and typically occur at regular intervals. In some cases, elections may occur at irregular times, such as to elect a replacement for a seat vacated due to death, resignation, or removal from office.	YES

Voting Variation	Description	Supported?
	Source: https://ballotpedia.org/General_election	
Partisan Closed Primary Election	A closed primary is a type of primary election in which a voter must affiliate formally with a political party in advance of the election date to participate in that party's primary. [1] [2] [3] Source: Ballotpedia	YES
N-of-M	-	YES
Issue Contest	A Decision to be made within an election is not a contest for an office. It is a question on the ballot for approval or rejection. This could be a contest for a referendum, proposition, and/or question. A single ballot may contain one or more contests. **Related terms:** • **Measure:** A proposal to enact a new law or constitutional amendment that is placed on the ballot for approval or rejection by voters. • **Proposition:** A proposal to enact a new law or constitutional amendment that is placed on the ballot for approval or rejection by voters. • **Questions On the Ballot:** Proposals to enact new laws or constitutional amendments that are placed on the ballot for approval or rejection by voters. • **Referendum:** Process whereby a state law or constitutional amendment may be referred to the voters before it goes into effect. • **Referenda:** The plural of Referendum, which is a process whereby a state law or constitutional amendment may be referred to the voters before it goes into effect.	YES

Voting Variation	Description	Supported?
	Source: https://www.eac.gov/sites/default/files/glossary_files/Glossary_of_Election_Terms_EAC.pdf	
Precinct Splits	A subdivision of a precinct which arises when a precinct is split by two or more election districts that may require different ballot styles. Synonyms: split, split precinct, sub-precinct	YES
Ballot Rotation	The process of varying the order of listed candidates within a contest. This allows each candidate to appear first on the list of candidates an approximately equal number of times (based on the number of precincts) across different ballot styles or election districts.	YES
Write-ins	A vote for a candidate that was not listed on the ballot. In some jurisdictions, voters may do this by filling in a write-in space provided on a paper ballot, or they may use a keypad, touch screen, or other electronic means to enter the name on an electronic voting device. Source: https://www.eac.gov/sites/default/files/glossary_files/Glossary_of_Election_Terms_EAC.pdf	YES
Party Affiliations	Refers to a candidate or elected official's relationship to a particular party, not necessarily to a particular set of philosophical beliefs. In terms of voting, this usually refers to voters registering with a recognized political party. Source: https://www.eac.gov/sites/default/files/glossary_files/Glossary_of_Election_Terms_EAC.pdf	YES

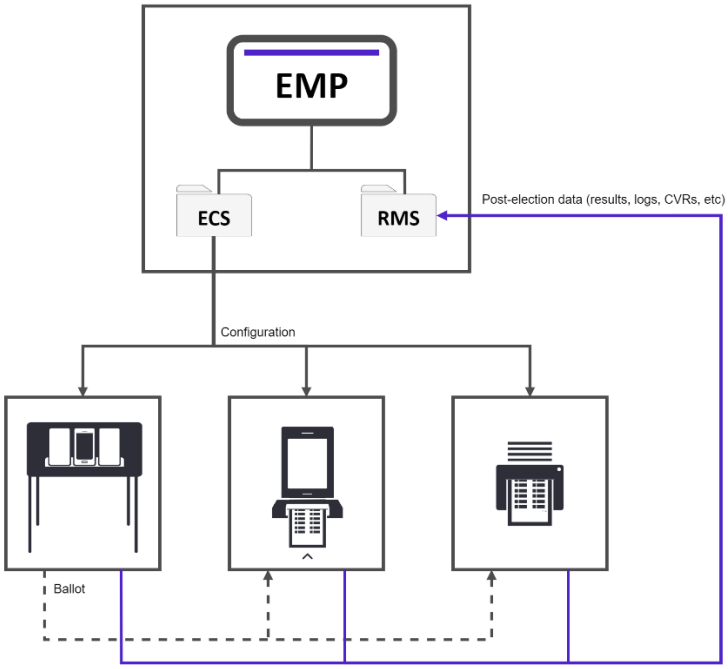
2.6 Devices that Support Core Functions

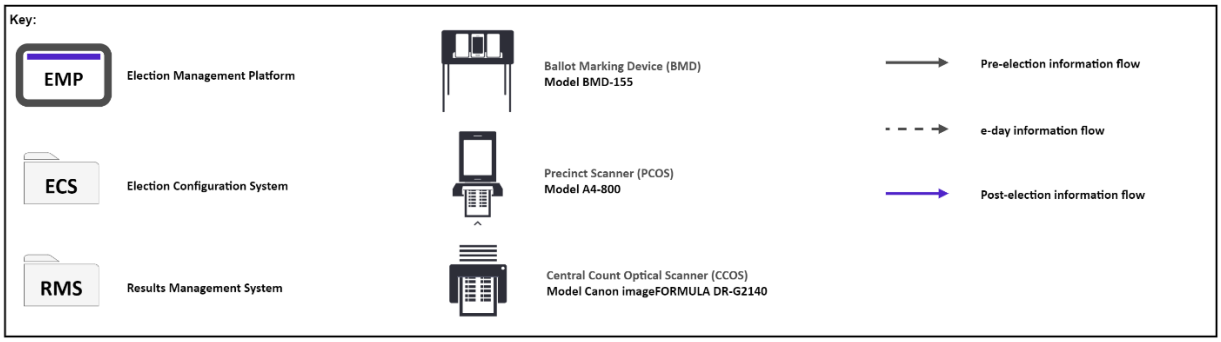
Smartmatic provides an end-to-end solution to increase integrity in the democratic process by offering user-centered technologies with the highest level of security, accessibility and, usability for voters, election workers, and election administrators. This section describes the Smartmatic Voting System and each of its components in broad terms.

The Smartmatic Voting System is made up of the following major components:

- Election Management Platform (EMP)
    - Election Configuration System (ECS)
    - Results Management System (RMS)
- Ballot Marking Device (BMD) - Model: BMD-155
- Precinct Count Optical Scanner (PCOS) - Model A4-800
- Central Count Optical Scanner (CCOS) - Scanner Model**:** Canon imageFORMULA DR-G2140

Components of the Smartmatic Voting System with their model numbers are in the following diagram**.**





The Smartmatic Voting System technology and services support operation at the main locations involved in an election.

Election Data Center	**Election Management Platform (EMP)**: A robust platform to support election officials in properly designing, planning and managing all the tasks regarding an election. The EMP is a complete platform that includes all the tools required to prepare, conduct, and manage the election event. This platform consists of the following sub-components that encompass task lists according to the voting stage:

	Electoral Configuration System (ECS) and Results Management System (RMS)
Central Count Location	**Central Count Optical Scanner (CCOS):** A high-speed COTS scanner processes physical ballots at a central location. The custom-made ballot processing software permits accurate processing and tabulation of large numbers of ballots
Polling Place	**Precinct Count Optical Scanner (A4-800):** An in-precinct voting machine offers usability for all voters, including those with disabilities. It allows everyone to cast their vote independently, thereby increasing confidence in the use of the electoral system. **Ballot Marking Device (BMD-155):** An in-precinct voting machine that offers the highest level of usability for all voters, including those with disabilities. It allows everyone to vote independently, thereby increasing confidence in the use of the electoral system.

2.6.1 Functionalities and Extensions

2.6.1.1 EMP

The following are the functionalities available in Smartmatic's Election Management Platform:

- Parameters configuration
- Results consolidation
- Reporting
- Accessibility functionalities for voting machine configurations
- Access, profiles, and permission functionalities
- Bulk-load/download, data validation/integrity, data processing, and reporting functionalities
- Ballot design, generation, and validation
- User registration and authentication
- Back-up and restore functionalities
- Contest, parties, polling places, districts, offices, and precincts
- Post-load processes

- Voting machine configuration module
- Voting machine's file generation
- Support for common data formats

Additional capabilities or extensions include:

- EMP Workflow Control
- Early Voting Location Types (may be enabled or disabled)
- Contest Configuration (may be enabled or disabled)

2.6.1.2 PCOS

The following are the functionalities available in Smartmatic's Precinct Count Optical Scanner. These capabilities are configured for each voting machine from the Election Management Platform (EMP); PCOS users do not have access to activate or deactivate any of the below.

- Install electoral data
- Diagnostics
- Authentication
- Open polls
- Ballot casting, variations
- Ballot scanning
- Exceptions and write-in support (voting experience)
- Multi-language support
- Accessibility -- audio, visual, audiovisual and support for COTS devices for different scenarios
- Close polls
- Consolidate results
- Export counters, vote records, ballot images

- Reporting
- System information
- Help
- Set system date and time
- Export audit log
- Export device logs
- Shut down

Additional capabilities or extensions include:

- Warehouse device setup (date and time, provisioning)
- Event selection (multiple events)
- Pause voting
- Resume voting
- Reopen voting
- Calibrate scanner
- Shoe shine
- Reset
- Ballot digital stamping

2.6.1.3 BMD

The following table includes the available functionalities in the BMD. These capabilities are configured for each voting machine from the Election Management Platform (EMP); BMD users do not have access to deactivate any of the below:

- Install electoral data
- Diagnostics
- Authentication
- Open polls
- Ballot printing, marking, casting, variations,
- Exceptions and write-in support (voting experience)
- Multi-language support
- Accessibility -- audio, visual, audiovisual and support for COTS devices for different scenarios
- Close polls
- Export electoral information
- Reporting
- System Information
- Help
- Set system date and time
- Export audit log
- Export device logs
- Shut down

Additional capabilities or extensions include:

- Warehouse device setup
- Event selection (multiple events)

- Pause voting
- Resume voting
- Reopen voting
- Empty ballot box
- Delete electoral configuration
- Reset

2.6.1.4 CCOS

The following are the functionalities available in Smartmatic's Central Count Optical Scanner.

These capabilities are configured for each voting machine from the Election Management Platform (EMP); CCOS users do not have access to deactivate any of the below.

- Install electoral data
- Diagnostics
- Authentication
- Open count
- Ballot scanning
- Scan ballot parameters
- Ballot batch transfer
- Close count
- Reporting
- System information
- Help
- Set system date and time
- Export audit log
- Export device logs
- Shut down

Additional capabilities or extensions include:

- Warehouse device setup (date and time, provisioning)
- Event selection (multiple events)
- Ballot removal for exceptions
- Ballot imprinting

- Pause count
- Resume count
- Reopen count
- Reset

2.7 List of Requirements

See *Appendix A. List of Requirements*.

2.8 Signatures

Name	Date	Signature

3 References

TDP

Document Number	Document Title
SMT-2022-TDP-01	*Implementation Statement*
SMT-2022-TDP-02	*System Overview*
SMT-2022-TDP-03	*System Performance*
SMT-2022-TDP-04	*System Operations*
SMT-2022-TDP-05	*System Security Specification*
SMT-2022-TDP-05-01	*Security Architecture*
SMT-2022-TDP-05-02	*Security Policy*
SMT-2022-TDP-05-03	*Key Management*
SMT-2022-TDP-05-04	*Smartmatic Protection Model*
SMT-2022-TDP-05-05	*Supply Chain and Risk Management*
SMT-2022-TDP-05-06	*Criticality Analysis*
SMT-2022-TDP-05-07	*Vulnerability Management Plan*
SMT-2022-TDP-06	*Personnel Deployment & Training*
SMT-2022-TDP-07	*Paper & Ballot Specifications*
SMT-2022-TDP-08	*System Functionality Description*
SMT-2022-TDP-09-01	*EMP Hardware Specification*
SMT-2022-TDP-09-02	*BMD Hardware Specification*
SMT-2022-TDP-09-03	*PCOS Hardware Specification*
SMT-2022-TDP-09-04	*CCOS Hardware Specification*
SMT-2022-TDP-10	*Software Design and Specification*
SMT-2022-TDP-10-01	*EMP Programming Specifications*
SMT-2022-TDP-10-02	*EMP System Database*
SMT-2022-TDP-10-03	*PCOS and CCOS Programming Specifications*
SMT-2022-TDP-10-04	*BMD Programming Specifications*
SMT-2022-TDP-10-05	*Design and Interface Specification*

Document Number	Document Title
SMT-2022-TDP-10-06	*Smartmatic Coding Conventions and Guidelines*
SMT-2022-TDP-QPL	*Master QA Plan*
SMT-2022-TDP-CPL	*Configuration Management Plan*
SMT-2022-TDP-AUP	*System Audit Procedures*
SMT-2022-TDP-ATS	*System Audit Type Specifications*
SMT-2022-TDP-ATM	*Logic and Accuracy Testing Manual*
SMT-2022-TDP-BCS	*System Barcode Specifications*
SMT-2022-TDP-CDS	*System Common Data Format Specifications*
SMT-2022-TDP-SLS	*System Log Event Code Specifications*
SMT-2022-EVM-TBP	*Voting Machines Trusted Build Procedures*
SMT-2022-EMP-TBP	*EMP Trusted Build Procedures*

Product Manuals

Document Number	Document Title
SMT-2022-PCOS-INM	*PCOS Installation Manual*
SMT-2022-PCOS-STP	*PCOS Setup Inspection*
SMT-2022-PCOS-USM	*PCOS User Manual*
SMT-2022-PCOS-TSM	*PCOS Troubleshooting Manual*
SMT-2022-PCOS-MNM	*PCOS Maintenance Manual*
SMT-2022-CCOS-INM	*CCOS Installation Manual*
SMT-2022-CCOS-STP	*CCOS Setup Inspection*
SMT-2022-CCOS-USM	*CCOS User Manual*
SMT-2022-CCOS-TSM	*CCOS Troubleshooting Manual*
SMT-2022-CCOS-MNM	*CCOS Maintenance Manual*
SMT-2022-BMD-INM	*BMD Installation Manual*
SMT-2022-BMD-STP	*BMD Setup Inspection*
SMT-2022-BMD-USM	*BMD User Manual*
SMT-2022-BMD-TSM	*BMD Troubleshooting Manual*

Document Number	Document Title
SMT-2022-BMD-MNM	*BMD Maintenance Manual*
SMT-2022-EMP-INM-01	*EMP Installation Manual*
SMT-2022-EMP-INM-02	*EMP Workstation Getting Started Guide*
SMT-2022-EMP-STP	*EMP Setup Inspection*
SMT-2022-EMP-USM-00	*EMP Getting Started Guide*
SMT-2022-EMP-USM-01	*EMP User Manual – System Administration*
SMT-2022-EMP-USM-02	*EMP User Manual - Election Management*
SMT-2022-EMP-USM-03	*EMP User Manual - Results Management*
SMT-2022-EMP-USM-04	*EMP User Manual - Jurisdiction Dashboard*
SMT-2022-EMP-TSM-01	*EMP Troubleshooting Manual*
SMT-2022-EMP-SYS-01	*EMP Data Bulk Load Specifications*
SMT-2022-EMP-MNM	*EMP Maintenance Manual*

4 Appendix A. List of Requirements

Key	Summary	Description	Component/s
SMTTVS-4	1.1.1-A – Election definition	The voting system must provide the capability to import, define, maintain, and export the information necessary to define ballots and hold an election, including for: 1. election districts, 2. contests and ballot measures, 3. candidates, and 4. ballot style information. **Discussion** This requirement states that election and ballot definition capabilities must be included within the voting system. Ballot style information includes those labels, headers, and other information typically found on ballots and that varies across jurisdictions and precincts. Requirements in *Principle 4: Interoperable* deal with using common data formats for importing and exporting election definition information.	EMP, Integration, TDP
SMTTVS-5	1.1.1-B – Serve multiple or split precincts and election districts	The voting system must describe election districts and precincts in such a way that a given polling place may serve: 1. two or more election districts; and/or 2. combinations of precincts and split precincts. **Discussion**	EMP, TDP

Key	Summary	Description	Component/s
		This requirement addresses the capability to accommodate multiple ballot styles depending on the political geography being served by a polling place.	
SMTTVS-6	1.1.1-C – Multiple identifiers	The voting system must enable election officials to associate at least three identifiers that can be cross-referenced with each other for administrative subdivisions, election districts, contests, and candidates. This also includes: 1. locally defined identifiers; 2. state-wide-defined identifiers; and 3. Open Civic Data Identifiers [OCD-ID] **Discussion** This requirement is based on the need to support cross-referencing of statewide identifier schemes, such as *Open Civic Data Identifiers [OCD-ID]* with those used on a more local level.	EMP, Integration, TDP
SMTTVS-7	1.1.1-D – Definition of parties and contests	The voting system must allow for: 1. the definition of political parties and indicate the affiliation or endorsements of each contest option; 2. information on both party-specific and non-party-specific contests, with the capability to include both contests on the same ballot; and 3. contests that include ballot positions with write-in opportunities.	EMP, TDP

Key	Summary	Description	Component/s
SMTTVS-8	1.1.1-E – Voting variations	The voting system must provide the capability to define and identify contests, contest options, candidates, and ballot questions using all voting variations indicated in the manufacturer-provided implementation statement. **Discussion** See requirements in sections *1.1.4 – Casting* and *1.1.8 – Tabulation* for voting variations most commonly used in the U.S.	EMP, TDP
SMTTVS-9	1.1.1-F – Confirm recording of election definition	The voting system must check and confirm that its data is correctly recorded to a persistent storage system. **Discussion** *Persistent storage* includes storage systems such as non-volatile memory, hard disks, and optical disks.	EMP, Integration, TDP
SMTTVS-10	1.1.1-G – Election definition distribution	The voting system must provide for creation of master copies of election definition information as needed to configure each voting device in the voting system.	EMP, Integration, TDP
SMTTVS-11	1.1.1-H – Jurisdiction-dependent content	The voting system must enable election officials to update jurisdiction-dependent text, line art, logos, and images to ballot styles.	EMP, Integration, TDP

Key	Summary	Description	Component/s
SMTTVS-12	1.1.1-I – Include contests	The voting system must provide for the inclusion of all contests in a given ballot style, in which the voter is entitled to vote.	EMP, TDP
SMTTVS-13	1.1.1-J – Exclude contests	The voting system must provide for the exclusion of any contest from a given ballot style, in which the voter is prohibited from voting because of place of residence or other administrative criteria. **Discussion** In systems supporting primary elections, this requirement would include the exclusion of party-specific contests for which voters in a particular political party are not eligible to vote.	EMP, TDP
SMTTVS-14	1.1.1-K – Primary elections, associate contests with parties	The voting system must support the association of different contests with different political parties when administering primary elections.	EMP, TDP
SMTTVS-15	1.1.1-L – Ballot rotation, Election definition	The voting system must support the production of rotated ballots or activating ballot rotation functions in vote-capture devices by including relevant metadata in distributed election definitions and ballot styles.	EMP, Integration, TDP

Key	Summary	Description	Component/s
SMTTVS-16	1.1.1-M – Ballot configuration in combined or split precincts	The voting system must include the capability of creating distinct ballot configurations for voters from two or more election districts that are served by a given polling place or vote center.	EMP, TDP
SMTTVS-17	1.1.1-N – Ballot style identification	The voting system must include the capability to generate codes or marks to uniquely identify the ballot style associated with any ballot.	EMP, TDP
SMTTVS-18	1.1.2-A – Built-in self-test and diagnostics	The voting system must include built-in measurement, self-testing, and diagnostic software and hardware for monitoring and reporting the system's status.	BMD, CCOS, EMP, Integration, PCOS, TDP
SMTTVS-19	1.1.2-B – Installation of software and ballot styles	The system must include the capability to verify that software and ballot styles have been properly selected and to provide notification of any errors that occur while selecting or installing software and ballot styles. **Discussion** At a minimum, *notification* means an error message and a log entry. Examples of detectable errors include use of software or data intended for a different type of device or operational failures in transferring the software or data.	BMD, CCOS, Integration, PCOS, TDP
SMTTVS-20	1.1.2-C – Use of test ballots	The voting system must provide the capability to submit test ballots for use in verifying the integrity of the system.	BMD, CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-21	1.1.2-D – Testing all ballot positions	Vote-capture devices must allow for testing that uses all potential ballot positions in the election as active positions.	CCOS, Integration, PCOS, TDP
SMTTVS-22	1.1.2-E – Testing cast vote record creation	The voting system must include the ability to verify that cast vote records (CVRs) are created and tabulated correctly by permitting election officials to compare the created CVRs with the test ballots. **Discussion** This requires providing a capability such as an export of CVRs and a tabulated summary that can be compared manually against their test ballot counterparts.	CCOS, EMP, Integration, PCOS, TDP
SMTTVS-23	1.1.2-F – Testing codes and image creation	The voting system must include the capability to verify that encoded versions or images of voter selections on a ballot and any other encoded information on a ballot are created correctly by permitting election officials to compare the encodings and images with the test ballots. **Discussion** The purpose of this requirement is to give election officials the capability, prior to opening the polls, to audit encoded versions of voter selections. This process may include the review of created ballots and encoded information on each ballot to ensure that the images correctly match the ballot, thus validating accuracy in ballot creation. This will include information as provided by a ballot marking device (BMD)	CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		using QR codes, allowing election officials to gain assurance that the QR codes and any encoded data represented by the QR codes contains the voter's selections exactly as made. Likewise, this will enable the election officials to audit any image of the ballot made by a scanner to gain assurance that the image correctly matches the ballot, and to audit any encoded information on the ballot to gain assurance it is being created correctly. **Related requirement:** 1.1.2-C – Use of test ballots	
SMTTVS-24	1.1.2-G – Testing equipment calibration	Scanners must support testing the calibration of the paper-to-digital conversion (such as the calibration of optical sensors, the density threshold, and the logical reduction of scanned images to binary values, as applicable).	BMD, CCOS, Integration, PCOS, TDP
SMTTVS-25	1.1.2-H – No side-effects from pre-election testing	Pre-election testing must introduce no lasting effects regarding the operation of the voting system during the election other than: 1. audit log entries; 2. status changes to note that the tests have been run with a successful or failed result; 3. separate storage of test results; 4. changes in counters that record ballots cast; and 5. normal wear and tear. **Discussion**	BMD, CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		It should be impossible (by design) for the pre-election testing to have any influence on the operation of the device(s) during the election or on the results that are reported for the election. Most notably, election results can never include any test votes that were counted during pre-election testing. If a test election is run on the voting system as a means of providing pre-election testing, an election official should be able to remove all artifacts of the test election except as noted in items 1 through 5 of this requirement.	
SMTTVS-26	1.1.2-I – Equipment status and readiness reports	The voting system must provide the capability to produce equipment readiness reports that show the readiness of the equipment, including: 1. whether calibration is needed; 2. consumable supplies such as toner or paper are sufficient for use; 3. batteries are fully charged; and 4. the status of other election-sensitive aspects of the equipment.	CCOS, PCOS, TDP
SMTTVS-27	1.1.2-J – Ballot style readiness reports	The voting system must provide the capability to produce pre-election reports that include: 1. the allowable number of votes in each contest; 2. the tabulation method for each contest; 3. the inclusion or exclusion of contests as the result of precinct splits; and 4. samples of all final ballot styles.	EMP, Integration, TDP

Key	Summary	Description	Component/s
SMTTVS-28	1.1.2-K – Precinct-based voting devices readiness reports	Precinct-based voting devices must have the capability of generating readiness reports that include: 1. the election's identification data; 2. the identification of the precinct and polling place; and 3. the identification of all ballot styles used in that precinct.	BMD, PCOS, TDP
SMTTVS-29	1.1.2-L – All vote-capture devices readiness reports	Vote-capture devices must have to capability to generate a report that includes the following: 1. the election's identification data; 2. the identification of the precinct and polling place, if applicable; 3. the identification of the device; 4. the identification of all ballot styles loaded; 5. the contents of each active contest option register at all storage locations; 6. confirmation that no hardware or software failures were detected during setup and testing, or a record of those that occurred; and 7. any other information needed to confirm the readiness of the equipment.	CCOS, Integration, PCOS, TDP
SMTTVS-30	1.1.3-A – Opening the polls	The voting system must provide functions to enter a mode in which voting is permitted. **Discussion**	BMD, CCOS, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		This and following requirements cover the process of enabling voting to occur by placing the voting system in a voting mode. More information about the activated stage is defined in Table 11-1.	
SMTTVS-31	1.1.3-B – Non-zero totals	The voting system must not enter the voting mode until all steps necessary to isolate test data from election data have been performed successfully and all vote counters have been zeroed. An attempt to open polls with non-zero counters: 1. must be recorded in the audit log, and 2. an election worker must be clearly notified of the event. **Discussion** Jurisdictions that allow early voting before the traditional election day should document that a distinction is made between the opening and closing of the polls. This can occur only once per election, with the suspension and continuance of voting between days of early voting. The open-polls operation, which requires zeroed counters, is performed only when early voting commences; the continuation of voting that was suspended overnight does not require that counters be zeroed again.	BMD, CCOS, PCOS, TDP
SMTTVS-32	1.1.4-A – Voting and casting the ballot	The voting system must provide a ballot to each voter containing contests and contest choices using all voting variations that are indicated in the voting system implementation statement.	EMP, TDP

Key	Summary	Description	Component/s
SMTTVS-33	1.1.4-B – Control ballot configuration	The voting system must, where applicable: 1. activate all portions of the ballot the voter is entitled to vote on; 2. disable all portions of the ballot the voter is not entitled to vote on; and 3. enable the selection of the ballot configuration that is appropriate to the party affiliation declared by the voter in a primary election. **Discussion** This requirement does not apply to pre-printed paper ballots. For on-demand ballot printing systems, item 3 requires that the proper ballot style be selected for the voter and the appropriate ballot be printed for the voter's use. For an electronic display or ballot marking device, items 1-3 would be required, where poll workers may control the ballot configuration by using an activation device, issuing a token, or following other jurisdictional procedures to select the appropriate ballot style.	BMD, EMP, Integration, TDP
SMTTVS-34	1.1.4-C – Precinct splits, Casting	Each ballot that is issued to a voter must include contests that are associated with a district that the voter's residential address falls within. **Discussion** If a precinct is not entirely contained in the district associated with the precinct, multiple ballot styles must be available to ensure that each voter in the precinct receives a ballot that only contains contests for which they are eligible to vote.	CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-35	1.1.4-D – Ballot rotation, Casting	The order of contest options listed on each ballot must be in the order prescribed. The voting system must be able to correctly associate a voter's choice with the associated contest choice independent of where it appears on a specific voter's ballot. **Discussion** Many states require contest choice position order to be rotated on different ballots to prevent bias for or against a choice based on position listed.	CCOS, EMP, PCOS, TDP
SMTTVS-36	1.1.4-E – Partisan closed primary ballot	The voting system must provide a type of ballot, used in a partisan primary election, to the voter that only contains contests associated with a specific party to which the voter is registered in addition to any nonpartisan contests that the voter is eligible to make choices. **Discussion** This type of ballot is used in states that run *closed primary elections* (voter is issued a ballot based on party of registration), *partially closed primary elections* (voter can receive a party-specific ballot that is different from their registration or an unaffiliated voter can choose a party ballot) and *partially open primary elections* (voters do not register by party and choose a party-specific ballot for the election).	CCOS, EMP, PCOS, TDP
SMTTVS-38	1.1.4-G – Indicate party	The voting system must provide a type of ballot associated with:	BMD, EMP, TDP

Key	Summary	Description	Component/s
	affiliations and endorsements	1. a *partisan primary election* that identifies the party associated with each listed primary election contest (all listed contest options are affiliated with the listed party); and 2. a *partisan general election* that identifies the affiliated/endorsing party of each contest choice.	
SMTTVS-39	1.1.4-H – Write-in contest options	The voting system must be capable of enabling and recording the voter's write-in of desired candidate names. **Discussion** A write-in is a contest option on the ballot that permits the voter to identify a candidate of choice that is not already listed as a contest option and is captured when the ballot is cast. State rules determine when a write-in candidate option may be placed as a contest option on the ballot and what qualifies as a valid write-in selection that may be counted.	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-40	1.1.4-I – Write-in reconciliation	The voting system must be capable of gathering and recording write-in votes within a voting process that allows for reconciliation of aliases and double votes. **Discussion** Reconciliation of aliases means allowing 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.	EMP, TDP

Key	Summary	Description	Component/s
SMTTVS-41	1.1.4-J – N-of-M contest, Casting	For the N-of-M contest, the voting system must be capable of gathering and recording votes in a contest where the voter may choose up to a specified number of choices from a list of contest options. These selections are independent of selections in any other contest. **Discussion** A baseline N-of-M contest is one where a voter is allowed N contest choices from a list of M choices and where votes are tallied independently of any other contest options on the ballot. N includes 1 (vote for one contest or typically a measure) or any larger number. If N is larger than M, all choices listed will be selected. It can be used for *approval voting* by setting N equal to M. It can also be used for *limited voting* by setting N to be less than the number of seats being elected.	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-51	1.1.5-A – Casting and recording	The voting system must support casting a ballot, recording each vote precisely as indicated by the voter subject to the rules of the election jurisdiction, and creating a cast vote record that can be tabulated and audited.	BMD, CCOS, EMP, Integration, TDP
SMTTVS-52	1.1.5-B – Ballot orientation	The voting system, when using pre-printed ballots, must either: 1. correctly mark pre-printed ballots regardless of whether they are loaded upside down, right side up, forward, or reversed; or 2. detect and reject pre-printed ballots that are oriented incorrectly.	BMD, Integration, TDP

Key	Summary	Description	Component/s
SMTTVS-53	1.1.5-C – Record contest selection information	The voting system must record contest selection information in the CVR that includes: 1. all contest selections made by the voter for all supported vote variations; and 2. positions on the ballot associated with each contest selection made by the voter when multiple selections are permitted, if applicable. **Discussion** For item 2, some contests may place candidate choices on the same line of the ballot, therefore the positions of the candidates may need to be recorded.	CCOS, EMP, PCOS, TDP
SMTTVS-54	1.1.5-D – Record write-in information	The voting system must record write-in information in the CVR that includes: 1. identification of write-in selections made by the voter; 2. the text of the write-in, when using a BMD or other device that marks the ballot for the voter; 3. an image or other indication of the voter's write-in markings; and 4. the total number of write-ins in the CVR.	CCOS, EMP, Integration, PCOS, TDP
SMTTVS-55	1.1.5-E – Record election and contest information	The voting system must record additional contest information in the CVR that includes: 1. identification of all contests in which a voter has made a contest selection; 2. identification of all overvoted and undervoted contests; 3. the number of write-ins recorded for the contest; and 4. identification of the party for partisan ballots or partisan contests.	CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		Discussion For identification of the party, a ballot in a *partisan primary election* may in some cases contain contests for different parties. Thus, an indication as to partisanship of the contests is required.	
SMTTVS-56	1.1.5-F – Record ballot selection override information	The voting system, if recording voter selections differently than as marked due to election or contest rules in effect, must record information in the CVR that includes: 1. identification of the original ballot selections made by the voter; 2. identification of the changed voter selections; and 3. identification of the reasons for the changes. **Discussion** When marking a ballot by hand, a voter may vote in contests in which the voter is not allowed to make contest selections. For example, a voter may elect to vote straight party, but then make contest selections in contests which differ from the political party contest choices. Election or contest rules may cause a scanner to invalidate the contest markings or require other actions.	EMP, PCOS, TDP
SMTTVS-57	1.1.5-G – Record audit information	The voting system must be capable of recording audit-related information in the CVR or collection of CVRs as they are created, that includes: 1. identification of the specific creating device such as a serial number; 2. identification of the geographical location of the device; 3. identification of the ballot style corresponding to the CVR;	CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		4. identification of the corresponding voted ballot; 5. for multi-sheet ballots, identification of the individual sheet corresponding to the CVR, along with the identification of the ballot style; 6. identification of the batch containing the corresponding voted ballot, when applicable; and 7. sequence of the corresponding voted ballot in the batch, when applicable. **Discussion** Item 2 can be any identification scheme that is preferential in the jurisdiction, e.g., polling place name, address, geographical coordinates, etc. Item 4 can be satisfied by printing a unique ID on the ballot as it is scanned and including that ID in the corresponding CVR. Item 5 ensures that every sheet of a multi-sheet ballot contains the sheet number as well as the ballot style ID. This way, a ballot style ID could be defined to include all sheets, or each sheet could be defined with a unique ballot style. Items 6 and 7 are necessary when ballot batching is in effect.	
SMTTVS-58	1.1.5-H – Store and link corresponding image	The voting system must be capable of storing an image of a paper ballot and linking this image to the specific associated CVR. **Discussion**	CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		The image could be linked to the CVR by, for example, creating a filename for the image that is the same as the identifier from item 4 in Requirement *1.1.5-G – Record audit information*.	
SMTTVS-59	1.1.6-A – Detect and prevent ballot style mismatches	The voting system must detect ballot style mismatches and prevent votes from being tabulated or reported incorrectly due to a mismatch. **Discussion** For example, if the ballot styles loaded on a scanner disagree with the ballot styles that were used by vote-capture devices, the system will raise an alarm and prevent the incorrect ballot styles from being used during tabulation. Otherwise, votes could be credited to the wrong contest options. Such a mismatch should have been detected and prevented during L&A testing but if it was not, it needs to be detected and prevented before tabulation begins.	BMD, CCOS, EMP, Integration, PCOS, TDP
SMTTVS-60	1.1.6-B – Detect and reject ballots that are oriented incorrectly	The voting system must 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.	BMD, CCOS, Integration, PCOS, TDP
SMTTVS-61	1.1.6-C – Ballot separation	Batch-fed scanners, in response to unreadable ballots, write-ins, and other designated conditions, must do one of the following:	CCOS, TDP

Key	Summary	Description	Component/s
	when batch feeding	1. out stack the ballot (that is, divert to a stack separate from the ballots that were normally processed); 2. stop the ballot reader and display a message prompting the election official to remove the ballot; 3. mark the ballot with an identifying mark to facilitate its later identification; and/or 4. if the ballot image uniquely identifies its corresponding ballot, use electronic adjudication to segregate the ballot. **Discussion** Item 4 allows the ballot image to be segregated if, for example, an identifier is printed on the ballot as it is scanned, so that the image of the ballot also contains this identifier. Without a unique identifier or other marking, the ballot image itself does not facilitate finding the corresponding paper ballot.	
SMTTVS-62	1.1.6-D – Overvotes, undervotes, blank ballots	Voter-facing scanners must provide a function that can be activated by election officials to stop the scanning process and display a message which will enable the removal and correction of the ballot in response to the following ballot conditions: 1. ballots containing overvotes in a designated contest; 2. ballots containing undervotes in a designated contest; 3. ballots containing contests that were not voted; and 4. blank ballots.	EMP, PCOS, TDP

Key	Summary	Description	Component/s
		Related requirements: 7.3-H – Overvotes 7.3-I – Undervotes	
SMTTVS-63	1.1.6-E – Write-ins, Ballot handling for vote-capture devices	Voter-facing scanners, when scanning a ballot containing a write-in vote, must either: 1. segregate the ballot in a manner that facilitate its later identification; or 2. if the ballot image uniquely identifies its corresponding ballot, use electronic adjudication to segregate the ballot. **Discussion** The requirement to separate ballots containing write-in votes is not applicable to systems in which a BMD encodes write-in votes in a machine-readable form. In this instance, a scanner generates individual tallies for all written-in candidates automatically. Separation of ballots containing write-in votes is only necessary in systems that require the allocation of write-in votes to specific candidates to be performed manually.	PCOS, TDP
SMTTVS-64	1.1.6-F – Ability to clear mis-fed ballots	If multiple feed or misfeeding (jamming) occurs, batch-fed scanners must: 1. permit the operator to remove the ballots causing the error and reinsert them in the input hopper (if unread) or insert them in the ballot box (if read); and 2. prevent duplicate scanning of the ballots. **Discussion**	CCOS, TDP

Key	Summary	Description	Component/s
		Number 2 deals with whether CVRs have been created for the ballots that were jammed.	
SMTTVS-65	1.1.6-G – Scan to manufacturer specifications	The voting system must have the capability to provide a report of the mark detection thresholds that have been used to program the scanner so that the information is available upon request. **Discussion** Manufacturers must not make their specifications proprietary; auditors must be able to understand what and what does not constitute a valid voter mark on a particular scanner.	CCOS, EMP, Integration, PCOS, TDP
SMTTVS-66	1.1.6-H – Accurately detect imperfect marks	The voting system must detect a *1 mm thick line* that: 1. is made with a #2 pencil that crosses the entirety of the contest option position on its long axis; 2. is centered on the contest option position; and 3. is as dark as can practically be made with a #2 pencil. **Discussion** 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;	CCOS, PCOS, TDP

Key	Summary	Description	Component/s
		• the size and shape of the scanner's aperture; • the color of the ink; • the sensed background-white and maximum-dark levels; and • the calibration of the scanner. The mark specified in this requirement is intended to be less than 100 % perfect, but reliably detectable. In plain language: scanning technologies may vary, but as a minimum requirement, all of them should be capable of reliably reading *this* mark.	
SMTTVS-67	1.1.6-I – Ignore extraneous marks inside voting targets	The voting system must include a capability to recognize any imperfections in the ballot stock, folds, and similar insignificant marks appearing inside the voting targets and not record them as votes. **Discussion** Insignificant marks appearing inside of the voting targets could be detected as votes, thus the capability to recognize the ballot folds or imperfections must be included as a part of the voting system. It may not be possible to completely eliminate this problem in all cases depending on scanner thresholds for detecting marks. **Related requirements:** 1.1.6-G – Scan to manufacturer specifications	CCOS, PCOS, TDP
SMTTVS-68	1.1.6-J – Marginal marks, without bias	The detection of marginal marks from manually marked paper ballots must not show a bias. **Discussion**	CCOS, PCOS, TDP

Key	Summary	Description	Component/s
		Bias errors are not permissible in any system. 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.	
SMTTVS-69	1.1.6-K – Repeatability	The determination of a vote on a manually marked paper ballot must be repeatable, such that it never changes from a vote to a non-vote or from non-vote to a vote. **Discussion** Since it is technically impossible to achieve repeatable readings of ballots containing marks that fall precisely on the scanning threshold, changing between a non-vote and a marginally machine-readable mark is allowed. Similarly, changing from a valid vote and a marginally machine-readable mark is allowed.	CCOS, PCOS, TDP
SMTTVS-70	1.1.7-A – Exiting or suspending election mode	The voting system must provide designated functions for exiting or suspending an election mode in which voting is permitted. **Discussion** When voting is conducted across multiple days, for example, during early voting, these requirements are still applicable even though the election itself may not be over; this is with the exception of requirement *1.1.7-E – Prevent re-entering election mode*, which deals with preventing re-opening of the polls once they have been closed on election day.	BMD, CCOS, PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-71	1.1.7-B – No voting when voting is stopped	The voting system must prevent the further activation, marking, or casting of ballots by any device once the voting has stopped. **Discussion** This requirement is applicable to voter-facing scanners, batch-fed scanners and any other device that enables the activation or tabulation of the voting process. However, a BMD cannot prevent a voter from marking a paper ballot with a writing utensil after polls have closed. This needs to be prevented through jurisdictional procedure.	BMD, CCOS, PCOS, TDP
SMTTVS-72	1.1.7-C – Voting stop integrity check	The voting system must provide an internal test that verifies that the prescribed closing or suspension procedures have been followed.	BMD, CCOS, PCOS, TDP
SMTTVS-73	1.1.7-D – Report on voting stop process	The voting system must provide a means to produce a diagnostic test record that verifies the sequence of events, which indicate that the voting mode has been deactivated or suspended.	BMD, CCOS, Integration, PCOS, TDP
SMTTVS-74	1.1.7-E – Prevent re-entering election mode	The voting system must not be capable of re-entering an election mode, in which voting is permitted, once the closing procedures have been completed for an election without an explicit override authorized by an administrator. **Discussion** When early voting is conducted across multiple days, this requirement does not prevent reopening of the polls on the following day.	BMD, CCOS, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		Related requirements: 11.3.1-B – Multi-factor authentication for critical operations	
SMTTVS-75	1.1.8-A – Tabulation	The voting system must support the tabulation function for all voting variations indicated in the implantation statement. This function includes: 1. extracting the valid votes from each ballot cast according to the defined rules; 2. creating and storing a CVR that contains the disposition of each contest selection as well as the disposition of each contest choice that is eligible to be cast; and 3. accumulation and aggregation of contest results and ballot statistics. **Discussion** Results accumulation and aggregation takes place at multiple levels within the voting system. Each tabulation unit must perform this function and must have the ability to transmit the CVRs and results to the election management system (EMS) for jurisdiction wide accumulation and aggregation.	CCOS, EMP, Integration, PCOS, TDP
SMTTVS-76	1.1.8-B – Partisan primary elections	In partisan primary elections, the voting system must be capable of reporting separate totals for the number of ballots read and the number of ballots counted for each political party. This is independent of whether the primary type is closed or open. **Discussion** From a tabulation perspective, there are two types of partisan primary election ballots. A *closed primary ballot* is one in which a ballot is limited to contests	CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		associated with one political party and any nonpartisan contests. An *open primary ballot* is one which contains contests from all parties on the same ballot, but the voter may only select contest choices applicable to a single party.	
SMTTVS-77	1.1.8-B.1 – Tabulation of a closed primary ballot	The voting system must support the tabulation of ballots that are specific to a party or are nonpartisan and must be able to report combined totals for nonpartisan contests no matter what party ballot the contest appears on.	CCOS, EMP, Integration, PCOS, TDP
SMTTVS-80	1.1.8-C – Write-ins, Tabulation	The voting system must be capable of 1. tabulating votes for write-in candidates with separate totals for each contest choice, and 2. tabulating valid individual write-in candidate totals in each contest. **Discussion** Tabulation of candidate names that are manually written in on a hand-voted paper ballot can only be tabulated as an aggregate total in each contest. Each name must be adjudicated from graphical images of the contest write-in area or from the ballot itself to determine the name of the candidate. When names are typed on an electronic voting unit such as a BMD, although the entered names must be recorded, only aggregate contest write-in totals are tabulated. Each individual write-in name must be adjudicated for validity before they can be aggregated. In most states, a write-in	CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		candidate must be registered to be valid. State rules also determine acceptable variations in the written name for the candidate to be credited with the vote. State rules also determine treatment of a written-in name of a candidate already listed on the ballot.	
SMTTVS-81	1.1.8-D – Ballot rotation, Tabulation	When the order of contest choices within a contest varies by ballot style, the voting system must tabulate votes for each contest selection independent of a contest selections location in the contest on the ballot. **Discussion** This means that ballot rotation will not impact the correctness of the count.	CCOS, EMP, Integration, PCOS, TDP
SMTTVS-84	1.1.8-G – Precinct splits, Tabulation	When multiple ballot styles are associated with a specific precinct, the voting system must be capable of keeping separate totals for the number of ballots read and counted for each ballot style or split. Tabulation must not be affected by variation of contest selection locations from one ballot style to another.	CCOS, EMP, Integration, PCOS, TDP
SMTTVS-85	1.1.8-H – N-of-M contest, Tabulation	For N-of-M voting, the voting system must be capable of tabulating votes, overvotes, and undervotes in contests where the voter is permitted to select up to a specified number of contest choices. **Discussion** An N-of-M contest is one where a voter is allowed *N contest selections* from a list of *M choices* and where votes are tallied independent of any other contest choices. N includes 1 vote (one vote for one contest or typically a measure) or any larger	CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		number. Contest choices include those where the contest choices are candidates for a specific office or measures/referenda where there are usually only two contest choices (Yes/No, For/Against) but may also be a list of choices (Tax rate A, Tax rate B, Tax rate C). An N-of-M contest is used for *approval voting* by setting N to be equal to M. This type of contest is used for *limited voting* by setting N to be less than the number of seats being elected. An N-of-M contest is also used for top-2 primary contests (blanket primary contests), where N is always 1 but the two candidates with the most votes will be on the general election ballot.	
SMTTVS-92	1.1.9-A – Post-election reports	The voting system must have the capability to create post-election reports that contain cast ballot counts and vote counts for contests on the ballot types served by precincts or splits of precincts.	BMD, CCOS, EMP, Integration, PCOS, TDP
SMTTVS-93	1.1.9-B – Report categories of cast ballots	The voting system must have the capability to report the number of ballots cast in total and broken down by ballot style. This is in addition to the associated units of political geography for the following categories of ballots cast: 1. All read ballots and all counted ballots, 2. For multi-page ballots, the number of different pages read, and number counted, 3. Read ballots and counted ballots that require review, 4. Absentee read and counted ballots, and 5. Blank ballots (ballots containing no votes).	CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		Discussion Associated units of political geography may also include state, county, city, town or township, ward, and districts.	
SMTTVS-94	1.1.9-C – Report categories of votes	The voting system must have the capability to report the following categories of votes: 1. in-person voting, 2. absentee voting, 3. write-ins, 4. accepted reviewed ballots, and 5. rejected reviewed ballots.	CCOS, EMP, Integration, PCOS, TDP
SMTTVS-95	1.1.9-D – Reporting combined or split precincts	The voting system must be capable of generating reports that consolidate vote data from selected precincts. **Discussion** 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 data from the voting location by precinct.	CCOS, EMP, Integration, PCOS, TDP
SMTTVS-96	1.1.9-E – Report counted ballots by contest	The voting system must have the capability to report the number of counted ballots for each relevant N-of-M or cumulative voting contest. **Discussion**	CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		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. N-of-M in this requirement includes the most common type of contest, 1-of-M.	
SMTTVS-97	1.1.9-F – Report votes for each contest option	The voting system must have the capability to report the vote totals for each contest option in each relevant N-of-M or cumulative voting contest. **Discussion** N-of-M in this requirement includes the most common type of contest, 1-of-M.	CCOS, EMP, Integration, PCOS, TDP
SMTTVS-98	1.1.9-G – Report overvotes for each contest	The voting system must have the capability to report the number of overvotes for each relevant N-of-M or cumulative voting contest.	CCOS, EMP, Integration, PCOS, TDP
SMTTVS-99	1.1.9-H – Report undervotes for each contest	The voting system must have the capability to report the number of undervotes for each relevant N-of-M or cumulative voting contest. **Discussion** Counting ballots containing undervotes instead of votes lost to undervoting is insufficient.	CCOS, EMP, Integration, PCOS, TDP
SMTTVS-101	1.1.9-J – Precinct reporting devices,	When more than one vote-capture device is used in a polling place, the voting system must have the capability to consolidate the data tabulated by each unit into a single report for the polling place. **Discussion**	Integration, PCOS, TDP

Key	Summary	Description	Component/s
	reporting device consolidation	This requirement essentially requires precinct-based vote-capture devices to be able to consolidate voting data for the purposes of issuing one consolidated report.	
SMTTVS-102	1.1.9-K – Precinct reporting devices, no tallies before polls close	The voting system must prevent the printing of vote data reports and extracting vote tally data while the polls are open. **Discussion** Providing ballot counts does not violate this requirement. The prohibition is against providing vote totals for ballot contests.	PCOS, TDP
SMTTVS-103	1.1.9-L – Report read ballots by party	The voting system must have the capability of reporting separate totals for each party in primary elections when reporting categories of read and counted cast ballots.	CCOS, EMP, Integration, PCOS, TDP
SMTTVS-104	1.1.9-M – Reports are time stamped	All reports must include the date and time of the report's generation, including hours, minutes, and seconds.	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-105	1.2-A – Assessment of accuracy	The voting system's accuracy must be assessed by using a combination of evidence items gathered during the entire course of testing, including: 1. A measurement of how accurately voter marks are recognized as valid or not valid according to manufacturer specifications. 2. A measurement of how accurately voter marks are tabulated and reported as results.	CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		3. An assessment of whether the remaining VVSG requirements are satisfied. **Discussion** The data collected during the testing of this requirement contributes substantially to the evaluations of reliability, accuracy, and misfeed rate.	
SMTTVS-106	1.2-B – Reliably detectable marks	The voting system must detect marks on the ballot consistent with system mark specifications and differentiate between voter-made marks constituting votes versus voter-made marginal marks or other marks on the ballot. **Discussion** The specification may have parameters for different configuration values. It should also state the degree of uncertainty.	CCOS, PCOS, Security, TDP
SMTTVS-107	1.2-C – Minimum ballot positions	A minimum of 10,000,000 ballot positions must be read by the voting system and tabulated accurately. **Discussion** The value of 10,000,000 ballot positions is taken from *VVSG 1.0 [VVSG2005]*, however it is used here as the minimum number of ballot positions to test without error. If a larger number of ballot positions is used, there still can be no error.	CCOS, Integration, PCOS, TDP
SMTTVS-108	1.2-D – Handle maximum volume	The voting system must be able to handle the maximum volume of activities in conditions approximating normal use in an entire election process according to manufacturer specifications. **Discussion**	BMD, CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		This requirement should be verified through operational testing if the limit is practically testable.	
SMTTVS-109	1.2-E – Respond gracefully to stress of system limits	Certain conditions tend to overload the system's capacity to process, store, or report data. These conditions include attempts to process more than the expected number of precincts, and to process more than the expected volume or ballot tabulation rate. Therefore, the voting system must be able to respond to the above conditions that overload the system's capacity, by ensuring that the voting system does not fail or halt suddenly. The voting system must give adequate warning if it is to fail or halt for any reason. **Discussion** This requirement should be verified through operational testing if the limit is practically testable.	BMD, CCOS, EMP, Integration, PCOS, Security, TDP
SMTTVS-110	1.2-F – No single point of failure	The voting system must protect against a single point of failure that would prevent further voting at the polling place. **Discussion** The intent of this requirement is to prevent, at the polling place, a situation in which failure of a component would prevent voting. This can be addressed in various ways, including being able to swap in/out devices without loss of data.	PCOS, Security, TDP
SMTTVS-111	1.2-G – Misfeed rate benchmark	The voting system misfeed rate must not exceed 0.002 (1 / 500). **Discussion**	BMD, CCOS, PCOS, TDP

Key	Summary	Description	Component/s
		Multiple feeds, misfeeds (jams), and rejections of ballots that meet all manufacturer specifications are all treated collectively as "misfeeds" for benchmarking purposes; that is, only a single count is maintained.	
SMTTVS-112	1.2-H – Protect against failure of input and storage devices	The voting system must withstand, without loss of data, the failure of any data input or storage device. **Discussion** The intent of this requirement is to prevent votes from being permanently lost due to the failure of a storage device that contains votes. For example, if a scanner fails, the voting system must have the ability to swap in a replacement data input device without the losing cast vote records that were previously recorded by the failed scanner.	CCOS, EMP, PCOS, Security, TDP
SMTTVS-113	1.2-I – FCC Part 15 Class A and B conformance	Voting devices must comply with the requirements of the *Rules and Regulations of the Federal Communications Commission, Part 15, Class B [FCC19a]*. 1. Voting devices located in polling places must minimally comply with Class B requirements. 2. Voting devices located in non-polling place settings such as back offices must minimally comply with Class A requirements.	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-114	1.2-J – Power supply from	Voting devices located in polling places must be powered by a 120 V, single phase power supply derived from typical energy service providers. **Discussion**	BMD, CCOS, PCOS, TDP

Key	Summary	Description	Component/s
	energy service provider	It is assumed that the AC power necessary to operate the voting system will be derived from the existing power distribution system of the facility housing the polling place. This single-phase power may be a leg of a 120/240 V single phase system, or a leg of a 120/208 V three-phase system, at a frequency of 60 Hz.	
SMTTVS-115	1.2-K – Power port connection to the facility power supply	Voting devices located in polling places must comply with Class B emission limits affecting the power supply connection to the energy service provider. **Discussion** The normal operation of an electronic system can produce disturbances that will travel upstream and affect the power supply system of the polling place, creating a potential deviation from the expected electromagnetic compatibility of the system. The issue is whether these actual disturbances (after possible mitigation means incorporated in the equipment) reach a significant level to exceed stipulated limits.	BMD, PCOS, TDP
SMTTVS-116	1.2-L – Leakage from grounding port	Voting devices located in polling places must comply with limits of leakage currents effectively established by the trip threshold of all listed Ground Fault Current Interrupters (GFCI), if any, installed in the branch circuit supplying the voting system. **Discussion** Excessive leakage current is objectionable for two reasons: • For a branch circuit or wall receptacle that could be provided with a GFCI (depending upon the wiring practice applied at the particular polling place),	BMD, PCOS, TDP

Key	Summary	Description	Component/s
		leakage current above the GFCI built-in trip point would cause the GFCI to trip and therefore disable the operation of the system. • Should the power cord lose the connection to the equipment grounding conductor of the receptacle, a personnel hazard would occur. (Note the prohibition of “cheater” adapters in the **Discussion** of general requirements for the polling place.)	
SMTTVS-117	1.3-A – Reporting of manufacturer-performed tests	Each test provided in a manufacturer-submitted report of internal testing performed (technical data package (TDP)) must, at least, include the following information: 1. requirement(s) under test; 2. items under test to exercise a given requirement; 3. pass-fail criteria necessary to determine whether a requirement has passed the test of conformity to the requirement; 4. evidence (observations, data) expected to provide justification for satisfying or failing a given pass-fail condition; 5. test procedures necessary to provide, observe, record, analyze, and interpret this evidence relative to pass-fail criteria; 6. where applicable, descriptions of the causes of variation, ambiguity, noise, or observed errors in observed and recorded evidence during tested procedures;	CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		7. where applicable, descriptions of any necessary techniques, procedures, or processes applied to normalize or clean data prior to subjecting it to data analysis and interpretation relative to pass-fail criteria; 8. report of actual tests performed and their results; and 9. description and justification if a given test cannot be fully performed or exercised due to internal resource constraints, including description of alternative means of verification. **Discussion** This is a documentation requirement. Its intent is to ensure a baseline set of information provided in manufacturer-submitted report of manufacturer-performed internal testing submitted as part of the TDP. Manufacturers may likely have additional information, formatting, etc., as part of their particular testing practices, that they will include as is consistent with their internal testing best-practices.	
SMTTVS-118	1.3-B – Coverage of manufacturer-performed tests	Each requirement identified in a manufacturer-submitted implementation statement or conformance statement must describe one-or-more tests in their test-plan describing how it was tested. **Discussion** This requirement is to ensure that all requirements identified in the respective implementation and conformance statements are covered by the submitted test-plan	CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-482	2.1-A – Acceptable programming languages	Application logic must be produced in a high-level programming language that has all of the following control constructs: 1. sequence; 2. loop with exit condition (for example, for, while, or do-loops); 3. if/then/else conditional; 4. case conditional; and 5. block-structured exception handling (for example, try/throw/catch). **Discussion** A list of acceptable programming languages may be specified by the EAC in conjunction with voting system test labs. This requirement can be satisfied by using COTS extension packages to add missing control constructs to languages that could not otherwise conform. 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, for example, by wrapping it in callable units expressed in the prevailing language to minimize the number of places that special code appears.	BMD, CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		Previous versions of VVSG required voting systems to handle such errors by some means, preferably using programming language exceptions (*[VVSG2005] 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. 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." *[Moulding89]* 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	

Key	Summary	Description	Component/s
		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 *2.1-B – COTS language extensions are acceptable*).	
SMTTVS-483	2.1-B – COTS language extensions are acceptable	Requirement *2.1-A – Acceptable programming languages* may be satisfied by using COTS extension packages to add missing control constructs to languages that could not otherwise conform. **Discussion** The use of non-COTS extension packages or manufacturer-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.	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-484	2.1-C – Acceptable coding conventions	Application logic must adhere to a published, credible set of coding rules, conventions, or standards (called "coding conventions") that enhance the workmanship, security, integrity, testability, and maintainability of applications. **Discussion**	BMD, CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		Coding conventions may be specified by the EAC in conjunction with voting system test labs. 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. 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. 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.	

Key	Summary	Description	Component/s
		As discussed, prescriptive coding conventions not directly related to integrity and transparency have been avoided in favor of published, credible conventions. Coding conventions are considered to be *published* 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. This requirement attempts to clarify the "published, reviewed, and industry-accepted" language appearing in previous iterations of the VVSG, but the intent of the requirement is unchanged. Coding conventions are considered to be *credible* if at least two different organizations with no ties to the creator of the rules or to the manufacturer seeking conformity assessment, and which are not themselves voting equipment manufacturers, independently decided to adopt them and made active use of them at some point within the three years before conformity assessment was first sought. This requirement attempts to clarify the "published, reviewed, and industry-accepted" language appearing in previous iterations of the VVSG, but the intent of the requirement is unchanged. Coding conventions evolve, and it is desirable for voting systems to be aligned with modern practices.	

Key	Summary	Description	Component/s
SMTTVS-485	2.1-D – Records last at least 22 months	All systems must maintain the integrity of election management, voting, and audit data, including cast vote records (CVRs), 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.	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-486	2.1.1-A – General build quality	All manufacturers of voting systems must practice proper workmanship by: 1. adopting and adhering to practices and procedures that ensure their products are free from damage or defect that could make them unsatisfactory for their intended purpose; and 2. ensuring 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.	BMD, CCOS, EMP, Integration, PCOS, TDP
SMTTVS-487	2.1.1-B – Durability estimation	A manufacturer must submit a warranty model to the EAC, testing labs, and customers, which includes for each product its relevant components and associated consumables: 1. estimated replacement rates (e.g., 3 years, 10 years); 2. estimated costs per replacement; 3. estimated warranty types and costs; 4. associated replacement policies, services, and available maintenance agreements; and	BMD, CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		5. plans for collecting, maintaining, and reporting data to the EAC to support and validate estimates. **Discussion** A number of factors associated with the durability of a product or its components can be highly variable and even particular to the type of components (e.g., COTS, consumables). This variance is also applicable to the resources of a given manufacturer. Thus, instead of prescribing a pre-estimated number for all manufacturers, the manufacturers are asked to make these estimates relative to their own products, components, and resources, and to provide the basis for these estimates (these warranties, replacement periods, etc.) to the EAC, labs, and customers. In this way, manufacturers can perform estimates most relevant to their chosen manufacturing strategies (i.e., COTS-centric vs. custom-built, and so on).	
SMTTVS-488	2.1.1-C – Durability of paper	Paper specified for use with the voting system must conform to the applicable specifications contained within the *Government Paper Specification Standards, February 1999 No. 11*, or the government standards that have superseded them. **Discussion** This is to ensure that paper records will be of adequate quality to survive the handling necessary for recounts, audits, etc. without problematic degradation. The Government Paper Specification Standards include different specifications for	BMD, CCOS, PCOS, TDP

Key	Summary	Description	Component/s
		different kinds of paper. As of 2020-02-29, the *Government Paper Specification Standards, February 1999 No. 11 [GPO19].*	
SMTTVS-489	2.1.1-D – Ensure compatibility of specified paper and ink	Ink specified for use with the voting system must be compatible with the paper specifications provided by the manufacturer. **Discussion** The purpose of this requirement is to ensure that both the types of ink and paper used with a given system are compatible with each other in an effort to avoid many of the side-effects of mismatched ink and paper (e.g., excessive smudging).	CCOS
SMTTVS-490	2.1.2-A – Electronic device maintainability	Electronic devices must 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; and 3. labels and alarms related to failures.	BMD, CCOS, EMP, Integration, PCOS
SMTTVS-491	2.1.2-B – System maintainability	Voting systems must allow for: 1. a non-technician to easily detect that the equipment has failed; 2. a trained technician to easily diagnose problems; 3. easy access to components for replacement; 4. easy adjustment, alignment, and tuning of components; and 5. low false alarm rates (that is, indications of problems that do not exist)	BMD, CCOS, EMP, PCOS

Key	Summary	Description	Component/s
SMTTVS-492	2.1.2-C – Nameplate and labels	All voting devices must: 1. Display a permanently affixed nameplate or label containing the name of the manufacturer, the name of the device, its part or model number, its revision identifier, its serial number, and if applicable, its power requirements. 2. If service or preventative maintenance is required, 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. 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.	BMD, CCOS, PCOS
SMTTVS-494	2.2-A – User-centered design process	The manufacturer must submit a report providing documentation that the system was developed following a user-centered design process. The report must include, at a minimum: 1. a listing of user-centered design methods used; 2. the types of voters and election workers included in those methods; 3. how those methods were integrated into the overall implementation process; and 4. how the results of those methods contributed to developing the final features and design of the voting system.	CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		Discussion The goal of this requirement is to allow the manufacturer to demonstrate, through the report, the way their implementation process included user-centered design methods. *ISO-9241-210:2019 Ergonomics of human-system interaction—Part 210: Human-centered design for interactive systems [ISO19b]* provides requirements and recommendations for human-centered principles and activities throughout the life cycle of computer-based interactive systems. It includes the idea of iterative cycles of user research to understand the context of use and user needs, creating prototypes or versions, and testing to confirm that the product meets the identified requirements. This requirement does not specify the exact user-centered design methods to be used, or their number or timing. The ISO group of requirements, Software engineering – Software product Quality Requirements and Evaluation (SQUARE) -- Common Industry Format (CIF) for Usability_ includes several standards that are a useful framework for reporting on user-centered design activities and usability reports: • *ISO/IEC TR 25060:2010: General framework for usability-related information [ISO10]* • *ISO/IEC 25063:2014: Context of use description [ISO14]*	

Key	Summary	Description	Component/s
		• *ISO/IEC 25062:2006: Usability test reports [ISO06b]* • *ISO/IEC 25064:2013: User needs report [ISO13b]* • *ISO/IEC 25066:2016 Evaluation report [ISO16]*	
SMTTVS-496	2.3-A – Block-structured exception handling	Application logic must handle exceptions using block-structured exception handling constructs. **Discussion** The concept of "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) [MS20].[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." *[ISO00]* Previous versions of VVSG required voting systems to handle such errors by some means, preferably using programming language exceptions ([_VVSG2005] 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.	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		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." *[Moulding89]*.	
SMTTVS-497	2.3-B – Legacy library units	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 must be wrapped in callable units that check for the relevant error conditions and translate them into exceptions, and the remainder of application logic must use only the wrapped version. **Discussion** 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 by 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	BMD, CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		when exceptional conditions arise, whereas in a programming environment that had exceptions to begin with the analogous library functions would already do this.	
SMTTVS-498	2.3-C – Separation of code and data	Application logic must not compile or interpret configuration data or other input data as a programming language. **Discussion** The applicable requirement in VVSG2005 reads "Operator intervention or logic that evaluates received or stored data must 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 conventional programming languages that should not be exhibited by configuration data. Configuration data must be declarative or informative in nature, not imperative. For example: Configuration data can contain a template that informs a report generating application about the form and content of a report that it should generate. However, configuration data cannot contain instructions that are executed	BMD, CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		or interpreted to generate a report, essentially embedding the logic of the report generator inside the configuration data. The reasons for this requirement are: • mingling code and data is bad design, and • embedding logic within configuration data evades the conformity assessment process for application logic.	
SMTTVS-499	2.3-D – Hard-coded passwords and keys	Voting system software must not contain hard-coded, including the use of: 1. passwords, or 2. cryptographic keys. **Discussion** Many examples of this vulnerability have previously been identified in voting system software. Additional information about this vulnerability can be found at *MITRE CWE-259: Use of Hard-coded Password [MITRE20a]* and *MITRE CWE-321: Use of Hard-coded Cryptographic Key [MITRE20b].*	BMD, CCOS, EMP, Integration, PCOS, Security, TDP
SMTTVS-500	2.3.1-A – Unstructured control flow	Application logic must contain no unstructured control constructs. **Discussion** Although it is typically developed by the voting system manufacturer, border logic is constrained by the requirements of the third-party or COTS interface with which it interacts. 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	BMD, CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		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.	
SMTTVS-501	2.3.1-B – Goto	Arbitrary branches (also known as gotos) must not be used.	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-502	2.3.1-C – Intentional exceptions	Exceptions must only be used for abnormal conditions. Exceptions must not be used to redirect the flow of control in normal ("non-exceptional") conditions. **Discussion** "Intentional exceptions" cannot be used as a substitute for arbitrary branch. Normal, expected events, such as reaching the end of a file that is being read from beginning to end or receiving invalid input from a user interface, are not exceptional conditions and should not be implemented using exception handlers.	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-503	2.3.1-D – Unstructured exception handling	Unstructured exception handling (for example, On Error GoTo, setjmp/longjmp, or explicit tests for error conditions after every executable statement) is prohibited. **Discussion** 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 *2.3-B – Legacy library units*, is allowed. Similarly, it is not a problem that source code written in a high-level programming language is	BMD, CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		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.	
SMTTVS-505	2.4-A – Modularity	Application logic must be designed in a modular fashion, meeting all the criteria stated in the definition of a module, namely that: 1. It must be a structural unit of software or analogous logical design. 2. If it contains callable units, those callable units must be tightly coupled. 3. Coupling between modules (“inter-module coupling”) must: a. be loose, and b. occur over defined interfaces. 4. It must contain all elements needed to compile or interpret successfully. 5. It must have limited access to data in other modules. 6. It must be substitutable with another module whose interfaces match the original module. **Discussion** The modularity rules described here apply to the component submodules of a library.	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-506	2.4-B – Module testability	Each module must have a specific function that can be tested and verified independently of the remainder of the code. **Discussion**	BMD, CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		In practice, some additional modules (such as library modules) can be needed to compile the module being tested, but the modular construction allows the supporting modules to be replaced by special test versions that support test objectives.	
SMTTVS-507	2.4-C – Module size and identification	Modules must be small and easily identifiable, such as being: 1. 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; 2. no more than 5% of all callable units SHOULD exceed 60 lines in length; and 3. no callable units SHOULD exceed 180 lines in length. **Discussion** "Lines," in this context, are defined as executable statements or flow control statements with suitable formatting.	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-508	2.4-D – Large data structures in separate files	Read-only large data structures longer than 25 lines must be placed in separate files from other source code if the programming language permits it. **Discussion** In practice, this case has often been illustrated by the need to put read-only large lookup tables into separate files. However, the same notion could apply to other kinds of data structures.	BMD, CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-510	2.5-A – Self-modifying code	Application logic must not be self-modifying.	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-511	2.5-B – Unsafe concurrency	Application logic must be free of race conditions, deadlocks, livelocks, and resource starvation. **Discussion** In addressing this requirement, information should be provided in the TDP describing how *safe concurrency* was ensured relative to the design, implementation, and testing of the application logic.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-512	2.5.1-A – COTS compilers	If compiled code is used, it must only be compiled using a COTS compiler. **Discussion** This prohibits the use of arbitrary, nonstandard compilers and, consequently, the invention of new programming languages.	EMP, TDP
SMTTVS-513	2.5.1-B – Interpreted code, specific COTS interpreter	If interpreted code is used, it must only be run under a specific, identified version of a COTS runtime interpreter. **Discussion** This ensures that: • no arbitrary, nonstandard interpreted languages are used, and • the software tested and approved during the conformity assessment process does not change behavior because of a change to the interpreter	EMP, TDP

Key	Summary	Description	Component/s
SMTTVS-514	2.5.1-C – Prevent tampering with code	Programmed devices must prevent replacing or modifying executable or interpreted code (for example, by other programs on the system, by people physically replacing the memory or medium containing the code, or by faulty code) except where this access is necessary to conduct the voting process. **Discussion** This requirement can be satisfied through a combination of: • read-only memory (ROM), • the memory protection implemented by most popular COTS operating systems, • error checking, and • access and integrity controls.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-515	2.5.1-D – Prevent tampering with data	All voting devices must prevent access to or manipulation of configuration data, vote data, or audit records (for example, by physically 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. **Discussion** This requirement can be satisfied through a combination of: • the memory protection implemented by most popular COTS operating systems, • error checking, and	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		• access and integrity controls. Systems using mechanical counters to store vote data need to protect the counters from tampering. If vote data are stored on paper, the paper needs to be protected from tampering. Modification of audit records after they are created is never necessary.	
SMTTVS-516	2.5.2-A - Input validation and error defense	The voting system must: 1. monitor I/O operations; 2. validate all input against expected parameters, such as data presence, length, type, format, uniqueness, or inclusion in a set of whitelisted values; 3. report any input errors and how they were corrected; and 4. check information inputs to ensure that incomplete or invalid inputs do not lead to irreversible error. **Discussion** Input includes data from any input source: input devices (such as touch screens, keyboards, keypads, optical/digital scanners, and assistive devices), networking port, data port, or file. This general requirement applies to all programmed devices, while the specific ones following are only enforceable for application logic.	BMD, CCOS, EMP, Integration, PCOS, Security, TDP
SMTTVS-517	2.5.3-A – Escaping and encoding output	Software output must be properly encoded, escaped, and sanitized. **Discussion**	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		The output of a software module can be manipulated or abused by attackers in unexpected ways to perform malicious actions. Ensuring that outputted data is of an expected type or format assists in preventing this abuse. Additional information about this software weakness can be viewed at *MITRE CWE 116: Improper Encoding or Escaping of Output [MITRE20c].*	
SMTTVS-518	2.5.3-B – Sanitize output	The voting system must sanitize all output to remove or neutralize the effects of any escape characters, control signals, or scripts contained in the data which could adversely manipulate the output source. **Discussion** Output includes data to any output source: output devices (such as touch screens, LCD screens, printers, and assistive devices), networking port, data port, or file. This applies to all parts of the voting system including the election management system (EMS)	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-519	2.5.3-C – Stored injection	The voting system must sanitize all output to files and databases to remove or neutralize the effects of any escape characters, control signals, or scripts contained in the data which could adversely manipulate the voting system if the stored data is read or imported at a later date or by another part of the voting system.	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		Discussion A stored injection attack saves malicious data which is harmless when stored, but which is potent when read later in a different context or when converted to a different format. For example, a malicious script might be written to a file and do no harm to the voting machine, but later be evaluated and harmful when the file is transferred and read by the EMS. Input should also be filtered, but sanitizing stored output provides defense in depth	
SMTTVS-520	2.5.4-A – Mandatory internal error checking	Application logic that is vulnerable to the following types of errors must check for these errors at run time and respond defensively when they occur: 1. common memory management errors, such as out-of-bounds accesses of arrays, strings, and buffers used to manage data; 2. uncontrolled format strings; 3. CPU-level exceptions such as address and bus errors, dividing by zero, and the like; 4. variables that are not appropriately handled when out of expected boundaries; 5. numeric and integer overflows; 6. validation of array indices; and 7. known programming language specific vulnerabilities. **Discussion**	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		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.	
SMTTVS-521	2.5.4-B – 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 must be ranged-checked on every access. **Discussion** Range checking code should not be duplicated before each access. Clean implementation approaches include: • consistently using dedicated accessors (such as functions, methods, operations, subroutines, and procedures) that range-check the indices; • defining and consistently using a new data type or class that encapsulates the range-checking logic; • declaring the array using a template that causes all accessors to be range-checked; or • 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 can be provided by the programming environment, or they can be defined in application logic. If acceptable values of the	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		index do not form a contiguous range, a map structure can be more appropriate than a vector.	
SMTTVS-522	2.5.4-C – Buffer overflows	If an overflow does not automatically result in an exception, the application logic must explicitly check for and prevent the overflow.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-523	2.5.4-D – CPU traps	The application logic must implement such handlers as needed to detect and respond to CPU-level exceptions. **Discussion** For example, under Unix, a CPU-level exception would manifest as a signal, so a signal handler is needed. If the platform supports it, it is preferable to translate CPU-level exceptions into software-level exceptions so that all exceptions can be handled in a consistent fashion within the voting application. However, not all platforms support it.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-524	2.5.4-E – Garbage input parameters	All scalar or enumerated type parameters whose valid ranges as used in a callable unit (such as function, method, operation, subroutine, and procedure) do not cover the entire ranges of their declared data types must be range-checked on entry to the unit. **Discussion** This applies to parameters of numeric types, character types, temporal types, and any other types for which the concept of range is well-defined. In cases where the	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		restricted range is frequently used 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 deals with user input that is expected to contain errors. User input errors are a normal occurrence; the errors discussed here are grounds for throwing exceptions.	
SMTTVS-525	2.5.4-F – Numeric overflows	If the programming language does not provide automatic run-time detection of numeric overflow, all arithmetic operations that could potentially overflow the relevant data type must be checked for overflow. **Discussion** Encapsulate overflow checking as much as possible.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-526	2.5.4-G – Uncontrolled format strings	Voting system software must not contain uncontrolled format strings. **Discussion** Many examples of this vulnerability have previously been identified in voting system software. Additional information about this vulnerability can be found at *MITRE CWE 134: Use of Externally-Controlled Format String [MITRE20d].*	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-527	2.5.4-H – Recommended	Application logic that is vulnerable to the following types of errors must check for these errors at run time and respond defensively when they occur: 1. pointer variable errors, and	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
	internal error checking	2. dynamic memory allocation and management errors.	
SMTTVS-528	2.5.4-I – Pointers	If application logic uses pointers or a similar mechanism for specifying absolute memory locations, the application logic must validate these pointers or addresses before they are used. **Discussion** The goal is to prevent improper overwriting, 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.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-529	2.5.4-J – Memory mismanagement	If dynamic memory allocation is performed in application logic, the application logic must be able to be instrumented or analyzed with a COTS tool for detecting memory management errors. **Discussion** Dynamic memory allocation that is fully encapsulated within a standard platform library is treated as COTS software.	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-530	2.5.4-K – Nullify freed pointers	If pointers are used, any pointer variables that remain within scope after the memory they point to is deallocated must be set to null or marked as invalid (pursuant to the idiom of the programming language used). **Discussion** 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. In languages using garbage collection, memory is not deallocated until all pointers to it have gone out of scope, so this requirement is moot.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-531	2.5.4-L – React to errors detected	Detecting any of the errors enumerated in these requirements must be treated as a complete failure of the callable unit in which the error was detected. 1. An appropriate exception must be thrown, and 2. Control must pass out of the unit immediately.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-532	2.5.4-M – Election integrity monitoring	Electronic devices must proactively detect or prevent basic violations of election integrity (for example, stuffing the ballot box or accumulating negative votes) and alert an election official or administrator if they occur.	BMD, CCOS, EMP, Integration, PCOS, Security, TDP

Key	Summary	Description	Component/s
		Discussion Equipment can only verify those conditions that are within the scope of what the equipment does. However, if 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.	
SMTTVS-533	2.5.4-N – SQL injection	The voting system application must defend against SQL injection. **Discussion** SQL injection is a classic type of software weakness still prevalent today. SQL injection is not just a web-based issue, as any application accepting untrusted user input and passing it to a database can be vulnerable. Additional information about this software weakness can be viewed at *MITRE CWE 89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') [MITRE20e].*	EMP, Security, TDP
SMTTVS-534	2.5.4-O – Parameterized queries	Any structured statement or command being prepared using dynamic data (including user input) to be sent to a database or other process must parameterize the data inputs and apply strict type casting and content filters on the data (such as prepared statements). **Discussion** Parametrized queries are a common defense against this class of software weakness.	CCOS, EMP, Integration, PCOS, Security, TDP
SMTTVS-536	2.6-A – Surviving device failure	All systems must be capable of resuming normal operation following the correction of a failure:	BMD, CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		1. in any device; 2. in any component (for example, memory, CPU, ballot reader, or printer) provided that catastrophic electrical or mechanical damage has not occurred; and 3. in a controlled fashion so that system status can be restored to the initial state existing before the error occurred. **Discussion** "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. The final state is optional because election officials responding to the error condition might want the opportunity to select a different state, such as a controlled shutdown with memory dump for later analysis.	
SMTTVS-537	2.6-B – No compromising voting or audit data	Exceptions and system recovery must be handled in a manner that protects the integrity of all recorded votes and audit log information.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-538	2.6-C – 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 must restore the device to the last known good state existing immediately before the error or failure, without loss or corruption of voting data previously stored in the device.	BMD, CCOS, EMP, PCOS

Key	Summary	Description	Component/s
		Discussion If 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.	
SMTTVS-540	2.7-A – Assessment of reliability	The voting system's reliability must be assessed using a combination of evidence items gathered during the entire course of testing, including: 1. continuous operation of the voting system under typical environmental conditions; 2. continuous operation of the voting system under varied environmental conditions across defined ranges; and 3. resistance of the voting system to electrical surges, interference, and loss of power. **Discussion** As with accuracy, reliability cannot be positively ascertained; a judgment of reliability must be determined from evidence. In this case, a volume test *[CA06]* is used during various environmental conditions to determine the reliability of the voting system operations, as well as data from the test campaign regarding relevant VVSG requirements.	BMD, CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-541	2.7-B – Continuous operation – typical environmental conditions	The voting system must operate for a continuous period of time during which ballots are cast and ballot positions are read and tabulated without error.	BMD, CCOS, Integration, PCOS, TDP
SMTTVS-542	2.7-C – Continuous operation – varied environmental conditions	The voting system must operate for a continuous period of time during which ballots are cast and ballot positions are read and tabulated without error and in which temperature and humidity are varied.	BMD, CCOS, Integration, PCOS, TDP
SMTTVS-543	2.7-D – Ability to support maintenance and repair physical environment conditions – non-operating	The voting system must be able to withstand non-operating physical environmental conditions simulating stresses that occur during maintenance and repair.	BMD, CCOS, PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-544	2.7-E – Ability to support transport and storage physical environment conditions – non-operating	The voting system must be able to withstand non-operating physical environmental conditions simulating stresses that occur during transport between storage locations and polling places.	BMD, CCOS, PCOS, TDP
SMTTVS-545	2.7-F – Ability to support storage temperatures in physical environment – non-operating	The voting system must be able to withstand non-operating physical environmental conditions simulating temperature-related and humidity-related stresses that occur during storage.	BMD, CCOS, PCOS, TDP
SMTTVS-546	2.7-G – Electrical disturbances	The voting system must continue to operate in the presence of electrical disturbances generated by other devices and people and must not cause electrical disruption to other devices and people. **Discussion** Voting devices located in a polling place or other places need to continue to operate despite disruption from electrical emanations generated by other devices, including static discharges from people. Likewise, voting devices need to operate without	BMD, PCOS

Key	Summary	Description	Component/s
		causing disruption to other devices and people due to electrical emanations from the devices.	
SMTTVS-547	2.7-H – Power outages, sags, and swells	The voting system must be able to withstand, without disruption of normal operation or loss of data, a complete loss of power lasting two hours. **Discussion** Essentially, battery backup must keep the voting system operational so that voting can continue for a minimum of two hours.	BMD, PCOS
SMTTVS-548	2.7-I – Withstand conducted electrical disturbances	All electronic voting systems must withstand conducted electrical disturbances that affect the power ports of the system.	BMD, PCOS
SMTTVS-549	2.7-J – Emissions from other connected equipment	All elements of an electronic voting system must be able to withstand the conducted emissions generated by other elements of the voting system.	BMD, PCOS
SMTTVS-550	2.7-K – Electrostatic discharge immunity	All electronic voting systems must withstand, without disruption of normal operation or loss of data, electrostatic discharges (ESD) associated with human contact and contact with mobile equipment (such as service carts and wheelchairs).	BMD, PCOS

Key	Summary	Description	Component/s
		Discussion ESD events can originate from direct contact between an “intruder” (person or object) charged at a potential different from that of the units of the voting system, or from an approaching person about to touch the equipment – an “air discharge.” The resulting discharge current can induce disturbances in the circuits of the equipment. This requirement is meant to ensure that voting devices are conformant to the typical ESD specifications met by other electronic devices used by the public such as ATMs and vending kiosks.	

Key	Summary	Description	Component/s
SMTTVS-256	3.1.1-A – System overview documentation	The manufacturer must provide system overview documentation that identifies the functional and physical components of the system, how the components are structured, and the interfaces between them.	TDP
SMTTVS-257	3.1.1-B – System overview, functional diagram	System overview documentation must include high-level functional diagrams of the voting system that include all of its components. The diagrams must portray how the various components relate and interact. **Discussion** The diagrams could be engineering renderings or photographs.	CCOS, PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-258	3.1.1-C – System description	System overview documentation must include written descriptions and diagrams that present the following, as applicable: 1. a description of the functional components (or subsystems) as defined by the manufacturer (for example, 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 components; 5. identification of all COTS products (both hardware and software) included in the system or used as part of the system's operation, identifying the name, manufacturer, and version used for each such component; 6. communications (dial-up, network) software; 7. interfaces among internal components and interfaces with external systems; 8. for components that interface with other components for which multiple products may be used, file specifications, data objects, or other means used for information exchange including the public standard used for such file specifications, data objects, or other means; and	TDP

Key	Summary	Description	Component/s
		9. benchmark directory listings for all software, firmware, and associated documentation included in the manufacturer's release in the order in which each piece of software or firmware would normally be installed upon system setup and installation. **Discussion** The diagrams could be engineering renderings or photographs.	
SMTTVS-259	3.1.1-D – Identify software and firmware by origin	System overview documentation must include full identification of all software and firmware items, indicating items that were: 1. written in-house including subcontracted; 2. procured as COTS, unmodified; and 3. procured as COTS and modified, including descriptions of the modifications to the software or firmware and to the default configuration options. **Description** Full identification would include authorship, version numbers, where procured, and other items to positively identify the COTs or in-house developed software	TDP
SMTTVS-260	3.1.1-E – Traceability of procured software	System overview documentation must include a declaration that procured software items were obtained directly from the manufacturer or a licensed dealer or distributor. **Discussion**	TDP

Key	Summary	Description	Component/s
		For most noncommercial software, this would mean a declaration 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.	
SMTTVS-261	3.1.2-A – System performance documentation	The manufacturer must provide system performance documentation that includes: 1. device capacities and limits that were stated in the implementation statement; 2. if not already covered in the implementation statement, 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.	TDP
SMTTVS-262	3.1.2-B – Maximum tabulation rate	System performance documentation must include the maximum tabulation rate for a bulk-fed scanner. This documentation must include the maximum tabulation rate for individual components that impact the overall maximum tabulation rate.	CCOS, TDP

Key	Summary	Description	Component/s
		Discussion The capacity to convert the marks on individual ballots into signals is uniquely important to central count systems.	
SMTTVS-263	3.1.2-C – Reliably detectable marks	System performance documentation must include, for all types of optical scanners: 1. what constitutes a mark that is tabulatable; 2. what constitutes a mark that is ambiguous and may require adjudication; and 3. what constitutes a marginal mark that would not be tabulatable. **Discussion** Marginal marks could include those marks considered as stray or caused by defects or folds on the ballot.	CCOS, PCOS, TDP
SMTTVS-264	3.1.2-D – Processing capabilities	System performance documentation must include a listing of the system's functional processing capabilities, encompassing capabilities required by the VVSG, and any additional capabilities provided by the system, with a description of each capability. Therefore, this documentation must include the following attributes: 1. an explanation regarding the capabilities of the system that were declared in the implementation statement; 2. additional capabilities (extensions) must be clearly indicated; 3. required capabilities that may be bypassed or deactivated during installation or operation by the user must be clearly indicated;	TDP

Key	Summary	Description	Component/s
		4. additional capabilities that function only when activated during installation or operation by the user must be clearly indicated; and 5. additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user must be clearly indicated.	
SMTTVS-267	3.1.3-A – System security documentation	Manufacturers must provide a specific system security document that includes detailed information on the security architecture of the voting system and its security-related functions and how users are to properly employ them. **Discussion** This document is intended to further ensure transparency of the voting system. It includes a complete specification of the voting system security architecture, its different components, and how they work together when used properly. Information about security-related functions and components may also appear in other parts of the TDP as applicable but should also appear in this document. The document may contain detailed technical information but also is to contain usage instructions for employing security controls that are written clearly for the intended types of users, e.g., administrator, poll worker, etc.	CCOS, PCOS, TDP
SMTTVS-268	3.1.3-B – Access control implementation	The system security document must include: 1. guidelines and usage instructions on implementing, configuring, and managing access control capabilities;	TDP

Key	Summary	Description	Component/s
		2. an access control policy template or instructions to facilitate the implementation of the access control policy and associated access controls on the voting system; 3. an access control policy under which the voting system was designed to operate and a description of the hazards of deviating from this policy; and information on all privileged accounts included on the voting system. **Discussion** Access control policy requirements include the minimum baseline policy definitions necessary for testing and implementing the voting system. The policies may be defined within the voting system or provided as guidelines in the documentation. The 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. Information on privileged accounts include the name of the account, purpose, capabilities, and permissions, and how to disable the account in the user documentation.	
SMTTVS-269	3.1.3-C – Physical security	The system security document must include an explanation of how to implement all physical security controls for voting devices and other security-sensitive components of the voting system, including model procedures necessary for effective use of countermeasures.	TDP

Key	Summary	Description	Component/s
SMTTVS-270	3.1.3-D – Audit procedures	The system security document must include an explanation of how to conduct audit procedures to determine whether tabulation is accurate.	TDP
SMTTVS-271	3.1.4-A – Software installation documentation	The manufacturer must provide software installation documentation that lists all software to be installed on the programmed devices of the voting system and the installation software used to install the software in the user documentation. **Discussion** Software to be installed on programmed devices of the voting system includes executable code, configuration files, data files, and election-specific software.	TDP
SMTTVS-272	3.1.4-B – Software information	Software installation documentation must include the following information for each piece of software to be installed or used to install software on programmed devices of the voting system: 1. software product name; 2. software version number 3. software manufacturer name; 4. software manufacturer contact information; 5. type of software (application logic, border logic, third party logic, COTS software, or installation software); 6. list of software documentation; and	TDP

Key	Summary	Description	Component/s
		7. component identifiers (such as filenames) of the software, and type of software component (executable code, source code, or data). 8. flag to indicate whether the given software product should be considered "election-specific" (e.g., election-specific=[True|False]) to differentiate software used for implementing essential election application logic functions (such as counting) from more generic software (such as generic file-system functions).	
SMTTVS-273	3.1.4-C – Software location information	Software installation documentation must include the location (such as full path name or memory address) and storage device (such as type and part number of storage device) where each piece of voting system software is installed on programmed devices of the voting system. **Discussion** This requirement applies to voting system software installed on programmed devices of the voting system. The full directory path is the final destination of the software when installed on non-volatile storage with a file system.	TDP
SMTTVS-274	3.1.4-D – Election specific software identification	Software installation documentation must identify election specific software in the user documentation. **Discussion** This requirement applies to voting system software installed on programmed devices of the voting system. If the documentation can provide information (such as what is	TDP

Key	Summary	Description	Component/s
		indicated in item 8 from 3.1.4-B – Software information) then this should be sufficient to clearly distinguish those pieces of software that perform essential election functions (such as counting) from those that perform more generic, non-election-specific tasks (such as those that might perform only general file-system operations, regardless of election concerns).	
SMTTVS-275	3.1.4-E – Installation software and hardware	Software installation documentation must include a list of software and hardware required to install software on programmed devices of the voting system in the user documentation.	TDP
SMTTVS-276	3.1.4-F – Software installation procedures	Software installation documentation must include the software installation procedures used to install software on programmed devices of the voting system in user documentation.	TDP
SMTTVS-277	3.1.4-G – Baseline image creation	To replicate programmed device configurations, the software installation procedures must create a baseline image of the initial programmed device configuration with storage media and mechanism for verifying the image's validity using a digital signature.	TDP
SMTTVS-278	3.1.4-H – Programmed device	The software installation procedures must use the baseline image and associated digital signature and digital signature validation mechanism of the initial validated image to replicate the configuration onto other programmed devices.	Integration, TDP

Key	Summary	Description	Component/s
	configuration replication	**Discussion** The main point of this requirement is to ensure transitive immutability of a given device configuration (based on a valid, original image that corresponds to an original cryptographic signature). In this way, it seeks to ensure that the starting image that is used for the replication of an image to a particular configuration or target device is the same as the one that was validated via digital signature mechanisms. The process for dealing with varying details of alternative target platforms can be addressed with the use of modern deployment technologies to create configurable installation mechanisms. This is not uncommon for major software technology providers. Thus, technology providers will be expected to develop appropriate install and configuration mechanisms that can have configurable images that can be signed through this digital signature mechanism at the outset and when replicating to any target configuration to ensure that both the image and the mechanisms for transforming that image in a given target deployment environment have been understood and validated from the beginning. The above descriptions are meant to provide a way to validate a much wider range of deployment scenarios than has been experienced in the past. As a result, it is not expected or intended that this process would necessarily require strictly binary images, but rather, configurable ones, with the configuration settings and	

Key	Summary	Description	Component/s
		mechanisms for installation and signature verification provided, signed, and validated from the beginning.	
SMTTVS-279	3.1.4-I – Software installation record creation	The software installation procedures must specify the creation of a software installation record that includes at a minimum: 9. a unique identifier (such as a serial number) for the record; a list of unique identifiers of storage media associated with the record; the time, date, and location of the software installation; 10. names, affiliations, and signatures of all people present; copies of the procedures used to install the software on the programmed devices of the voting system; 11. the certification number of the voting system; list of the software installed as well as associated digital signatures and mechanisms for installation and verification on programmed devices of the voting system; and 12. a unique identifier (such as a serial number) of the vote-capture device or election management system (EMS) which the software is installed. **Discussion**	TDP

Key	Summary	Description	Component/s
		The purpose of this requirement is a continuation of 3.1.4-I – Software installation record creation, to ensure transitive immutability from the original baseline image through a given installation process (i.e., installation of certified software). The requirement emphasizes the importance of the final act of performing an installation of certified software on a target system configuration. It is a requirement to ensure that this event has some means by which an appropriate record, attesting to the facts of the installation event itself, can be produced and can provide the given information. Creators of software installation mechanisms and procedures are asked to provide information in their installation user documentation specifying the elements of this record and that it should be recorded in the event of a certified software installation. **Related requirements**: 3.1.4-H – Programmed device configuration replication	
SMTTVS-280	3.1.4-J – Procurement of voting system software	Software installation documentation must include that voting system software be obtained from a trusted distribution repository. **Discussion** Distribution repositories provide software they receive to parties approved by the owner of the software.	TDP
SMTTVS-281	3.1.4-K – Open market	Software installation documentation must include that COTS software be obtained from the open market.	TDP

Key	Summary	Description	Component/s
	procurement of COTS software		
SMTTVS-282	3.1.4-L – Erasable storage media preparation	Software installation documentation must specify how previously stored information on erasable storage media is removed before installing software on the media. **Discussion** The purpose of this requirement is to prepare erasable storage media for use by the programmed devices of the voting system. The requirement does not mandate the prevention of previously stored information leakage or recovery. Simply deleting files from file systems, flashing memory cards, and removing electrical power from volatile memory satisfies this requirement.	TDP
SMTTVS-283	3.1.4-M – Trusted storage media	Software installation documentation must specify that trusted storage media be used to install software on programmed devices of the voting system. **Discussion** Trusted storage media can include read-only media. Previous VVSGs emphasized the use of unalterable storage media which is believed to be too restrictive in the current technological context. Instead, it is preferable that read-only storage be used. And, as indicated in related requirements, it is assumed that any use of media, transport, or use of original images be associated with a mechanism for verifying the cryptographic signatures of those original images.	CCOS, PCOS, TDP

Key	Summary	Description	Component/s
		Related requirements: 3.1.4-H – Programmed device configuration replication 3.1.4-I – Software installation record creation 3.1.5 – System operations documentation	
SMTTVS-284	3.1.5-A – System operations documentation	Manufacturers must provide a specific system operations document for 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. It must: 1. provide a detailed description of procedures required to initiate, control, and verify proper system operation; 2. provide procedures that clearly enable the operator to assess the correct flow of system functions (as evidenced by system-generated status and information messages); 3. provide procedures that clearly enable the administrator to intervene in system operations to recover from an abnormal system state; 4. define and illustrate the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system; define and illustrate procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved. (This information is provided for the interaction of the system with other data processing systems or data interchange protocols.);	Integration, TDP

Key	Summary	Description	Component/s
		5. provide 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; support successful election definition and software installation and control by central election officials; 6. provide a schedule and steps for the software and ballot installation, including a table outlining the key dates relative to the start of voting, events, and deliverables; and 7. specify 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. **Discussion** The nature of the instructions for operating personnel will depend upon the overall system design and required skill level of system operations support personnel.	
SMTTVS-285	3.1.5-B – Support training	The operations document must include 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 election workers.	TDP
SMTTVS-286	3.1.5-C – Functions and modes	The operations document must include a summary of system operating functions and modes to permit understanding of the system's capabilities and constraints.	TDP

Key	Summary	Description	Component/s
SMTTVS-287	3.1.5-D – Roles	The operations document must identify the roles of operating personnel and relate them to the operating modes of the system.	TDP
SMTTVS-288	3.1.5-E – Conditional actions	The operations document must describe decision criteria and conditional operator functions such as error and failure recovery actions.	TDP
SMTTVS-289	3.1.5-F – References	The operations document must list all reference and supporting documents pertaining to the use of the system during election operations.	TDP
SMTTVS-290	3.1.5-G – Operational environment	The operations document must identify all facilities, furnishings, fixtures, and utilities that will be required for equipment operations, including a statement of all requirements and restrictions regarding: 1. environmental protection; 2. electrical service; 3. recommended auxiliary power; 4. telecommunications service; and 5. any other facility or resource required for the proper installation and operation of the system.	TDP
SMTTVS-291	3.1.5-H – Readiness testing	The operations document must include specifications for testing system installation and readiness.	Integration, TDP

Key	Summary	Description	Component/s
		Discussion Readiness testing refers to steps that election officials can take after configuring equipment to establish that it was correctly configured. Logic and accuracy testing would be part of this.	
SMTTVS-292	3.1.5-I – Features	The operations document must include documentation of system operating features that includes: 1. detailed descriptions 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.	TDP
SMTTVS-293	3.1.5-J – Support	The operations document must include documentation of system operating procedures that: 1. describes procedures for providing technical support, system maintenance, and correction of defects, and for incorporating hardware upgrades and new software releases; and 2. defines the procedures required to support system installation and readiness testing.	TDP

Key	Summary	Description	Component/s
SMTTVS-294	3.1.5-K – Transportation and storage	The operations document must include any special instructions for the care and handling of voting devices and any removable media or records for: 1. shipment; 2. storage; and 3. archiving information.	CCOS, EMP, PCOS, TDP
SMTTVS-295	3.1.6-A – System maintenance documentation	Manufacturers must include system maintenance documentation that provides information to support election workers, information systems personnel, or maintenance personnel in adjusting or removing and replacing components or modules in the field. **Discussion** Election workers such as polling place workers may not be permitted to replace components, however in some cases they may be permitted to adjust them. Thus, the documentation should be geared to the appropriate personnel.	TDP
SMTTVS-296	3.1.6-B – General contents	Maintenance documentation must include service actions recommended to correct malfunctions or problems, personnel and expertise required to repair and maintain the system, and equipment and materials facilities needed for proper maintenance.	TDP
SMTTVS-297	3.1.6-C – Maintenance viewpoint	Maintenance documentation must include the structure and function of the hardware, firmware, and software for election preparation, programming, vote	TDP

Key	Summary	Description	Component/s
		recording, tabulation, and reporting in sufficient detail to provide an overview of the system for maintaining and identifying faulty hardware or software.	
SMTTVS-298	3.1.6-D – Equipment overview details	Maintenance documentation must include a concept of operations that fully describes such items as: 1. electrical and mechanical functions of the equipment; 2. for paper-based systems, how ballot handling and reading processes are performed; 3. for electronic vote-capture devices, how vote selection and ballot casting are performed; 4. how data transmission over a network is performed (if applicable); 5. how data are handled in 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. **Discussion** The documentation should indicate how and when information is written from volatile to non-volatile memory, including redundant storage.	TDP

Key	Summary	Description	Component/s
SMTTVS-299	3.1.6-E – Maintenance procedures	Maintenance documentation must include preventive and corrective maintenance procedures for hardware, firmware, and software.	TDP
SMTTVS-300	3.1.6-F – Preventive maintenance procedures	Maintenance documentation must identify and describe: 1. all required and recommended preventive maintenance tasks, including software and data backup, database performance analysis, and database tuning; 2. the number and skill levels of personnel required for each task; 3. the parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance; and 4. any maintenance tasks that must be coordinated with the manufacturer or a third party (such as coordination that may be needed for COTS used in the system).	TDP
SMTTVS-301	3.1.6-G – Troubleshooting procedure details	Maintenance documentation must identify specific procedures to be used in diagnosing and correcting problems in the system hardware, firmware, and software. Descriptions must 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;	TDP

Key	Summary	Description	Component/s
		4. 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 manufacturer, or other party, for COTS.	
SMTTVS-302	3.1.6-H – Special equipment	Maintenance documentation must identify and describe any special purpose test or maintenance equipment recommended for fault isolation and diagnostic purposes.	TDP
SMTTVS-303	3.1.6-I – Parts and materials	Maintenance documentation must include detailed documentation of parts and materials needed to operate and maintain the system.	TDP
SMTTVS-304	3.1.6-J – Approved parts list	Maintenance documentation must include a complete list of approved parts and materials needed to operate and maintain the system. This list must 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.	TDP
SMTTVS-305	3.1.6-K – Marking devices	Maintenance documentation must 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.	TDP

Key	Summary	Description	Component/s
		Discussion Includes pens or pencils and possibly a compatible ballot marking device (BMD).	
SMTTVS-306	3.1.6-L – Approved manufacturers	Maintenance documentation must include a listing of sources and model numbers for marking devices manufactured by multiple external sources that satisfy these requirements.	TDP
SMTTVS-307	3.1.6-M – Ballot stock specification	Maintenance documentation must: 1. 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 2. 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.	TDP
SMTTVS-308	3.1.6-N – Ballot stock specification criteria	Maintenance documentation for optical scanners must include specifications for ballot materials to ensure that votes are read from only a single ballot at a time, without bleed-through or transferal of marks from one ballot to another.	TDP
SMTTVS-309	3.1.6-O – Printer paper specification	Maintenance documentation for voting systems that include printers must include specifications of the paper necessary to ensure correct operation and minimize jamming.	TDP

Key	Summary	Description	Component/s
		Discussion This requirement covers all printers, either stand-alone or integrated with another device, regardless of whether they are used for reporting, for logging, for voter verified paper records (VVPR), etc.	
SMTTVS-310	3.1.6-P – System maintenance, maintenance environment	Maintenance documentation must identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance.	TDP
SMTTVS-311	3.1.6-Q – System maintenance, maintenance support and spares	Maintenance documentation must identify: 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 (for example, jurisdiction, manufacturer) of qualified maintenance personnel.	TDP
SMTTVS-326	3.1.7-A – Training documentation	The manufacturer must describe the personnel resources and training required for a jurisdiction to operate and maintain the system.	TDP
SMTTVS-327	3.1.7-B – Personnel	The manufacturer must specify the number of personnel and skill levels required to perform each of the following functions:	TDP

Key	Summary	Description	Component/s
		1. pre-election or election preparation functions (such as entering an election, contest and candidate information, designing a ballot, and 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.	
SMTTVS-328	3.1.7-C – User functions versus manufacturer functions	The manufacturer must distinguish which functions may be carried out by user personnel and which must be performed by manufacturer personnel.	TDP
SMTTVS-329	3.1.7-D – Training requirements	The manufacturer must specify requirements for the orientation and training of administrators, central election officials, election judges, and election workers	TDP

Key	Summary	Description	Component/s
SMTTVS-330	3.2-A – Setup inspection process	Manufacturers must provide setup inspection process documentation that includes the setup inspection process that the voting device was designed to support including a description of the risks of deviating from the process. **Discussion** The setup inspection process provides a means to inspect various properties of voting devices as needed during the election process.	TDP
SMTTVS-331	3.2-B – Minimum properties included in the setup inspection process	Setup inspection process documentation must at a minimum include: 1. inspecting voting system software; 2. inspecting storage locations that hold election information that changes during an election; 3. inspecting other voting device properties; and 4. executing logic and accuracy testing related to readiness of use in an election.	CCOS, PCOS, TDP
SMTTVS-332	3.2-C – Setup inspection record generation	Setup inspection process documentation must describe the records that result from performing the setup inspection process.	CCOS, PCOS, TDP
SMTTVS-333	3.2-D – Installed software identification procedure	Setup inspection process documentation must include the procedures to identify all software installed on programmed devices of the voting system.	PCOS, TDP

Key	Summary	Description	Component/s
		Discussion This requirement provides the ability to identify if the proper software is installed and that no other software is present on programmed devices of the voting system. This requirement covers software stored on storage media with or without a file system.	
SMTTVS-334	3.2-E – Software integrity verification procedure	Setup inspection process documentation must include the procedures to verify the integrity of software installed on programmed devices of the voting system.	PCOS, TDP
SMTTVS-335	3.2-F – Election information value	Setup inspection process documentation must include a list of voting device storage locations for holding election information that can change during the election, except for the static values set to conduct a specific election.	PCOS, TDP
SMTTVS-336	3.2-G – Maximum and minimum values of election information storage locations	Setup inspection process documentation must include the maximum and minimum values of voting device storage locations for holding election information that can change during an election.	PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-337	3.2-H – Variable value inspection procedure	Setup inspection process documentation must include the procedures to inspect the values of voting device storage locations for holding election information that can change during an election.	PCOS, TDP
SMTTVS-338	3.2-I – Backup power operational range	Setup inspection process documentation must include the nominal operational range for the backup power sources of the voting device.	PCOS, TDP
SMTTVS-339	3.2-J – Backup power inspection procedure	Setup inspection process documentation must include the procedures to inspect the remaining charge of the backup power sources of the voting device.	PCOS, TDP
SMTTVS-340	3.2-K – Cabling connectivity inspection procedure	Setup inspection process documentation must include the procedures to inspect the connectivity of the cabling attached to the voting device.	PCOS, TDP
SMTTVS-341	3.2-L – Communications operational status	Setup inspection process documentation must include the procedures to inspect the operational status of the communications capabilities of the voting device.	PCOS, TDP

Key	Summary	Description	Component/s
	inspection procedure		
SMTTVS-342	3.2-M – Communications on/off status inspection procedure	Setup inspection process documentation must include the procedures to inspect the on/off status of the communications capabilities of the voting device.	CCOS, PCOS, TDP
SMTTVS-343	3.2-N – Quantity of voting equipment	Setup inspection process documentation must include a list of consumables associated with the voting device, including estimated number of usages per unit.	PCOS, TDP
SMTTVS-344	3.2-O – Consumable inspection procedure	Setup inspection process documentation must include the procedures to inspect the remaining amount of each of the voting device's consumables.	PCOS, TDP
SMTTVS-345	3.2-P – Calibration of voting device components	Setup inspection process documentation must include: 1. a list of components associated with the voting device that require calibration; 2. the nominal operating ranges for each component; 3. the procedures to inspect the calibration of each component; and 4. the procedures to adjust the calibration of each component.	TDP

Key	Summary	Description	Component/s
SMTTVS-346	3.2-Q – Checklist of properties to be inspected	Setup inspection process documentation must include a checklist of other properties of the voting device to be inspected, to include: 1. a description of the risks of not performing each documented inspection; 2. power sources; 3. cabling for communications; 4. capabilities; 5. consumables; 6. calibration of voting device components; 7. general physical features of the voting device; and 8. securing external interfaces of the voting device not being used.	CCOS, PCOS, TDP
SMTTVS-347	3.3-A – System security, system event logging	Manufacturers must provide publicly available documentation that: 1. describes system event logging capabilities and usage, and 2. fully documents the log format information. **Discussion** The log format and the meaning of all possible types of log entries must be fully documented in sufficient detail to allow independent manufacturers to implement utilities to parse the log file. This documentation must be publicly available and not just in the TDP.	BMD, CCOS, PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-348	3.3-B – Specification of common data format usage	Manufacturers must provide publicly available documentation describing how the manufacturer has implemented a CDF specification for a particular device or function. This includes such items as: 1. descriptions of how elements and attributes are used; 2. constraints on data elements; and 3. extensions as well as any constraints. **Discussion** Conformance to a common data format does not guarantee data interoperability. The manufacturer needs to document fully how it has interpreted and implemented a CDF specification for its voting devices and the types of data exchanged or exported. Here is list of related references: NIST SP 1500-103 Cast Vote Records Common Data Format Specification [CVR_CDF], NIST SP 1500-100 Election Results Common Data Format Specification [NIST16], NIST SP 1500-101 Election Event Logging Common Data Format Specification [LOG_CDF], NIST SP 1500-102 Voter Records Interchange (VRI) CDF Specification [VRI_CDF].	BMD, CCOS, PCOS, TDP
SMTTVS-349	3.3-C – Bar and other codes	Manufacturers must provide publicly available documentation that fully specifies the barcode, how barcoded data is formatted, and any other encoding standards or methods used on ballots or audit material.	TDP

Key	Summary	Description	Component/s
		Discussion The voting system documentation needs to include the name and version of the standard used for barcodes or for any other codes that encode information that the public sees on ballots or other material that can be used in audits or verification of the election. The documentation also needs to include how the data may be packed or compressed within the encoding. The report should be sufficient for a voter to understand the barcoded contents and for an auditor to develop applications that examine the barcoded contents.	
SMTTVS-350	3.3-D – Ballot selection codes	The voting system must be capable of producing a report on an election-by-election basis to show the meaning of codes and other data used within barcodes and CVRs to represent ballot selections and ballot style information. **Discussion** Codes that represent a voter's ballot selections are commonly used within barcodes and CVRs to save space. The codes will likely change for each election. The codes are meaningless to a voter or an auditor unless the voting system can produce a report that shows all codes possible and what contests and ballot selections they represent. If, for example, a code of 90 is used to represent a particular contest, then the report must show that 90 refers to the title or description of that particular contest. This	EMP, Integration, TDP

Key	Summary	Description	Component/s
		includes other information within the barcode generally found on clear-text ballots to identify the ballot style.	

Key	Summary	Description	Component/s
SMTTVS-355	4.1-A – Election programming data input and output	The voting system must include support for CDF specification(s) regarding: 1. import and export of election programming data, and 2. import and export of ballot programming data. **Discussion** This requirement concerns import and export of pre-election data into an election definition device, such as for identification of political geography, contest, candidate, ballot data, and other pre-election information used to setup an election and produce ballots. This also includes reports of pre-election data from the election definition device that can be used to verify the election programming setup. More information can be found in SP 1500-100 Election Results Common Data Format Specification [NIST16].	EMP, Integration, PCOS, TDP
SMTTVS-356	4.1-B – Tabulator report data	The voting system must include support for CDF specification(s) for import and export of election results reporting data.	EMP, Integration

Key	Summary	Description	Component/s
		Discussion Importing results data is required to provide support for aggregations of vote data from different election management systems such as what occurs during state roll-ups on election night and during the process of election results certification. More information can be found in: NIST SP 1500-100 Election Results Common Data Format Specification [NIST16].	
SMTTVS-357	4.1-C – Exchange of cast vote records (CVRs)	The voting system's audit, casting, tabulation, and vote-capture functions dealing with CVRs must have the capability of importing or exporting CVRs according to CDF specification(s). **Discussion** Devices that export or import CVRs typically include voter-facing and batch-fed scanners, election management systems, and other devices used for adjudication or auditing. This requirement indicates that these devices have the capability to import or export CVRs in the respective CDF(s). More information can be found in: NIST SP 1500-103 Cast Vote Records Common Data Format Specification [CVR_CDF].	EMP, Integration, PCOS
SMTTVS-358	4.1-D – Exchange of voting device election event logs	The voting devices comprising the voting system must include support for CDF specification(s) for import or export of election event log data.	BMD, CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		Discussion This requirement refers to election event logs and not system logs provided by common operating systems such as Microsoft Windows or Apple iOS. This requirement does not mandate that manufacturers use the format for storing election log information; a manufacturer can meet this requirement by conversion or translation from a native format into the CDF. More information can be found in:], NIST SP 1500-101 Election Event Logging Common Data Format Specification [LOG_CDF].	
SMTTVS-359	4.1-E – Voting device event code documentation	Manufacturers must provide a publicly available specification for event codes used in their equipment. **Discussion** Use of NIST SP 1500-101 Election Event Logging Common Data Format Specification [LOG_CDF] for election event logs only addresses the data format; it does not mandate a common lexicon for event codes. NIST SP 1500-101 [LOG_CDF] provides a separate schema for including documentation of event codes; manufactures may make this available publicly or upon request without condition.	EMP, PCOS, TDP
SMTTVS-360	4.1-F – Specification of common format usage	Manufacturers must include a specification describing how the manufacturer has implemented a CDF specification for a particular device or function. This includes such items as descriptions of how elements and attributes are used, as well as any constraints or extensions.	EMP, PCOS, TDP

Key	Summary	Description	Component/s
		Discussion Conformance to a common data format does not guarantee data interoperability. The manufacturer needs to document fully how it has interpreted and implemented a CDF specification for its voting devices and the types of data exchanged or exported.	
SMTTVS-361	4.2-A – Standard formats	Publicly available non-proprietary formats must be used, where possible, for exchanging data. **Discussion** Examples include the use of common data encodings such as bar or QR codes.	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-362	4.2-B – Public documented manufacturer formats	Where publicly available non-proprietary formats are not available, manufacturers must include a specification that describes the protocol or data format. **Discussion** As an example, a manufacturer's algorithm or method for packing or compressing data before encoding in a QR code will be documented so that its implementation and usage is available publicly.	BMD, EMP, PCOS
SMTTVS-363	4.3-A – Standard device interfaces	Standard, common hardware interfaces and protocols must be used to connect devices. **Discussion**	BMD, CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		Examples include using published communications protocols, such as, IEEE, and using common hardware interfaces, such as, USB, when connecting to printers, disks, and other devices. **EAC Decision on Request for Interpretation:** The intent of 4.3-A Standard device interfaces may be considered satisfied if the proprietary hardware or cabling terminates in a standardized electrical format and utilizes a published communication protocol. Components utilized in this capacity must be documented in the manufacturer TDP, and part numbers must be documented appropriately by the VSTL in the Test Report. This termination may be considered the boundary of the hardware interface.	
SMTTVS-364	4.4-A – COTS devices meet applicable requirements	COTS devices, if used, must satisfy all applicable VVSG requirements. **Discussion** As an example, use of a COTS scanner to scan ballots is potentially possible, but it will need to meet applicable environmental and electrical requirements and, potentially, other requirements depending on how the scanner is used. For example, if it is used to create CVRs, it will need to meet those requirements dealing with CVR creation and handling.	CCOS, EMP, TDP

Key	Summary	Description	Component/s
SMTTVS-121	5.1-A – Voting methods and interaction modes	Within any method of voting, all display formats including enhanced visual and audio and all interaction modes including tactile and limited dexterity must have the same functionality as the visual format and touch mode including voting, verification, and casting. **Discussion** Methods of voting that a voting system might support include in-person voting, vote-by-mail, remote ballot marking, among others. The VVSG scope is in-person voting. For voting systems to meet this requirement they would need to include, for example: • Features that support limited dexterity interaction to enable voters who lack fine motor control or the use of their hands, to submit their ballots privately and independently without manually handling the ballot. • Features for paper ballots or paper verification records that assist voters with poor reading vision to read these ballots and records. • Features to allow blind voters and voters with limited dexterity to perform paper-based verification or feed their own optical scan ballots into a scanner, if all other voters do so. For example, ballot papers or smart cards might provide tactile cues that allow the correct insertion of the card.	BMD, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		• Support for all voting variations. For example, if a visual ballot supports voting a straight party ticket and then changing the vote for a single contest, so do all other display formats and interaction modes. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.	
SMTTVS-122	5.1-B – Languages	The voting system must be capable of displaying and printing the ballot, contest options, review screens, voter verifiable paper records, and voting instructions in all languages the manufacturer has declared the system supports, in both visual and audio formats where applicable. **Discussion** Both written and unwritten languages are within the scope of this requirement. The system will be tested in all languages that the manufacturer claims it is capable of supporting. This requirement originates with the *VRA [VRA65]*.	BMD, EMP, PCOS, TDP
SMTTVS-123	5.1-C – Vote records	All records, including paper ballots and voter verifiable paper records, must have the information required to support auditing by election workers and others who can only read English. **Discussion** Although the system needs to be easily usable by voters using an alternative language, records of the vote also need to be fully available to English-only readers	BMD, EMP, TDP

Key	Summary	Description	Component/s
		to support election administration and auditing. See *9.4 - The voting system supports efficient audits* for related requirements. To meet this requirement, a paper ballot may not be a fully bilingual ballot. For instance, the full text of a ballot question might appear only in the alternative language, but the contest option (for example, “yes / no”) needs to be readable by English-only readers.	
SMTTVS-124	5.1-D – Accessibility features	Accessibility features must be integrated into the manufacturer’s voting system so accessibility for voters with disabilities is supported throughout the voting session, including any steps to activate the ballot at the voting station, ballot marking, verification, and casting. **Discussion** This requirement ensures accessibility to the voter throughout the entire session. Not only are individual system components (such as ballot markers, paper records, and optical scanners) accessible, but they also support voters with disabilities throughout the process of voting from activation through casting. Requirements for individual system components are described in *Principle 7: Marked, Verified, and Cast as Intended*. This general requirement supports *HAVA [HAVA02].* **Related requirements:** 6.1-B – Warnings	BMD, Integration, PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-125	5.1-E – Reading paper ballots	If the voting system generates a paper record (or some other durable, human-readable record) that can be the official ballot or determinative vote record, then the voting system must allow the voter to verify the paper record using the same access features they used to mark the ballot, including enhanced visual and audio formats and tactile and limited dexterity modes. **Discussion** Paper records present difficulties for voters who use large font, high contrast, alternative languages, and other settings. The purpose of this requirement is to ensure that all voters have a similar opportunity for vote verification. For ballot marking devices, for example, if the voter is using audio to make their selections, the voter verifiable paper record, not the stored voter selections, must be read back. This requirement allows the voter to use the same access features throughout the entire voting session. It also does not preclude the voter from choosing a different access feature to verify the record. For example, the voting system might provide a reader that converts the paper record contents into audio output. This requirement supports *HAVA [HAVA02]*. **Related requirements:** 7.1-I – Text size (paper)	BMD, PCOS

Key	Summary	Description	Component/s
SMTTVS-126	5.1-F – Accessibility documentation	As part of the overall system documentation the manufacturer must include descriptions and instructions for all accessibility features that describe: • recommended procedures that fully implement accessibility for voters with disabilities, and • how the voting system supports those procedures. **Discussion** The purpose of this requirement is for the manufacturer not simply to deliver system components, but also to describe the accessibility scenarios they are intended to support, so that election offices have the information they need to effectively make accessibility features available to voters with disabilities. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*. **Related requirements:** 7.3-N – Instructions for voters 7.3-O – Instructions for election workers	BMD, PCOS, TDP
SMTTVS-127	5.2-A – No bias	The voting system must not introduce bias for or against any of the contest options presented to the voter. In enhanced visual and audio formats and tactile and limited dexterity modes, all ballot options are to be presented in an equivalent manner.	BMD, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		Discussion Certain differences in ballot presentation are mandated by state law, such as the order in which candidates are listed and provisions for voting for write-in candidates. This requirement ensures that comparable characteristics such as font size or audio volume and speed are the same for all ballot options.	
SMTTVS-128	5.2-B – Presenting content in all languages	All information that is presented to the voter in English must also be capable of being presented in all other languages that are supported, whether the language is in visual or audio format. This includes instructions, warnings, messages, notification of undervotes or overvotes, contest options, and vote verification information. **Discussion** It is not sufficient simply to present the ballot options in the alternative languages. All the supporting information voters need to mark their ballot is also covered in this requirement. This requirement originates with the *VRA [VRA65]*.	BMD, EMP, PCOS, TDP
SMTTVS-129	5.2-C – Information in all modes	Instructions, warnings, messages, notifications of undervotes or overvotes, and contest options must be presented to voters in the display formats and interaction modes required in *5.1-A – Voting methods and interaction modes*. This includes voting, verification, and casting.	BMD, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		Discussion For audio mode, this requirement can be met with an audio that includes cues to help users know what to expect. For example, announcing the number of items in a list of candidates or contests makes it easier to jump from one item to another without waiting for the audio to complete. Audio cues also ensure that the voter is aware of possible undervotes or overvotes. This includes information about activation. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*	
SMTTVS-130	5.2-D – Audio synchronized	The voting system must provide the option for synchronized audio output to convey the same information that is displayed visually to the voter. **Discussion** This requirement covers all information, including information entered by the voter such as write-in votes. This requirement applies to any audio output, whether it is recorded or generated as text-to-speech. Any differences between audio and visual information are for functional purposes only, with variations only based on differences in the display format and interaction mode, especially for instructions. This feature can assist voters with cognitive disabilities. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*	BMD, EMP, PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-131	5.2-E – Sound cues	Sound and visual cues must be coordinated so that: • sound cues are accompanied by visual cues unless the system is set to audio-only; and • visual cues are accompanied by sound cues unless the system is set to visual-only. **Discussion** The voting equipment might beep if the voter attempts to overvote. If so, there has 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, there would be no visual cue. Audio output also supports non-written languages, voters with low literacy, or voters with low vision. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*	BMD, PCOS
SMTTVS-132	5.2-F – Preserving votes	At any time during a voting session, an electronic voting interface must allow the voter to change all language and display format options, and the interaction settings that the voter can chose directly, while preserving all current vote selections. When changing settings, the system must preserve navigation, screen position, visual settings, audio settings, and other information within and across contests.	BMD, PCOS, TDP

Key	Summary	Description	Component/s
		Discussion A voter who initially chooses an English version of the ballot might switch to another language in order to read a referendum question. Many blind voters have preferences for audio settings, including the rate of speech and volume that are important for comprehension. Changing visual settings for text size might change the layout of the information on the screen, making it important to maintain the screen position. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*	

Key	Summary	Description	Component/s
SMTTVS-367	6.1-A – Preserving privacy for voters	Privacy for voters must be preserved during the entire voting session including ballot activation, voting, verifying, and casting the ballot. **Discussion** This requirement allows for different approaches for electronic and paper interfaces. In both cases, appropriate shielding of the voting station is important – for example, privacy screens for the voting stations. When a paper record with ballot information needs to be transported by the voter, devices such as privacy sleeves can be necessary. This requirement applies to all	BMD, Integration, PCOS, Security, TDP

Key	Summary	Description	Component/s
		records with information on votes (such as a vote verification record) even if that record is not itself a ballot. This requirement supports HAVA [HAVA02]. **Related requirement:** • 7.2-F – Voter speech	
SMTTVS-368	6.1-B – Warnings	During the voting session, the voting system must issue all warnings in a way that preserves privacy for voters and the confidentiality of the ballot. **Discussion** HAVA 301 (a)(1)(C) [HAVA 02] mandates that the voting system notifies the voter of an attempted overvote in a way that preserves privacy for voters and the confidentiality of the ballot. This requirement addresses that mandate. **Related requirements:** • 7.3-K– Warnings, alerts, and instructions	BMD, PCOS, Security, TDP
SMTTVS-369	6.1-C – Enabling or disabling output	During the voting session, the voting system must make it possible for the voter to independently enable or disable either the audio or the visual output and be notified of the change, resulting in a visual-only or audio-only presentation. **Discussion**	BMD, PCOS, Security, TDP

Key	Summary	Description	Component/s
		Voters can be notified of the change to the display or audio output in a variety of ways including beep, voice, or visual notification. An unobtrusive notification that the system has changed the visual display format is helpful to voters who cannot see the screen to confirm the change visually. This requirement is based on WCAG 2.0 [W3C10] and Section 508 [USAB18]. **Related requirements:** • 7.2-A – Display and interaction options • 7.3-K – Warnings, alerts, and instructions	
SMTTVS-370	6.1-D – Audio privacy	Audio during the voting session must be audible only to the voter. **Discussion** Voters who are hard of hearing but need to use an audio interface sometimes need to increase the volume of the audio. Such situations require headphones or other devices (such as a hearing loop) with low sound leakage so the contents of the audio cannot be overheard and understood by others. Voters who are hard of hearing can share audio interfaces with their designated assistants. This requirement is based on WCAG 2.0 [W3C10] and Section 508 [USAB18]. **Related requirements:**	BMD, PCOS, Security

Key	Summary	Description	Component/s
		• 7.2-F – Voter speech • 8.1-J – Hearing aids	
SMTTVS-371	6.2-A - Voter independence	Voters must be able to mark, verify, and cast their ballot or other associated cast vote records independently and without assistance from others. 1. If a voting system includes any features voters might use after casting a ballot as part of end-to-end (E2E) verifiable system ballot tracking, they must be accessible. **Discussion** This requirement ensures that voters can vote with their own interaction preferences and without risk of intimidation or influence. HAVA 301 (a)(1)(C)[HAVA02] mandates that the voting system 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. This requirement directly addresses this mandate. Note that in addition to features for voters after casting their ballot for E2E system ballot tracking, there are other features not in the scope of VVSG requirements that should be designed for accessibility such as forms or notices to cure problems with a vote-by-mail ballot, and sites to learn whether a provisional ballot was accepted for counting.	BMD, PCOS, Security, TDP

Key	Summary	Description	Component/s
		Related requirements: • 5.1-D – Accessibility features • 5.1-E – Reading paper ballots • 8.2-A – Federal standards for accessibility • 2.2-A – User-centered design process	

Key	Summary	Description	Component/s
SMTTVS-221	7.1-A – Reset to default settings	If the adjustable settings of the voter interface have been changed by the voter or election worker during the voting session, the system must automatically reset to the default setting when the voter finishes voting, verifying, and casting. **Discussion** This ensures that the voting system presents the same initial appearance to every voter. This requirement covers all settings that can be adjusted, including font size, color, contrast, audio volume, rate of speech, turning on or off audio or video, and enabling alternative input devices. **Applies to:** Electronic interfaces **Related requirements:** 7.1-K – Audio settings	BMD, PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-222	7.1-B – Reset by voter	If either the voter or an election worker can adjust the settings of the voter interface, there must be a way for the voter to restore the default settings while preserving the current votes. **Discussion** This requirement allows a voter or election worker who has adjusted the system to an undesirable state to reset all settings with the ballot presented to the voter using the new settings, while keeping what was selected thus far. **Applies to:** Electronic interfaces **Related requirements:** 5.2-F – Preserving votes	BMD, PCOS
SMTTVS-223	7.1-C – Default contrast	The default contrast ratio must be at least 10:1 for all elements that visually convey information such as text, controls, and infographics or icons. 1. For electronic displays for voters and election workers, this is measured as a luminosity contrast ratio between the foreground and background colors of at least 10:1. 2. For paper ballots and other paper records, the contrast ratio will be at least 10:1 as measured based on ambient lighting of at least 300 lx. **Discussion** For example, this applies to: • candidate names,	BMD, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		• a broken arrow, • the outline of an oval, circle, or rectangular target used to mark voter selections, or • informational icons identifying voter selections or other information. Purely decorative elements that do not communicate meaning do not have to meet this requirement. A 10:1 luminosity contrast ratio provides enough difference between the text and background to enable people with most color vision deficiencies to read the ballot. This is higher than the highest contrast requirements of 7:1 in WCAG 2.0 Checkpoint 1.4.6 (Level AAA) to accommodate a wider range of visual disabilities. There are many free tools available to test color luminosity contrast using the WCAG 2.0 algorithm. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].* **Applies to:** Electronic interfaces	
SMTTVS-224	7.1-D – Contrast options	The voting system must provide options for high and low contrast displays, including the alternative display contrast options as listed below: 1. A high contrast option with a white background and dark text, with a luminosity contrast ration of at least 20:1. 2. A high contrast option with a black background (between #000000 and #111111) and one of the following foreground options, including:	BMD, PCOS

Key	Summary	Description	Component/s
		a. yellow text similar to #FFFF00, providing a contrast ratio of at least 17.5:1, b. cyan text similar to #00FFFF, providing a contrast ratio of at least 15:1, and c. white text similar to #FAFAFA, providing a contrast ratio of at least 18:1. 3. A low contrast option, providing a contrast ratio in the range of 4.5:1 to 8:1. **Discussion** This requirement for options for the overall display contrast ensures that there is an option for the visual presentation for people whose vision requires either high or low contrast. High and low contrast options apply to the entire screen, including decorative elements. Examples of color combinations for low contrast options include: • brown text similar to #BB9966 on a black background (7.8:1), • black text on a background with text similar to #BB9966 (7.8:1), • grey text similar to #6C6C6C on a white background (5.2:1), • grey/brown text similar to #97967E on a black background (6.9:1), and • grey text similar to #898989 on a dark background similar to #222222 (4.5:1). This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.	

Key	Summary	Description	Component/s
		Applies to: Electronic interfaces	
SMTTVS-225	7.1-E – Color conventions	The use of color by the voting system must follow these common conventions: 1. Green, blue, or white is used for general information or as a normal status indicator; 2. Amber or yellow is used to indicate warnings or a marginal status; and 3. Red is used to indicate error conditions or a problem requiring immediate attention.	BMD, PCOS
SMTTVS-226	7.1-F – Using color	Color coding must not be used as the only means of communicating information, indicating an action, prompting a response, distinguishing a visual element, or providing feedback on voter actions or selections. **Discussion** While color can be used for emphasis, some other non-color design element is also needed. This could include shape, lines, words, text, or text style. For example, an icon for “stop” can be red enclosed in an octagon shape, or a background color can be combined with a bounding outline and a label to group elements on the ballot. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.	BMD, PCOS
SMTTVS-227	7.1-G – Text size (electronic display)	A voting system’s electronic display must be capable of showing all information in a range of text sizes that voters can select from, with a default text size at least 4.8 mm	BMD, PCOS

Key	Summary	Description	Component/s
		(based on the height of the uppercase I), allowing voters to both increase and decrease the text size. The voting system may meet this requirement in one of the following ways: 1. Provide continuous scaling with a minimum increment of 0.5 mm that covers the full range of text sizes from 3.5 mm to 9.0 mm. 2. Provide at least four discrete text sizes, in which the main ballot options fall within one of these ranges. a. 3.5-4.2 mm (10-12 points) b. 4.8-5.6 mm (14-16 points) c. 6.4-7.1 mm (18-20 points) d. 8.5-9.0 mm (24-25 points) **Discussion** The text size requirements have been updated from the *VVSG 1.1 [VVSG2015]* requirement to better meet the needs of voters who need larger text, including older voters, voters with low literacy, and voters with some cognitive disabilities. This requirement also fills a gap in the text sizes required in *VVSG 1.1* which omitted text sizes needed or preferred by many voters. Although larger font sizes assist most voters with low vision, certain visual disabilities such as tunnel vision require smaller text.	

Key	Summary	Description	Component/s
		The sizes are minimums. These ranges are not meant to limit the text on the screen to a single size. The text can fall in several of these text sizes. For example, candidate names or voting options might be in the 4.8-5.6 mm range, secondary information in the 3.5-4.2 mm range, and titles or button labels in the 6.4-7.1 mm range. The default text size of 4.8 mm is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].* **Applies to:** Electronic interfaces **Related requirements:** 5.2-A – No bias 5.2-F – Preserving votes 7.2-D – Scrolling 7.3-B – No split contests	
SMTTVS-228	7.1-H – Scaling and zooming (electronic display)	When the text size is changed, all other information in the interface, including informational icons, screen titles, buttons, and ballot marking target areas, must change size to maintain a consistent relationship to the size of the text. Informational elements in the interface do not have to be scaled beyond the size of the text. 1. When the text is enlarged up to 200% (or 7.1 mm text size), the ballot layout must adjust so that there is no horizontal scrolling or panning of the screen.	BMD, PCOS

Key	Summary	Description	Component/s
		2. When the text is enlarged more than 200%, there may be horizontal scrolling or panning if needed to maintain the layout of the ballot and a consistent relationship between the text for ballot options and associated marking targets. **Discussion** The intention of this requirement is that all of the informational elements of the interface change size in response to the text size. However, some interface designs include elements that are already large enough that making them larger would distort the layout. In this case, this does not require those elements to grow proportionately beyond the size of the text. Techniques for managing scaling and zooming an electronic interface while adjusting the layout to fit the new size are sometimes called responsive design or responsive programming. This requirement does not preclude novel approaches to on-screen magnification such a zoom lens showing an enlarged view of part of a screen (as long as it meets the requirements in 7.2 for the operability of the controls). This requirement follows WCAG 2.0 [WCAG10] in requiring scaling with no horizontal scrolling up to 200% and allowing zooming with horizontal scrolling for larger text. **Applies to:** Electronic interfaces	

Key	Summary	Description	Component/s
		Related requirements: 7.1-G – Text size (electronic display) 7.2-D – Scrolling 5.1-A – Voting methods and interaction modes 5.2-A – No bias 5.2-C – All information in all modes 5.2-F – Preserving votes	
SMTTVS-229	7.1-I – Text size (paper)	The voting system must be capable of printing paper ballots and other paper records with a font size of at least 3.5 mm (10 points). **Discussion** Although the system can be capable of printing in several font sizes, local or state laws and regulations can also govern the use of various font sizes. If the voting system includes a large-print display option, a good range for the text size is 6.4-7.1 mm matching the size in 7.1-G – Text size (electronic display) If typography changes such as text size or display style are used to differentiate languages on a multi-lingual ballot, the requirements in *5.2-A – No bias* (and relevant state election law for ballot design) still apply. **Applies to:** Printed Material **Related requirements:**	BMD, CCOS, EMP, PCOS

Key	Summary	Description	Component/s
		5.1-E – Reading paper ballots 7.1-G – Text size (electronic display)	
SMTTVS-230	7.1-J – Sans-serif font	The voting system must be capable of presenting text intended for the voter in a sans-serif font. **Discussion** This requirement ensures that systems are capable of best practice while allowing them to also meet local or state laws or regulations that might differ. In general, sans-serif fonts are easier to read on-screen, look reasonably good when their size is reduced, and tend to retain their visual appeal across different platforms. Examples of sans-serif fonts with good readability characteristics include Arial, Calibri, Microsoft Tai Le, Helvetica, Univers, Clearview ADA, or Open Sans. *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]* require that at least one mode of characters displayed on the screen be a sans-serif font.	BMD, EMP, PCOS, TDP
SMTTVS-231	7.1-K – Audio settings	The voting system's audio format interface must meet the following requirements: 1. The settings for volume and rate of speech are followed regardless of the technical means of producing audio output. 2. The default volume for each voting session is set between 60 and 70 dB SPL. 3. The volume is adjustable from a minimum of 20 dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.	BMD, PCOS

Key	Summary	Description	Component/s
		4. The rate of speech is adjustable throughout the voting session while preserving the current votes, with 6 to 8 discrete steps in the rate. 5. The default rate of speech is 120 to 125 words per minute (wpm). 6. The range of speech rates supported is from 60-70 wpm to 240-250 wpm (or 50% to 200% of the default rate), with no distortion. 7. Adjusting the rate of speech does not affect the pitch of the voice. **Discussion** The top speech rate is slower than some audio users prefer for narrative reading to ensure that candidate names are pronounced clearly and distinctively. Note that calculation of rate of speech can vary based on the length of the words in the sample, so requirements are stated as a small range. Speech rates as slow as 50 wpm and as fast as 300 wpm can be included if this can be done without distortion or flanging. This requirement is intended to be tested using “real ear” measurements not simply measurements at the point of the audio source. According to an explanation written by the Trace Center *[TC04]*, 60 dB SPL is the volume of ordinary conversation. FCC regulations for hearing aids, *47 CFR Parts 20 and 68: Hearing Aid Standard [FCC18]*, includes useful information about how to test audio volume and quality. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.	

Key	Summary	Description	Component/s
		Related requirements: 7.1-A – Reset to default settings	
SMTTVS-232	7.1-L – Speech frequencies	The voting system's audio format interface must be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz. **Discussion** The required frequencies include the range of normal human speech. This allows the reproduced speech to sound natural. This is a requirement for the capability of the system so that it is possible to create intelligible audio. It is not a requirement for a ballot in a real election, which is outside of the scope of the VVSG. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*	BMD, PCOS
SMTTVS-233	7.1-M – Audio comprehension	The voting system's audio format interface must be capable of presenting audio content so that it is comprehensible to voters who have normal hearing and are proficient in the language with: 1. proper enunciation, normal intonation, accurate pronunciation in the context of the information, and the capability to pronounce candidate names as intended; 2. low background noise; and 3. recording or reproduction in dual-mono, with the same audio information in both ears.	BMD, PCOS, TDP

Key	Summary	Description	Component/s
		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 are generated by default. To the extent that election officials designing the ballot determine the audio presentation, it is beyond of the scope of this requirement. Support for non-written languages and low literacy includes audio output that is usable by voters who can see the screen. The International Telecommunications Union (ITU) provides a set of freely available test signals for testing audio quality in *Rec. ITU-T P.50 Appendix I [ITU19]*. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.	
SMTTVS-234	7.1-N – Tactile keys	Mechanically operated controls, buttons, keys, or any other hardware interfaces (including dual switches or sip-and-puff devices) on the voting system available to the voter must: 1. be tactilely discernible without activating those controls or keys; 2. include a Unified English Braille, Contracted label if there is a text label; and 3. not require sequential, timed, or simultaneous presses or activations, unless using a full keyboard. **Discussion**	BMD, PCOS, TDP

Key	Summary	Description	Component/s
		A blind voter can operate the voting system by “feel” alone. This means that vision is not necessary for such operations as inserting a smart card or plugging into a headphone jack. Controls that are distinguished only by shape without a text label do not need a Braille label. Controls do not depend on fine motor skills. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].* **Related requirements:** 7.2-E – Touch screen gestures 7.2-H – Accidental activation 7.2-R – Control labels visible 7.3-L – Icon labels	
SMTTVS-235	7.1-O – Toggle keys	The status of all locking or toggle controls or keys (such as the "shift" key) for the voting system available to the voter must be visually discernible, and also discernible through either touch or sound. **Discussion** This applies to any physical controls or keys that have a locking or toggle function. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*	PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-236	7.1-P – Identifying controls	Buttons and controls for the voter that perform different navigation or selection functions must be distinguishable by both shape and color for visual and tactile perception. Well-known arrangements of groups of keys may be used only for their primary purpose. For example, a full alphabetic keyboard is acceptable for entering a write-in candidate name, but individual keys cannot be used for navigation or selection. **Discussion** This applies to buttons and controls implemented either on-screen or in hardware. For on-screen controls, shape includes the label on the button. Redundant cues help those with low vision. They also help individuals who have difficulty reading the text on the screen, those who are blind but have some residual vision, and those who use the controls on a voting system because of limited dexterity. While this requirement primarily focuses on those with low vision, features such as tactile controls and on-screen controls intended primarily to address one kind of disability often assist other voters as well. The Trace Center's EZ Access design is an example of button functions distinguishable by both shape and color *[TCnd].* Some examples are: • Color can be helpful to make different sets of functions visually distinct: groups of buttons can share a color, such as Volume UP/DOWN.	BMD, PCOS

Key	Summary	Description	Component/s
		• Tactile perception requires different shapes, so that finding a control does not rely solely on the layout: all the shapes cannot be squares, but two or four triangles can be used if they point in different directions. • As a group of well-known keys, a full alphabetic keyboard is acceptable for entering a write-in candidate name, but individual keys cannot be used for navigation or selection. Using these keys for functions would require a voter to see the visual labels or know the arrangement for those functions. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.	
SMTTVS-237	7.2-A – Display and interaction options	The voting system must provide at least the following display format and interaction mode options to enable voters to mark their ballot to vote, and verify and cast their ballot, supporting the full functionality in each mode: 1. Visual format; 2. Enhanced visual format; 3. Audio format; 4. Touch mode; and 5. Limited dexterity mode. **Discussion** Voters need to be able to choose the combination of display formats and types of controls that work for them, for example, combining the audio format with the tactile mode.	BMD, Integration, PCOS

Key	Summary	Description	Component/s
		Limited dexterity mode controls include those that do not require dexterity and those that can be operated without use of hands. Full functionality includes at least instructions and feedback regarding: • on how to use accessibility features and setting; • on a change in the display format or control options; • for navigating the ballot; • for contest options, including write-in candidates; • on confirming and changing votes; and • on final ballot submission. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].* **Related requirements**: 5.1-A – Voting methods and interaction modes 5.2-A – No bias	
SMTTVS-238	7.2-B – Navigation between contests	The electronic ballot interface must provide navigation controls that allow the voter to advance to the next contest or go back to the previous contest before completing their vote. **Discussion** For example, voters are not forced to proceed sequentially through all contests before going back to check their votes within a previous contest.	BMD, PCOS

Key	Summary	Description	Component/s
		This requirement applies whether the voter is using the visual or audio format or synchronized audio and visual. As with all requirements, this applies to all display formats and interaction modes. **Related requirements:** 7.2-A – Display and interaction options	
SMTTVS-239	7.2-C – Voter control	An electronic ballot interface must give voters direct control over making or changing vote selections within a contest. This requirement includes the following: 1. In a vote-for-one contest, selecting a candidate may deselect a previously selected candidate, but the system must announce the change in audio and visual display. 2. In a vote-for-N-of-M contest, the system must not deselect any candidate automatically. 3. In a vote-for-N-of-M contest, the system must inform the voter that they have attempted to make too many selections and offer an opportunity to change their selections. 4. Ballot options intended to select a group of candidates, such as straight-party voting, must provide clear feedback on the result of the action of selecting this option. 5. Ballots with preferential or ranking voting methods must not re-order candidates except in response to an explicit voter command.	BMD

Key	Summary	Description	Component/s
		Discussion This requirement covers any selection, de-selection, or change to ballot options. It can be met in a variety of ways, including notifications or announcements of the action the system is taking. For example, if a voter attempts to mark a selection for more candidates than allowed, the system does not take an independent action to de-select a previously selected candidate, but instead notifies the voter of the problem and offers ways to correct it. As with all requirements, this applies to all display formats and interaction modes. This requirement addresses situations in which the voter cannot see the change take effect because the previously selected candidate is on another screen, has scrolled off the visible display area, or is out of the voter's field of vision. It is particularly important to voters using the audio format and no visual display because they often do not have a way to know that a change that occurs higher up in the contest has taken place. Examples of feedback include visual changes on the screen and related sounds or messages in text and audio. For example, selecting a candidate is often announced visually with a check-mark image and in audio by naming the candidate selected. If there is a visual change or announcement about the number of candidates selected (or selections still available), for example, the audio says "you have selected the maximum number of candidates in this contest" in a vote-for-N contest.	

Key	Summary	Description	Component/s
		An example of feedback on the result of a complex action, such as making a selection in straight party voting, might be a message confirming the party whose candidates were selected, or even the number of candidates and contests affected by the voter's action. **Related requirements:** 7.2-A – Display and interaction options 7.3-E – Feedback 7.3-F – Correcting the ballot	
SMTTVS-240	7.2-D – Scrolling	If the number of candidates or length of the ballot question means that the contest does not fit on a single screen using the voter's visual display preferences, the voting system must provide a way to navigate through the entire contest. 1. The voting system may display the contest by: a. *pagination* - dividing the list of candidates or other information into "chunks," each filling one screen and providing ways for the voter to navigate among the different chunks; or b. *scrolling* – keeping all of the content on a single long display and providing controls that allow the voter to scroll continuously through the content.	BMD, PCOS

Key	Summary	Description	Component/s
		2. For either display method, the voting system interface must: a. have a fixed header or footer that does not disappear, so voters always have access to navigation elements, the name of the current contest, and the voting rules for the contest; b. include easily perceivable cues in every display format to indicate that there is more information or there are more contest options available; and c. include an option for an audio format and visual format that sync during scrolling. 3. The navigation method must ensure that the voting system: a. meets all requirements for providing feedback to the voter; b. accurately issues all warnings and alerts including notifications of undervotes and overvotes; c. meets all requirements for control size and interaction, and keeping all controls visible; d. does not rely only on conventional platform scroll bars; and e. provides an opportunity to review and correct selections before leaving the contest. **Discussion**	

Key	Summary	Description	Component/s
		The ability to scroll through a list of candidates on a single logical page can be particularly important when a voter selects larger text or is using the audio format. Information elements that need not scroll might include the name of the contest ("City Council Member"), the voting rules ("vote for 1") and general controls including preference settings or navigation between contests. A scrolling interface that meets this requirement offers voters a combination of easily perceivable controls or gestures to navigate through the list of candidates or text of a ballot question. For example: • Navigation within the contest does not rely on knowledge of any particular computer platform or interface standard. • Navigation within the contest does not only rely on conventional platform scroll bars, which operate differently on two of the major commercial computer platforms. • Controls have visible labels that include words or symbols. • Controls are located in the voter's visual viewing area at the bottom (or top) of the scrolling area, for example in the center of the column of names or paragraph of text. This is especially helpful for people with low digital or reading literacy. • Controls are identified in the audio format and can be activated in all interaction modes.	

Key	Summary	Description	Component/s
		This overall requirement relates to 7.1-G – Text size (electronic display), 7.1-H – Scaling and zooming (electronic display), and 7.3-B – No split contests The controls used to meet this requirement also need to meet all other requirements including 7.2-H – Accidental activation, 7.2.I – Touch area size, 7.2-F – Voter speech, and 7.2-E – Touch screen gestures. Meeting requirements for notifications relates to 7.3-E – Feedback, 7.3-F – Correcting the ballot, 7.3-H – Overvotes, 7.3-I – Undervotes, and 7.3-K – Warnings, alerts, and instructions. **Applies to:** Electronic interfaces **Related requirements:** 7.1-G – Text size (electronic display) 7.1-H – Scaling and zooming (electronic display) 7.3-B – No split contests 7.2-H – Accidental activation 7.2.I – Touch area size 7.2-F – Voter speech 7.2-E – Touch screen gestures 7.3-E – Feedback 7.3-F – Correcting the ballot	

Key	Summary	Description	Component/s
		7.3-H – Overvotes 7.3-I – Undervotes 7.3-K – Warnings, alerts, and instructions	
SMTTVS-241	7.2-E – Touch screen gestures	Voting system devices used by voters with a touch screen may use touch screen gestures (physical movements by the user while in contact with the screen to activate controls) in the interface if the following conditions are met: 1. Gestures are offered as another way of interacting with a touch screen and an optional alternative to the other touch interactions. 2. Gestures work consistently across the entire voting interaction. 3. Gestures do not include navigation off the current contest. 4. Gestures are used in a way that does not create accidental activation of an action through an unintended gesture. 5. Gestures are limited to simple, well-known gestures. 6. Gestures do not require sequential, timed or simultaneous actions. **Discussion** This requirement ensures that the use of gestures does not interfere with the accessibility features of the voting system or make the interface difficult to use by relying on an interaction mode with no easy way to make them perceivable in the visual or audio formats.	BMD, PCOS

Key	Summary	Description	Component/s
		In relying on simple and common gestures, this requirement does not intend to fully duplicate the gestures for commercial mobile platforms used with an audio format for accessibility. Tapping (touching the screen briefly) is the most basic gesture and is used on all touch screens. Other commonly used gestures include: • pinching or spreading fingers to zoom, • swiping to scroll, and • pressing and holding to drag Examples of gestures that require sequential or simultaneous actions are double-tapping, 2, 3 or 4 finger swiping, touch and hold for a set period of time, or those that require coordinated actions with fingers on both hands. On desktop systems, assistive preference options like Sticky Keys can make these complex gestures accessible, but they require familiarity beyond what is acceptable in a voting system. Examples of timed gestures include differentiating between long and short touches, or which require touching twice in rapid succession to highlight and then activate the button or selection. **Applies to:** Electronic interfaces **Related requirements:** 7.2-H – Accidental activation	

Key	Summary	Description	Component/s
		7.1-N – Tactile keys	
SMTTVS-242	7.2-F – Voter speech	If the voting system includes speech or human sounds as a way for voters to control the system: 1. it must not require the voter to speak recognizable voting selections out loud, and 2. speech input must not be the only non-visual interaction mode. **Discussion** This requirement allows the use of speech input as long as voters can choose other ways of interacting with the voting system that do not require either vision or use of their hands. It is also important to consider how speech would work as a way of voting in a noisy polling place environment. **Related requirements:** 6.1-A – Preserving privacy for voters 6.1-D– Audio privacy	BMD, PCOS, TDP
SMTTVS-243	7.2-G – Voter control of audio	The voting system must allow the voter to control the audio format including: 1. pausing and resuming the audio; 2. repeating any information;	BMD, PCOS

Key	Summary	Description	Component/s
		3. skipping to the next or previous contest; and 4. skipping over the reading of the ballot question text. **Discussion** These features can also be useful to voters with cognitive disabilities. This is comparable 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, or • skip over the wording of a referendum on which they have already made a decision prior to the voting session (for example, "Vote yes on proposition #123"). **Applies to:** Electronic interfaces	
SMTTVS-244	7.2-H – Accidental activation	Both on-screen and physical controls on the voting system must be designed to prevent accidental activation. **Discussion** There are at least two kinds of accidental activation: • When a control is activated to execute an action as it is being “explored” by the voter because the control is overly sensitive to touch.	BMD, CCOS, PCOS, TDP

Key	Summary	Description	Component/s
		• When a control is in a location where it can easily be activated unintentionally. For example, when a button is in the very bottom left corner of the screen where a voter might hold the unit for support. The draft of WCAG 2.1, the next version of *WCAG 2.0 [W3C10]* includes a similar requirement and offers guidelines for preventing accidental activation including that the activation be on the release of the control (an "up-event") or equivalent, or that the system provides an opportunity to confirm the action. In addition to the accessibility needs for preventing accidental activation, it can be an issue if voters perceive the voting system as changing their voting selections.	
SMTTVS-245	7.2-I – Touch area size	If the voting system has a touch screen, the touch target areas must: 1. be at least 12.7 mm (0.5 inches) in both vertical and horizontal dimensions; 2. be at least 2.54 mm (0.1 inches) away from adjacent touch areas; and 3. not overlap another touch area. **Discussion** The requirements for touch size areas on voting systems are larger than commercial standards for mobile devices: • to ensure that the touch areas are large enough for voters with unsteady hands; • to ensure that voting systems allow full adjustment to the most comfortable posture; and	BMD, CCOS, PCOS, TDP

Key	Summary	Description	Component/s
		• to allow for touch screens that do not include advanced algorithms to detect the center point of a touch. The required touch area size is larger than some of the commercial standards for mobile phones to allow for use by voters with limited dexterity. The required marking area size is within sizes suggested in the draft WCAG 2.1 (the next version of *WCAG 2.0 [W3C10]*) for target areas that accept a touch action. An MIT Touch Lab study of Human Fingertips to Investigate the Mechanics of Tactile Sense found that the average human finger pad is 10-14mm and the average fingertip is 8-10mm. **Applies to:** Touch screen interfaces	
SMTTVS-246	7.2-J – Paper ballot target areas	On a paper ballot that a voter marks by hand, the area of the target used to mark a voting selection must be at least 3 mm (0.12 inches) across in any direction. **Discussion** This requirement applies to marking ovals, circles, squares, or other optical scan ballot designs. Although the marking target for hand-marked paper ballots needs to be large enough to see, a target that is too large can also make it hard to fill in the area completely. **Applies to:** Paper ballots	CCOS, EMP, Integration, PCOS, TDP

Key	Summary	Description	Component/s
SMTTVS-247	7.2-K – Key operability	Physical keys, controls, and other manual operations on the voting station must be operable with one hand and not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys must be no greater than 5 lbs. (22.2 N). **Discussion** Voters can operate controls without excessive force. This includes operations such as inserting an activation card and inserting and removing ballots. This does not apply to on-screen controls. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*	BMD, PCOS
SMTTVS-248	7.2-L – Bodily contact	**7.2-L – Bodily contact** The voting station controls must not require direct bodily contact or for the body to be part of any electrical circuit. If some form of contact is required, a stylus or other device with built-in permanent tips will be supplied to activate capacitive touch screens. **Discussion** This requirement ensures that controls and touch screens can be used by individuals using prosthetic devices or that it is possible to use a stylus on touch screens for either greater accuracy or limited dexterity input.	BMD, CCOS, PCOS, TDP

Key	Summary	Description	Component/s
		One type of touch screen – capacitive touch panels – rely on the user's body to complete the circuit. They can be used if manufacturers supply a stylus or other device that activates the capacitive screen. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].* — **Applies to:** Electronic interfaces	
SMTTVS-249	7.2-M – No repetitive activation	Voting system keys or controls must not have a repetitive effect when they are held in an active position. **Discussion** 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. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.	BMD, CCOS, PCOS
SMTTVS-250	7.2-N – System response time	The voting system's response time must meet the following response times: 1. The system initially responds to a voter action in no more than: a. 1 seconds for a visual change, or b. 5 seconds for an audio response.	BMD, Integration, PCOS

Key	Summary	Description	Component/s
		2. The system responds to a voter marking a vote in no more than 1 second for both a visual response and an initial audio response. 3. The system completes the visual response or display in no more than 1 second or displays an indicator that a response is still being prepared. **Discussion** This is so the voter can very quickly perceive that an action has been detected by the system and is being processed. The voter never gets the sense of dealing with an unresponsive or "dead" system. Note that this requirement applies to both auditory and visual voting system responses. For example, if the voter touches a button to indicate a vote for a candidate, a visual system might display an "X" next to the candidate's name, and an audio system might announce, "You have voted for John Smith for Governor". Even for "large" operations such as initializing the ballot or painting a new screen, touch screen system ideally should not take more than 10 seconds. In the case of audio systems, no upper limit is specified, since certain operations can take longer, depending on the length of the text being read (for example, reading out a long list of candidates running in a contest). For instance, the system might present a progress bar 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,	

Key	Summary	Description	Component/s
		as long as some visual change is apparent (such as progressively "painting" a new screen or providing audio feedback). **Applies to:** Electronic interfaces	
SMTTVS-251	7.2-O – Inactivity alerts	If the voter has not interacted with the voting system for a long time, that is, between 2-5 minutes, the system must notify the voter and meet the following requirements: 1. The system must document the inactivity time. 2. When the voter's inactivity time expires, the electronic ballot interface must issue an alert and provide a way for the voter to receive additional time. 3. The alert time must be between 20 and 45 seconds. 4. If the voter does not respond to the alert within the alert time, the electronic ballot interface must go into an inactive state requiring election worker intervention. **Discussion** Each type of system will have a given inactivity time that is consistent among and within all voting sessions. This ensures that all voters are treated equitably. For a referendum, in audio format, the timer starts when the audio finishes. **Applies to:** Electronic interfaces	BMD, PCOS

Key	Summary	Description	Component/s
SMTTVS-252	7.2-P – Floor space	When used according to the manufacturer's installation instructions, the voting station must allow floor space for voters using a wheelchair or a voter's assistant by: 1. providing a clear area for a wheelchair of 760 mm (30 inches) wide and 1220 mm (48 inches) deep, and 2. providing adequate room for a voter's assistant, including enough room for both the voter and an assistant to enter the area of the voting station. **Discussion** This requirement sets minimum dimensions for clear floor space around a voting station and ensures that the manufacturer's voting station design and associated installation instructions support polling place layouts that can achieve this requirement. In planning a polling place layout, election officials should consult the *U.S Access Board Technical Guide: Clear Floor or Ground Space and Turning Space [USAB14a]* and the *U.S. Department of Justice ADA Checklist for Polling Places [USDOJ16]* to be sure that a voter using a wheelchair can reach the voting station. They should also consider space needed if a voter's assistant also uses a mobility device.	PCOS, TDP
SMTTVS-253	7.2-Q – Physical dimensions	The physical dimensions of the voting station must meet the U.S. Access Board requirements in *Appendix A* to *Part 1194 – Section 508* of the *Rehabilitation Act: Application and Scoping Requirements, Chapter 4: Hardware, Section 407.8 Operable Parts: Reach Height and Depth [USAB14b].*	BMD, PCOS

Key	Summary	Description	Component/s
		Discussion This requirement is part of *Section 508 Information and Communication (ICT) Standards and Guidelines [USAB18]*. with the text of the requirements for reach height and depth with illustrations in the "#407 operable parts" section. Many voting systems can be set up in a variety of ways for use in a polling place or vote center. For example, a system might sit on a table that allows voters to put their legs under the table in a polling place, but on a counter with no legroom in a vote center. Wheelchairs and scooters also allow voters different abilities to reach controls, and the voter might approach the voting system from the front or side, depending on the physical design and how it is presented to the voter. A guide to meeting the requirements in the ADA standard for ensuring that voters can reach and us all operable parts can be found at *[USAB14b]*.	
SMTTVS-254	7.2-R – Control labels visible	Labels for physical controls used by voters must be placed: 1. on a surface of the voting system where voters can see them from a seated or standing posture, and 2. within the dimensions required in *2-Q – Physical dimensions*. **Discussion** This requirement ensures that voters can find controls, even if they are placed on a side or top surface of the voting system, and that blind voters can discover any Braille labels associated with the text label by touch.	BMD, PCOS

Key	Summary	Description	Component/s
		Related requirements: 7.1-N – Tactile keys 7.2-Q – Physical dimensions 7.3-L – Icon labels	
SMTTVS-265	7.3-A – System-related errors	The voting system must help voters complete their ballots effectively, ensuring that the features of the system do not lead to voters making errors during the voting session. **Discussion** This requirement is included as a summary requirement for *Guideline 7.3* to avoid repeated text in the requirements. As a separate requirement, it is used as a criterion in testing the rest of the requirements in 7.3 and is a way to encourage innovation in meeting this principle.	BMD, PCOS
SMTTVS-266	7.3-B – No split contests	The voting system must have the capability of displaying a ballot so that no contest is split into two groups of options. 1. For paper ballot formats, the system must include a way of presenting a contest that does not divide the options across two columns or two pages. 2. For electronic interfaces, if a contest does not fit onto one screen view, the system must include a way to meet the requirements in *2-D – Scrolling* for managing the way the list of options is displayed. **Discussion**	BMD, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		There is strong evidence from recent elections that when a contest is split into two or more sections, there is a risk that the voter can perceive one contest as two (and overvote), or fail to see all of the contest options (and vote for a candidate other than the one they intend to). This a requirement for a capability of the ballot design or election management tools for the voting system to allow election officials to lay out a ballot with good usability. **Related requirements:** 7.2-D – Scrolling	
SMTTVS-312	7.3-C – Contest information	All ballots must clearly indicate the office or question title and the maximum number of choices allowed for each contest. 1. In an electronic ballot marking interface, the information for each contest includes, in a consistent order: The title of the office or ballot question, including any distinguishing information such as the length of the term or the jurisdiction. 2. The maximum number of selections allowed in the contest. 3. In the audio format only, the number of options or candidates. 4. If any selections have already been made, the number of selections remaining.	BMD, PCOS

Key	Summary	Description	Component/s
		5. In the audio format only, if any selections have been made, the currently selected candidates or options. 6. Any instructions or reminders of how to find marking instructions, placed visually and in audio after the contest information. **Discussion** This requirement is intended to work with any relevant state election laws or regulations for ballot design. For voters using audio features, best practice is to announce how many candidates or voting options are available, providing an audio cue similar to a visual scan of the ballot in a similar way to assistive technology such as screen readers. Placing basic instructions last helps voters using the audio format know when they can skip to making selections in the contest without missing any important information.	
SMTTVS-313	7.3-D – Consistent relationship	The relationship between the name of a candidate or other voting option and the way the voter marks that selection, including the spatial relationship in the ballot layout, must be consistent throughout the ballot for each type of contest. **Discussion** A type of contest includes contests to: • vote for one or more candidates, • answer a ballot question, • vote whether to retain a judge,	BMD, EMP

Key	Summary	Description	Component/s
		• indicate preferential ranking of candidates, or • make a selection in other contests with distinct voting methods. This requirement ensures that the mechanism for marking a selection in a contest to elect one or more candidates to an office is not to the left of some candidates' names and to the right of others. If there is more than one spatial relationship, the difference should not be contradictory or confusing to a voter when combined on a single ballot. **Related requirements:** 7.3-N – Instructions for voters 5.2-A – No bias 2.2-A – User-centered design process 8.3-A – Usability tests with voters	
SMTTVS-314	7.3-E – Feedback	The voting system must provide unambiguous feedback confirming the voter's selection. **Discussion** This requirement applies to electronic interfaces because on paper ballots, the voter supplies the mark to indicate a selection, not the voting system. For example, the system can display a checkmark beside the selected option or conspicuously change its appearance.	BMD

Key	Summary	Description	Component/s
		This requirement also applies to the audio format. It is especially important that the way the status of the process of making selections is announced in the audio format is unambiguous. For example, the phrase “is selected” and “de-selected” can sound similar, especially at faster audio speeds. Choosing phrases that are more distinct, paying attention to the audio phrasing, and testing with the maximum audio speed can help avoid this problem. Designers of paper ballots that include straight-party voting should test feedback features carefully to ensure that voters can understand the scope of their selection and the ballot options it affects. **Applies to:** Electronic interfaces **Related requirements:** 7.2-C – Voter control 7.3-G – Full ballot selections review	
SMTTVS-315	7.3-F – Correcting the ballot	The voting system must provide the voter the opportunity to correct the ballot before it is cast and counted. An electronic ballot interface must: 1. allow the voter to change a vote within a contest before advancing to the next contest;	BMD, PCOS, TDP

Key	Summary	Description	Component/s
		2. provide the voter the opportunity to correct the ballot before it is cast or printed; and 3. allow the voter to make these corrections without assistance. **Discussion** For paper ballots, this can be achieved through appropriately placed written instructions, including requiring the voter to obtain a new paper ballot to correct a mistake. Vote-by-mail ballots can have different instructions for making corrections from those cast in-person. Some voting methods allow a voter to print a replacement ballot, as long as they only cast one. Also, note the requirements for both electronic ballot interfaces and scanners and precinct-count optical scanners in *7.3-H – Overvotes* and in *7.3-I – Undervotes.* This requirement supports *HAVA [HAVA02]*. **Related requirements:** 5.2-F – Preserving votes 7.3-H – Overvotes 7.3-I – Undervotes	

Key	Summary	Description	Component/s
SMTTVS-316	7.3-G – Full ballot selections review	A voting system with an electronic voting interface must provide the voter with a function to review their selections before printing or casting their ballot that: 1. displays all of the contests on the ballot with: a. the voter's selections for that contest, b. a notification that they have not made a selection, or c. a notification that they have made fewer selections than allowed; 2. offers an opportunity to change the selections for a contest and return directly to the review screen to see the results of that change; and 3. allows the voter to continue to the function for casting the ballot without making a correction at any time in the review process. The review function may also be provided on a scanner or other device where the voter marks and casts a paper ballot. **Discussion** This requirement is an implementation of the *HAVA [HAVA02]* requirement that voters be able to review and change their ballot before casting. Electronic interfaces are required to prevent overvotes. This is usually done while originally marking a contest, so there are no overvoted contests to display on the review screen.	BMD, PCOS

Key	Summary	Description	Component/s
		Including a review screen on a scanner that accepts ballots marked by hand gives those voters an opportunity to review how their ballot will be read by the scanner and make any corrections before casting the ballot. **Related requirements:** 5.2-F – Preserving votes 7.3-H – Overvotes 7.3-I – Undervotes	
SMTTVS-317	7.3-H – Overvotes	The voting system must notify the voter if they attempt to select more than the allowable number of options within a contest (overvotes) and inform them of the effect of this action before the ballot is cast and counted. 1. An electronic ballot interface must prevent voters from selecting more than the allowable number of options for each contest. 2. A scanner or other device that a voter uses to cast a paper ballot must be capable of providing feedback that identifies specific contests that have been overvoted in visual format, and with either audio format or sound cues. **Discussion** This requirement does not specify exactly how the system will respond when a voter attempts to select an "extra" candidate. For instance, the system can present the	BMD, Integration, PCOS

Key	Summary	Description	Component/s
		warning, or, in the case of a single-choice contest (vote for 1), simply change the vote selection and issue a warning. For electronic ballot interfaces, this requirement does not allow disabling the features that prevent overvotes. Voters marking paper ballots can be informed of the effect of overvoting through appropriately placed instructions. This requirement supports *HAVA [HAVA02]*. **Applies to:** Electronic interfaces and ballot scanners **Related requirements:** 5.1-D – Accessibility features 7.2-C – Voter control 7.3-K – Warnings, alerts, and instructions	
SMTTVS-318	7.3-I – Undervotes	The voting system must notify voters in both visual and audio formats of the specific contest in which they select fewer than the allowable number of options (that is, for undervotes). 1. Both electronic interfaces and scanners must allow the voter to submit an undervoted ballot without correction.	BMD, Integration, PCOS

Key	Summary	Description	Component/s
		2. The voting system may allow election officials to disable the notification of undervotes on a scanner. **Discussion** For electronic interfaces, this notification can be incorporated into the review feature. This requirement supports *HAVA [HAVA02]*. **Applies to:** Electronic interfaces and scanners **Related requirements:** 7.2-C – Voter control 7.3-K – Warnings, alerts, and instructions	
SMTTVS-319	7.3-J – Notification of casting	1. The voting system must notify the voter in both visual and audio format whether their ballot was successfully or unsuccessfully cast. If a ballot is not successfully cast (that is, the device did not complete the documented procedures for the system, including reading a paper ballot, recording an electronic image or record, or transporting the ballot to a ballot box), the voting device must notify the voter and provide clear instruction as to the steps the voter needs take to cast the ballot.	BMD, PCOS

Key	Summary	Description	Component/s
		2. A scanning device must be capable notifying the voter that they have cast a paper ballot that is blank on one or both sides. The system may provide a means for an authorized election official to deactivate the notification of a blank ballot. **Discussion** The purpose of this requirement is to provide feedback to voters to assure them that the voting session has been completed. Note that either a false notification of success or a missing confirmation of actual success violates this requirement. Detecting situations in which the voter might be unaware that the ballot is two-sided and left one side blank is distinct from the ability to detect and warn about undervoting. At a minimum, this requirement is intended to ensure that blind and low-vision voters receive an audio notification that a ballot is successfully cast. This might be a sound that is the audio equivalent of a waving flag or other visual. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*	
SMTTVS-320	7.3-K – Warnings, alerts, and instructions	Warning, alerts, and instructions issued by the voting system must be distinguishable from other information. 1. Warnings and alerts must clearly state in plain language: a. the nature of the issue or problem,	BMD, PCOS, TDP

Key	Summary	Description	Component/s
		b. whether the voter has performed or attempted an invalid operation or whether the voting system itself has malfunctioned in some way, and c. the responses available to the voter. 2. Each step in an instruction or item in a list of instructions must be separated: a. spatially in visual formats, and b. with a noticeable pause in audio formats. **Discussion** For instance, “Do you need more time? Select ‘Yes’ or ‘No’.” rather than “System detects imminent timeout condition.” In case of an equipment failure, the only action available to the voter might be to get assistance from an election worker. Keeping instructions separate includes not "burying" several unrelated instructions in a single long paragraph. Alerts intended to confirm visual changes to a voter using the audio format (such as confirmation that the screen has been turned on or off) can be communicated in audio, with a short text or sound. This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.	
SMTTVS-321	7.3-L – Icon labels	When an icon is used to convey information, indicate an action, or prompt a response, it must be accompanied by a corresponding label that uses text.	BMD, PCOS, TDP

Key	Summary	Description	Component/s
		The only exception is that the two 3.5 mm (1/8 inch) jacks for audio and personal assistive technology (PAT) may be labeled with tactilely discernable and visually distinct icons of a headset (for audio) and wheelchair (for the PAT connector) that are at least 13 x 13 mm in size. **Discussion** While icons can be used for emphasis when communicating with the voter, they are not to be the only means by which information is conveyed, since there is no widely accepted "iconic" language, and therefore, not all voters might understand a given icon. The exception is based on the *ADA Standards for Accessible Design. Chapter 7 [ADA10]*. **Related requirements:** 7.1-N – Tactile keys 7.2-R – Control labels visible 8.1-E – Standard audio connectors 8.1-I – Standard PAT jacks	
SMTTVS-322	7.3-M – Identifying languages	A vote-capture device or other voting session device that offers language options to a voter must: 1. visibly present the controls to identify or change language on the screen at all times, not hidden within a help or settings feature, and	BMD, PCOS

Key	Summary	Description	Component/s
		2. include the native version of each language name in the list of language options. **Discussion** Voters looking for an option for an alternative language can recognize it more easily as it is written in the language itself. The English name or spelling can also be used to identify language, along with the native name. **Applies to:** Electronic interfaces	
SMTTVS-323	7.3-N – Instructions for voters	The voting system must provide voters access to instructions for all its operations at any time during the voting session. 1. For electronic interfaces, the voting system must provide a way for voters to get help directly from the system. 2. For paper ballots, the system must be capable of including on the ballot both text and images with instructions for how to mark the ballot. 3. Voting systems must present instructions near to where they are needed during the voting session. **Discussion**	BMD, PCOS, TDP

Key	Summary	Description	Component/s
		The purpose of this requirement is to minimize voters' need for assistance from an election worker and to permit the voter to verify and cast, privately and independently, the votes selected. When the system works correctly, the voter will find the help they need from the system when and where they need it. For instance, only general instructions should be grouped at the beginning of the ballot; those pertaining to specific situations should be presented near those situations. If an operation is available to the voter, it will be documented. Examples include how to make a vote selection, navigate among contests, cast a straight party vote, cast a write-in vote, adjust display and audio characteristics, or select a language. Electronic ballot interface systems often provide assistance with a distinctive "help" button. Instructions can be on the ballot itself or separate from the ballot, as long as the voter can find them easily. **Related requirements:** 5.1-F – Accessibility documentation	
SMTTVS-324	7.3-O – Instructions for election workers	The voting system must include clear, complete, and detailed instructions and messages for setup, polling, shutdown, and how to use accessibility features. 1. The documentation required for normal voting system operation must be:	BMD, CCOS, PCOS, TDP

Key	Summary	Description	Component/s
		a. presented at a level appropriate for election workers who are not experts in voting system and computer technology, and b. in a format suitable for use in the polling place. 2. Printed procedural instructions, and on-screen instructions and messages must enable the election workers to verify that the voting system a. has been set up correctly (setup), b. is in correct working order to record votes (polling), and c. has been shut down correctly (shutdown). **Discussion** This requirement covers documentation for those aspects of system operation normally performed by election workers and other "non-expert" operators. It does not address inherently complex operations such as ballot definition. The instructions are usually in the form of a written manual, but can 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 election workers as they attempt to perform a setup, polling, or shutdown operation. Specific guidance on how to implement this requirement is contained in *[NIST08]*. For instance, the documentation should not presuppose familiarity with personal computers. And a single large reference manual that simply presents details of all	

Key	Summary	Description	Component/s
		possible operations would be difficult to use, unless accompanied by aids such as a simple "how-to" guide. It is especially important that election workers and other non-expert workers know how to set up accessibility features which are not used frequently. This will help ensure voters who need these features can vote privately and independently. Overall, election workers should not have to guess whether a system has been setup correctly. The documentation should make it clear what the system "looks like" when correctly configured. **Related requirements:** 5.1-F – Accessibility documentation	
SMTTVS-325	7.3-P – Plain language	Information and instructions for voters and election workers must be written clearly, following the best practices for plain language. This includes messages generated by the voting system for election workers in support of the operation, maintenance, or safety of the system. **Discussion** The plain language requirements apply to instructions that are inherent to the voting system or that are 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.	BMD, CCOS, PCOS, TDP

Key	Summary	Description	Component/s
		Any legally required text is an exception to this plain language requirement. Plain language best practices are guidelines for achieving clear communication and include: • Using familiar, common words and avoiding technical or specialized words that voters are not likely to understand. For example, "There are more contests on the other side" rather than "Additional contests are presented on the reverse." • Issuing instructions on the correct way to perform actions, rather than telling voters what not to do. For example, “Fill in the oval for your write-in vote to count” rather than, “If the oval is not marked, your write-in vote cannot be counted.” • Addressing the voter directly rather than use passive voice when giving instructions. For example, "remove and retain this ballot stub" rather than "this ballot stub must be removed and retained by the voter." • Stating a limiting condition first, followed by the action to be performed when an instruction is based on a condition. For example, use "In order to change your vote, do X", rather than "Do X, in order to change your vote." • Avoiding the use of gender-based pronouns. For example, "Write in your candidate’s name directly on the ballot" rather than "Write in his name directly on the ballot."	

Key	Summary	Description	Component/s
		For specific guidance on how to implement this requirement, see *[NIST09a].* Although part of general usability, using plain language is also expected to assist voters with cognitive disabilities. Information written in plain language is easier to translate to meet language access requirements.	

Key	Summary	Description	Component/s
SMTTVS-186	8.1-A – Electronic display screens	If the voting system uses an electronic display screen, the display must have the following characteristics: 1. For all electronic display screens: • antiglare screen surface that shows no distinct virtual image of a light source or a means of physically shielding the display from such reflections, and • minimum uniform diffuse ambient contrast ratio for 500 lx illuminance: 10:1. 2. If the display is the primary visual interface for making vote selections: • minimum diagonal display size: 12 inches, and • minimum display resolution: 1920 x 1080 pixels. 3. If the display screen is for messages to voters or poll workers:	BMD, CCOS, PCOS, TDP

Key	Summary	Description	Component/s
		• minimum diagonal display size: 7.9 inches, and • minimum display resolution: 1024x768 pixels. **Discussion** Displays that measure larger than the 12-inch diagonal provide the opportunity for ballot layouts that can more easily use large text settings. **Applies to**: Electronic interfaces	
SMTTVS-187	8.1-B – Flashing	If the voting system emits light in flashes, there must be no more than three flashes in any one-second period. **Discussion** This requirement has been updated to meet WCAG 2.0 [W3C10] and Section 508 [USAB18] software design issue standards. **Applies to**: Electronic interfaces	BMD, CCOS, PCOS, TDP
SMTTVS-188	8.1-C – Personal Assistive Technology (PAT)	The support provided to voters with disabilities must be intrinsic to the voting system so that a voter's personal assistive devices will not be necessary to operate the voting system correctly. **Discussion** This requirement does not preclude the voting system from providing interfaces to assistive technology. (See definition of "personal assistive devices" in Appendix A -	BMD, PCOS, TDP

Key	Summary	Description	Component/s
		Glossary). Its purpose is to ensure that voters are not required to bring special devices with them to vote successfully. This requirement assumes that voters can use their personal headsets, hearing aids, eyeglasses, canes, or other aids they typically have with them.	
SMTTVS-189	8.1-D – Secondary ID and biometrics	If a voting system uses biometric measures for identifying or authenticating voters and election workers, it must provide an alternative that does not depend on the same biometric capabilities. **Discussion** For example, if fingerprints are used for voter identification, another mechanism will be provided for voters without usable fingerprints. This requirement is based on WCAG 2.0 [W3C10] and Section 508 [USAB18].	Integration, TDP
SMTTVS-190	8.1-E – Standard audio connectors	The voting system must provide its audio signal for the audio format interface through an industry standard connector using a 3.5 mm (1/8 inch) stereo headphone jack to allow voters to use their own audio assistive devices for private listening. **Applies to**: Electronic interfaces	BMD, PCOS, TDP
SMTTVS-191	8.1-F – Discernable audio jacks	The audio jack on any voting station device must be in a location that voters can discover, discernable by touch while sitting or standing in front of the unit, and not located near a sharp edge. **Discussion**	BMD, PCOS, TDP

Key	Summary	Description	Component/s
		For example, if the jack is slightly recessed with a round bezel, it will be easier for voters to identify the jack and to insert the headset plug into it.	
SMTTVS-194	8.1-G – Telephone style handset	If the voting system uses a telephone style handset or headphone to provide audio information, it must provide a wireless T-Coil 9 coupling for assistive hearing devices so it provides access to that information for voters with partial hearing, achieving at least a category T4 rating as defined by the American National Standard Institute (ANSI) for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19-2019 [ANSI19]. **Discussion** This requirement applies only to telephone style handsets/headphones to ensure their compatibility with assistive hearing devices. This requirement is based on WCAG 2.0 [W3C10] and Section 508 [USAB18]. **Related requirements**: 8.1-J – Hearing aids 6.1-D – Audio privacy	TDP
SMTTVS-212	8.1-H – Sanitized headphones	The voting system must be supplied with a means to sanitize headphones or handsets and instructions on the procedure to ensure that a sanitized headphone or handset is available to each voter. **Discussion**	BMD, PCOS, TDP

Key	Summary	Description	Component/s
		This requirement can be achieved in various ways, including the use of "throwaway" headphones or sanitary coverings.	
SMTTVS-213	8.1-I – Standard PAT jacks	A vote-capture device or voter-facing device must provide a 3.5 mm (1/8 inch) industry standard jack which voters can use to connect their personal assistive technology switch to the system. The jack must allow only switch activations to be transmitted to the system. The system must accept switch input that is functionally equivalent to other input methods. All the functionality of the voting system must be available through technology using this input mechanism. **Discussion** This requirement is related to the requirements for low dexterity modes (in 5.1-A – Voting methods and interaction modes and in 7.2-A – Display and interaction options). It ensures that voters with very low dexterity, in particular those who do not have the use of their hands, can use the vote-capture devices by providing a means for them to connect personal assistive technology (PAT) if they cannot use the supplied touch or tactile input devices. Examples of personal assistive technology switches include dual switches (sometimes called “adaptive switches” or “jelly switches”) and "sip and puff" devices that communicate as a single key press.	BMD, PCOS, TDP

Key	Summary	Description	Component/s
		Ideally, the jack will be on the tactile keypad or have some other mechanism to provide sufficient reach to a wheelchair tray or the voter's lap. 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. The PAT jack is separate from the audio jack required in 8.1-F – Discernible audio jacks, which connects to the audio output provided by the system. **Related requirements**: 5.1-A – Voting methods and interaction modes 7.2-A – Display and interaction options	
SMTTVS-214	8.1-J – Hearing aids	Voters who use assistive hearing devices must be able to use voting devices as intended: The voting device must not cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices. The voting device, measured as if it were a wireless device, must 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 C63.19-2019 [ANSI19]. **Discussion** "Hearing devices" include hearing aids and cochlear implants. This requirement is based on WCAG 2.0 [W3C10] and Section 508 [USAB18].	BMD, PCOS, TDP

Key	Summary	Description	Component/s
		Related requirements 8.1-G – Telephone style handset	
SMTTVS-215	8.1-K – Eliminating hazards	Devices associated with the voting system must be certified in accordance with the requirements of IEC/UL 62368-1 [UL19], Edition 3: Standard for Audio/video, Information and Communication Technology Equipment - Part 1: Safety requirements 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 is acceptable if it includes IEC/UL 62368-1 [UL19]. **Discussion** IEC/UL 62368-1 is a comprehensive standard for IT equipment and addresses all the hazards discussed above under Safety. It replaces IEC/UL 60950-1 [UL07].	BMD, CCOS, EMP, PCOS, TDP
SMTTVS-216	8.2-A – Federal standards for accessibility	Voting systems must meet federal standards for accessibility, including the version of Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines [USAB18], in effect as of January 18, 2018, and the WCAG 2.0 Level AA checkpoints [W3C10] included in that standard. **Discussion** This applies to all parts of the voting system including the election management system (EMS).	BMD, CCOS, EMP, PCOS, TDP

Key	Summary	Description	Component/s
		Section 508 standards apply to electronic and information technology, including computer hardware and software, websites, multimedia, and other technology such as video, phone systems, and copiers. This requirement also supports the ADA [ADA10]. **Applies to:** Electronic interfaces, including EMS	
SMTTVS-217	8.3-A – Usability tests with voters	The manufacturer must conduct usability tests with voters using the voting system, including all voter activities in a voter session from ballot activation to verification and casting. The test participants must include voters who represent the following: General population, using the visual interface (without audio), including: voters who are native speakers of the language being tested for each language defined as supported in the technical data package (TDP); blind voters, using the audio format plus tactile controls; voters with low vision, using the enhanced visual features with and without audio; and voters with limited dexterity, using the visual interface with low and no dexterity controls. The manufacturer must submit a report of the results of their usability tests, including effectiveness, efficiency, and satisfaction measures, as part of the TDP using ISO/IEC 25062:2006: Common Industry Format (CIF) for Usability Test Reports [ISO06b]. **Discussion**	BMD, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		Voting system developers are required to conduct realistic usability tests on their product before submitting the system to conformance testing. This is to ensure that the user-centered design process required for quality implementation has produced a usable and accessible voting system. **Related requirements** 5.1-D – Accessibility features 2.2-A – User-centered design process	
SMTTVS-255	8.4-A – Usability tests with election workers	The manufacturer must conduct usability tests of the voting system setup, operation during voting, and shutdown as documented by the manufacturer, with representative election workers, to demonstrate that election workers can learn, understand, and perform these tasks successfully. The tasks to be covered in the test must include: 1. Setup and opening for voting, which involves: operation during voting; 2. use of assistive technology or language options that are part of the voting system; 3. shutdown at the end of a voting day during a multi-day early voting period, if supported by the voting system; 4. shutdown at the end of voting including running any reports;	BMD, Integration, PCOS, TDP

Key	Summary	Description	Component/s
		5. providing ballots in different languages; 6. selecting the correct ballot type (for example, for vote centers); and 7. setting up the voting system to use different display formats and interaction modes. The test participants must include election workers representing a range of experience. The manufacturer must submit a report of the results of their usability tests, as part of the TDP using ISO/IEC 25062:2006: Common Industry Format (CIF) for Usability Test Reports [ISO06b]. **Discussion** Voting system manufacturers are required to conduct realistic usability tests on their product before submitting the system to conformance testing. This is to ensure that the user-centered design process required for quality implementation has produced a usable and accessible voting system. This requirement covers the procedures and operations for those aspects of system operation normally performed by election workers and other "non-expert" operators. It does not address inherently complex operations such as ballot definition or system repair. These "normal" procedures should not require any special expertise. The procedures may require a reasonable amount of training, similar to the training generally provided for temporary election workers. **Related requirements** 7.3-O – Instructions for election workers	

Key	Summary	Description	Component/s
		2.2-A – User-centered design process	

Key	Summary	Description	Component/s
SMTTVS-389	9.1.1-A – Software independent	The voting system must be software independent. 1. The voting system must meet the requirements within the Paper-based System Architectures or Cryptographic E2E Verifiable System Architectures section, or both. 2. The voting system documentation must include the method used to provide software independence. **Discussion** Software independence *[Rivest06]* means that an undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results. All voting systems need to be software independent in order to conform to the VVSG. There are two essential concepts behind applying software independence: • it must be possible to audit voting systems to verify that ballots are being recorded correctly, and	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		• testing software is so difficult that audits of voting system correctness cannot rely on the software itself being correct. Therefore, voting systems need to be 'software independent' so that the audits do not have to trust that the voting system's software is correct. The voting system will provide proof that the ballots have been recorded correctly, that is, voting records will be produced in ways in which their accuracy does not rely on the correctness of the voting system's software. This is a major change from previous versions of the VVSG because previous versions permitted voting systems that are software dependent, that is, voting systems whose audits rely on the correctness of the software. One example of a software dependent voting system is the DRE, which is now non-conformant to this version of the VVSG. There are currently two methods specified in the VVSG for achieving software independence: • through the use of independent voter-verifiable paper records, and • cryptographic E2E verifiable voting systems. Paper-based and cryptographic E2E verifiable system architectures are software independent, and both can be used within the same voting system. In this case where a voting system is identified as being a combination of both architectures, the system would need to be compliant with both sets of requirements.	

Key	Summary	Description	Component/s
		Knowing the specific mechanism used to achieve software independence assists with determining if the system truly is software independent. The documentation should explain how any changes to the election outcome are detectable regardless of any fault or error in the voting system software. This may include how the voting systems handles a ballot after it is cast by the voter. For example, this documentation may answer the following questions: • Is it able to print on the ballot? • What information is printed on the ballot? • Where is that information printed?	
SMTTVS-390	9.1.2-A – Tamper-evident records	The voting system must produce tamper-evident records that enable detection of incorrect election outcomes, including: 1. capturing the contents of each vote at the time of each ballot's casting, and 2. recording detected errors in a tamper-evident manner. **Discussion** Tamper-evident records include CVRs, ballot images and artifacts from a cryptographic E2E verifiable voting system. The record also ensures that identified issues and other problems cannot be lost or unintentionally modified once they are discovered.	CCOS, EMP, Integration, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-391	9.1.2-B – Tamper-evident record creation	Paper records or other tamper-evident electronic records of the voter's ballot selections must be captured when each ballot is cast. **Discussion** Voter-facing scanners and other vote-capture devices produce the paper records or other tamper evident electronic records. These records can be useful artifacts for post-election audits.	BMD, PCOS, Security, TDP
SMTTVS-392	9.1.3-A – Records for voter verification	The voting system must provide individual voters the opportunity to verify that the voting system correctly interpreted their ballot selections. **Discussion** • Voter-facing scanners and other vote-capture devices can be used to meet this requirement. An electronic ballot marker can print a voter's ballot selections to review before casting. An E2E verifiable system can print a receipt that allows a voter to verify their selections are tabulated and captured correctly. *Principle 7: Marked, Verified, and Cast as Intended* includes more requirements for voter verification.	BMD, Integration, PCOS, Security, TDP
SMTTVS-393	9.1.3-B – Ballot error correction	The voting system must allow a voter to start a new voting session if they would like to correct an error found in their ballot selections. **Discussion** If, after printing their ballot, a voter decides they would like to update or change a selection before casting, the voter must be able to get a new ballot and start a new	BMD, PCOS, Security, TDP

Key	Summary	Description	Component/s
		voting session to mark their ballot as they intend. A voter can contact a poll worker to spoil their current ballot, receive a new ballot, and start a new voting session	
SMTTVS-394	9.1.3-C – Voter reported errors	Voting system documentation must describe a method, either through procedural or technical means, for voters to report detected errors or incorrect results. **Discussion** This can include a voter alerting an election worker or pressing a button on the machine to report detected errors or incorrect results.	BMD, PCOS, Security, TDP
SMTTVS-395	9.1.4-A – Auditor verification	Voting systems must generate records that would enable external auditors to verify that cast ballots were correctly tabulated. **Discussion** The voting systems themselves cannot make records available to the public. The manner and decision to make these records available is made by a state and or local jurisdiction. This requirement only ensures that the records themselves are generated and can be easily accessed without additional software or assistance from the voting system manufacturer. This requirement is meant to enable external auditors to perform their own count of the election results.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-396	9.1.4-B – Documented procedure	The voting system manufacturer must provide a documented procedure to verify that cast ballots were correctly tabulated. **Discussion**	EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		This documentation includes procedures and technical practices that verify the results post-election and demonstrates software independence. This documentation could be used as a starting point for election officials to develop the procedures used to audit an election.	
SMTTVS-397	9.1.5-A – Paper record production	A paper-based voting system must produce a voter-verifiable paper record of the voter's ballot selections. **Discussion** Voting systems that use independent voter-verifiable records can satisfy the software independence requirement and achieve conformance to the VVSG.	BMD, PCOS, Security, TDP
SMTTVS-398	9.1.5-B – Paper record retention	The recorded ballot selections must be presented in a human-readable format that is understandable by the voter. **Discussion** The requirement ensures that a human-readable version of the data is also printed whenever a barcode is used to encode ballot selections.	BMD, PCOS, Security, TDP
SMTTVS-399	9.1.5-C – Paper record intelligibility	The recorded ballot selections must be presented in a human-readable format that is understandable by the voter. **Discussion** The requirement ensures that a human-readable version of the data is also printed whenever a barcode is used to encode ballot selections.	BMD, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-403	9.1.5-D – Matching selections	All representations of a voter's ballot selections produced by the voting system must agree with the selections made by the voter.	BMD, CCOS, PCOS, Security, TDP
SMTTVS-405	9.1.5-E – Paper record transparency and interoperability	All barcode representations of a voter's ballot selections must use an open and interoperable format.	BMD, PCOS, Security, TDP
SMTTVS-407	9.1.5-F – Unique identifier	A paper-based voting system must be capable of adding a unique identifier after a voter casts their ballot. **Discussion** Although not all jurisdictions may use this feature, voting systems are required to have the capability to add a unique identifier to ballots.	CCOS, PCOS, Security, TDP
SMTTVS-408	9.1.5-G – Preserving software independence	After a voter verifies their selections on a voted ballot and submits the ballot for casting, a paper-based voting system must not be capable of making an undetectable change to the paper record. **Discussion** After a voter verifies and submits their ballot, a voting system may print on paper ballot to apply a unique identifier that is later used for auditing purposes. To	BMD, CCOS, PCOS, Security, TDP

Key	Summary	Description	Component/s
		preserve software independence the voting system should not be able to print over or within the ballot selection area because that would cause an undetectable change to the election outcome. Instead, the voting system should only be able to print outside of the bounds of the ballot selection area and may also create further distinction by printing in a different font style or color. This printing process should be preserved regardless of software or hardware updates.	
SMTTVS-431	9.2-A – Audit support documentation	The voting system documentation must specify the types of audits the voting system supports and the artifacts that the voting system provides to support those audits. **Discussion** Ballots, CVRs, and ballot images are examples of artifacts that can support a post-election audit.	BMD, EMP, PCOS, Security, TDP
SMTTVS-436	9.3-A – Data protection requirements for audit records	All voting systems must meet the requirements listed under Guidelines *13.1* and *13.2* that are related to protecting audit records. **Discussion** CVRs and ballot images need sufficient data protection because they are needed for audits.	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-443	9.4-A – Risk-limiting audit	A paper-based voting system must produce paper records that allow election officials to conduct a risk-limiting audit. **Discussion** Voting systems contain information which enables election officials to conduct risk-limiting audits. For example, batch subtotal reporting by the voting system may make the process of ballot sampling more efficient. An evidence-based election requires convenient access to ballot sheets, ballot sheet images, and cast vote records for efficient and trustworthy public tabulation audits. Vendors should demonstrate how an election system provides all the information necessary for an independent Risk-Limiting Audit (RLA). Some example features/paper records that may be produced to support risk-limiting audits include the following: • the ability to associate electronic cast vote records (CVRs) with corresponding paper records while also preserving ballot secrecy; • the ability to export of CVRs in an open and interoperable format; • the ability to create a ballot manifest that allows users to identify the physical location of ballots (e.g., scanner name or number, batch number, and ballot sequence number); and • supporting multi-sheet ballots, including association of each sheet with its corresponding CVR.	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-448	9.4-B – Random numbers supporting audit processes	Voting systems that generate or rely on random or pseudo-random numbers for auditing purposes must document the method used to obtain the numbers and how the random numbers are used within the voting system. **Discussion** Various systems used to implement software independence require random numbers, whether for ballot selection for audits. This documentation should specify: • how random numbers are generated, and • what any random numbers are used for. One common use for random numbers is to create unique identifiers associated with ballots to assist in supporting audits. The method for generating the pseudo-random numbers should meet the requirement *10.2.2-E Randomly generated identifiers.* For additional information, see *NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators [NIST15a].*	BMD, EMP, Integration, PCOS, Security, TDP
SMTTVS-450	9.4-C – Unique ballot identifiers	The voting system must enable election auditors to uniquely address individual ballots. **Discussion**	CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		This capability is needed to support RLAs. Although the voting system has this capability, this does not require jurisdictions to use this feature if it conflicts with state laws. In order to conduct a ballot-comparison risk-limiting audit, paper ballot records must either be stored in the order in which they were scanned or contain a unique ballot identifier. A unique ballot identifier is a unique ID that provides information about the device it was scanned on and the batch in which it is stored. One example of a unique ballot identifier is scanner ID, batch ID, and ballot card number. The unique ballot identifier must not tie a ballot to an individual voter. The voting system must enable election auditors to uniquely address individual ballots.	
SMTTVS-452	9.4-D – Multipage ballots	The voting system must be able to account for multipage ballots.	CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-195	10.1-A – System use of voter information	The voting system must be incapable of accepting, processing, storing, and reporting identifying information about a specific voter. **Discussion**	CCOS, PCOS, Security, TDP

Key	Summary	Description	Component/s
		Examples include first name, last name, address, driver's license, and voter registration number and other personally identifiable information (PII). This requirement applies to the voting system itself, as the voting system cannot prevent a voter from self-identifying within write-in fields or other areas of the ballot.	
SMTTVS-196	10.2.1-A – Direct voter associations	The voting system must not create or store direct associations between a voter's identity and their ballot. **Discussion** A direct voter association would be the voting system storing that John Smith voted for George Washington. Other examples of a direct association would include tying ballot selections to a social security number, voter identification number, or driver's license number. (This is not an exhaustive list of direct voter association examples.)	PCOS, Security, TDP
SMTTVS-197	10.2.1-B – Indirect voter associations	Indirect voter associations must only be used to associate a voter with their encrypted ballot selections. **Discussion** Certain channels of voting require indirect associations so that ineligible ballots can be removed before the ballot is read and counted. Some reasons include signature mismatch or death of a voter. The most common example of indirect association would be a randomly generated number. Best practice would ensure that indirect voter associations are only available to authorized election personnel.	Security, TDP

Key	Summary	Description	Component/s
		This requirement only applies to paperless voting systems that also meet the requirements under Guideline 9.1, which states that the voting system must be software independent. During the writing of these requirements, cryptographic E2E verifiable voting systems are a potential paperless and software independent system that could be applicable for this requirement.	
SMTTVS-202	10.2.2-A – Identifiers used for audits	Identifiers used for tying a cast vote record (CVR) and ballot images to physical paper ballots must be distinct from identifiers used for indirect associations. **Discussion** For the purpose of these requirements, associations between physical ballots and CVRs are not considered direct or indirect identifiers.	CCOS, EMP, Integration, PCOS, Security, TDP
SMTTVS-203	10.2.2-B – No voter record order information	The voting system must not contain data or metadata associated with the CVR and ballot image files that can be used to determine the order in which ballots votes are cast. **Discussion** No data or metadata is allowed whether in CVRs and ballot images or elsewhere if that metadata can be used to associate a voter with a record of voter intent. Otherwise, metadata can be useful for verification. For instance, date of creation of record in the voter-facing device might reveal the order of voting. Most other metadata will not be a problem.	CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-204	10.2.2-C – Identifying information in voter record file names	CVR and ballot image file names must not include any information identifying a voter. **Discussion** This helps to ensure that information that could accidentally be used to reference a voter is not used within a file name.	CCOS, PCOS, Security, TDP
SMTTVS-205	10.2.2-D – Aggregating and ordering	Aggregated and final totals: 1. must not contain voter identifying information, and 2. must not be able to recreate the order in which the ballots were cast. **Discussion** Voter identifying information includes social security number, voter identification number, or driver's license number.	CCOS, EMP, PCOS, Security, TDP
SMTTVS-206	10.2.2-E – Randomly generated identifiers	Randomly generated identifiers used for audits must use random bit generators specified in the latest revision of *NIST SP 800-90* series on random bit generators. **Discussion** This requirement is important to ensure the use of a cryptographically secure pseudo-random number generator (CSPRNG) and also to ensure any random numbers, such as unique identifiers on a ballot, cannot be used to recreate the order in which a ballot was cast. Recreating the order of cast ballots can cause ballot secrecy issues if a voter's ballot can be identified.	EMP, Integration, PCOS, Security, TDP

Key	Summary	Description	Component/s
		To ensure voting system vendors are following the random number generation recommendations in the 800-90 series, they will need to submit to the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP) for conformance testing. For additional information, see *NIST SP 800-90A Rev 1*, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators [NIST15a]* and *NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation [NIST18a].*	
SMTTVS-207	10.2.3-A – Restrict access to records of voter intent	The voting system must require administrator-level authorization to access the directory or storage location of CVRs, ballot images, and ballot selections. **Discussion** Cast vote records, ballot images, and ballot selections should be subject to special restrictions on access. Permissions to access these storage locations are limited only to those users who need to access the location. This may be especially essential during voting to protect ballot secrecy and avoid any exposure of results until polls are closed.	CCOS, EMP, PCOS, Security, TDP
SMTTVS-208	10.2.3-B – Digital voter record access log	The voting system must log all access to the directory or storage location for CVRs, ballot images, and ballot selections in addition to logging access to all actions occurring within the system.	CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		Discussion This ensures that any person, process, or other entity reading, writing, or performing other actions to the electronic audit trail is properly logged. This requirement does not apply when the CVR, ballot images, and ballot selections are stored on removable media and removed from the vote-capture device.	
SMTTVS-210	10.2.4-B – Logging of ballot selections	Logs and other portions of the audit trail must not contain individual or aggregate ballot selections. **Discussion** The voting system needs to be constructed so that the security of the system does not rely upon the secrecy of the event logs. It will be considered routine for event logs to be made available to election officials, and possibly even to the public, if election officials so desire. The system will be designed to permit the election officials to access event logs without fear of negative consequences to the security and integrity of the election. For example, cryptographic secret keys or passwords will not be logged in event log records.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-211	10.2.4-C – Activation device records	Ballot activation devices must not create or retain information that can be used to identify a voter's ballot, including the order and time at which a voter uses the voting system. **Discussion**	BMD, PCOS, Security, TDP

Key	Summary	Description	Component/s
		Information such as the time the voter arrived at the polls or the specific vote-capture device used by the voter may be used to link a voter with their specific ballot and violates the principle of ballot secrecy.	
SMTTVS-406	11.1-A – Logging activities and resource access	The voting system must log any access to, and activities performed on, the voting system, including: 1. timestamps for all log entries; 2. all failed and successful attempts to access the voting system; and 3. all events which change the access control system including policies, privileges, accounts, users, groups or roles, and authentication methods. **Discussion** In the event of an error or incident, the user access log can assist in narrowing down the reason for the incident or error. • Timestamped log entries will allow for easy auditing and review of access to the voting system. • Access control logging supports accountability of actions by identifying and authenticating users. • Groups are a collection of users that are assigned a specific set of permissions. Roles are an identity that is given specific permissions and can be assigned to a user. Any changes to the permissions assigned to groups and roles should be logged to identify updates to a user's privileges.	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-409	11.1-B – Voter information in log files	The voting system must not log any voter identifying information. **Discussion** The logging and storing of voter identifying information after a ballot is cast potentially violates voter privacy and ballot secrecy. Examples of voter identifying information include first name, last name, address, driver's license, and voter registration number. **Related requirements** 10.1-A – System use of voter information 10.2.4-B – Logging of ballot selections	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-418	11.1-C – Preserving log integrity	The voting system must prevent: 1. the logging capability from being disabled; 2. the log entries from being modified in an undetectable manner; and 3. The deletion of logs; with the exception of log rotation. **Discussion** This requirement promotes the integrity of the information logged by ensuring all activities are logged. Additionally, it prevents these abilities from being an option within the user interface. This requirement promotes the integrity of the information logged by ensuring all activities are not modifiable. The removal of logs is only appropriate for log rotation, which is when the stored logs are rotated out to create more space for continuous logging. The voting system should	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		be capable of rotating the event log data to manage log file growth. Log file rotation may involve regular (e.g., 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. Preserved log files may be compressed to save storage space.	
SMTTVS-419	11.1-D – On-demand access to logs	The voting system must provide administrators access to logs on demand, allowing for continuous monitoring and periodic review. **Discussion** Enabling administrators to export and review the logs is a useful feature. Continuous monitoring and review of access control logs gives the administrator the opportunity to analyze and make changes to permissions and privileges, and quickly identify issues.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-422	11.2.1-A – Ensuring authorized access	The voting system must allow only authorized users to access the voting system. **Discussion** Authorized users include voters, election officials, and election workers.	BMD, CCOS, EMP, Integration, PCOS, Security, TDP
SMTTVS-424	11.2.1-B – Modifying authorized user lists	The voting system must allow only an administrator to create or modify the list of authorized users. **Discussion** This requirement assists with ensuring only authorized users are given access to the voting system.	CCOS, EMP, PCOS, Security, TDP

<table>
<tr><th>Key</th><th>Summary</th><th>Description</th><th>Component/s</th></tr>
<tr><td>SMTTVS-425</td><td>11.2.1-C – Access control by voting stage</td><td>The voting system access control mechanisms must distinguish at least the following voting stages from Table 11-1:
1. Pre-voting
2. Activated
3. Suspended
4. Post-voting
Table 11-1 – Voting stage descriptions<table><tr><th>Stage</th><th>Description</th></tr><tr><td>Pre-voting</td><td>Loading, and configuring device software, maintenance, loading election-specific files, preparing for election day usage</td></tr><tr><td>Activated</td><td>Activating the ballot, printing, casting, spoiling the ballot</td></tr><tr><td>Suspended</td><td>Occurring when an election official suspends voting</td></tr><tr><td>Post-voting</td><td>Closing polls, tabulating votes, printing records</td></tr></table>Discussion
The groups or roles in 11.2-H (Table 11- 2) will be given specific permissions which can be affected by the voting stage (Table 11-1).</td><td>BMD, CCOS, EMP, PCOS, Security, TDP</td></tr>
</table>

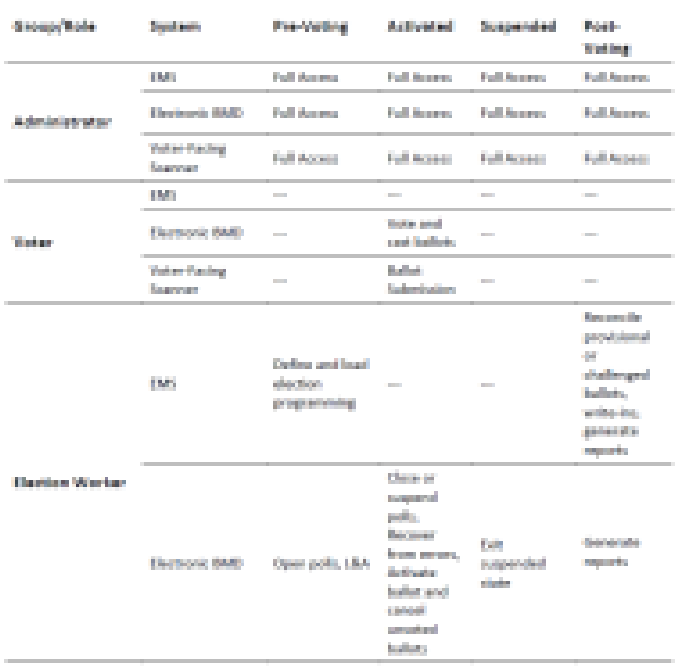
Key	Summary	Description	Component/s
SMTTVS-426	11.2.1-D – Access control configuration	The voting system must allow only an administrator to configure the permissions and functionality for each identity, group or role, or process to include account and group or role creation, modification, disablement, and deletion. **Discussion** For vote-capture devices, it is possible for each group or role to have (or not have) permissions for every voting stage. Additionally, the permissions that a group or role has for a voting stage can be restricted to certain functions. Table 11-3 shows an example matrix of group/role to system to voting state access rights; the table is not meant to include all activities. This requirement extends *[VVSG2005] I.7.2.1.1-a* by allowing configuration flexibility for permissions and functionality for each identity or group/role. Privileged accounts include any accounts within the operating system, voting device software, or other third-party software with elevated privileges such as administrator, root, and maintenance accounts. This requirement extends *[VVSG2005] I.7.2.1.2* by allowing the creation and disabling of privileged accounts. An administrator is the only user authorized to make major changes within a voting system. Administrators are given this group or role to ensure all other users have proper access to the information necessary to perform their duties.	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-428	11.2.1-E – Administrator modified permissions	The voting system must allow only an administrator to create or modify permissions assigned to specific groups or roles. **Discussion** The administrator's authority to create or modify permissions restricts users from gaining unauthorized permissions.	CCOS, EMP, PCOS, Security, TDP
SMTTVS-429	11.2.1-F – Authorized assigning groups or roles	The voting system must allow only an administrator to create or assign the groups or roles. **Discussion** Table 11-2 is a list of groups or roles that need to be included within the voting system. **Related requirements** 11.2.2-B – Minimum groups or roles	CCOS, EMP, PCOS, Security, TDP
SMTTVS-430	11.2.2-A – Role-based access control standard	Voting systems that implement role-based access control must support the recommendations for Core Role Based Access Control (RBAC) in the *ANSI INCITS 359-2004 American National Standard for Information Technology – Role Based Access Control [ANSI04]* document. **Discussion** This requirement extends *[VVSG2005] I. 7.2.1.1-a* by requiring role-based methods to follow *ANSI INCITS 359-2004 [ANSI04].*	CCOS, EMP, PCOS, Security, TDP

<table>
<tr><th>Key</th><th>Summary</th><th>Description</th><th>Component/s</th></tr>
<tr><td>SMTTVS-432</td><td>11.2.2-B – Minimum groups or roles</td><td>At minimum, voting systems that implement RBAC must define groups or roles with the role descriptions within Table 11-2.

Table 11-2 – Minimum voting system groups or roles for RBAC<table><tr><th>Group or role</th><th>Role description</th></tr><tr><td>Administrator</td><td>Can update and configure the voting devices and troubleshoots system problems.</td></tr><tr><td>Voter</td><td>A restricted process in the vote-capture device. It allows the vote-capture device to enter the activated state for voting activities.</td></tr><tr><td>Election Worker</td><td>Has the ability to open the polls, close the polls, recover from errors, and generate reports; Checks in voters and activates the ballot style; Loads ballot definition files.</td></tr></table>Discussion
Table 11-2 is a baseline list of groups or roles to be included in the voting system.</td><td>BMD, CCOS, EMP, PCOS, Security, TDP</td></tr>
<tr><td>SMTTVS-434</td><td>11.2.2-C – Minimum group or role permissions</td><td>At minimum, the voting system must use the groups or roles from Table 11-2 – Minimum voting system groups or roles for RBAC and the voting stages from Table 11-1 – Voting stage descriptions, to assign the minimum permissions in Table 11-3.
Discussion</td><td>BMD, CCOS, EMP, PCOS, Security, TDP</td></tr>
</table>

Key	Summary	Description	Component/s
		Table 11-3 – Minimum permissions for each group or role defines the minimum functions according to the user, voting stage, and system. Other capabilities can be defined as needed by jurisdiction. **Table 11-3 - Minimum permissions for each group or role**	

Key	Summary	Description	Component/s
		Table 11-3 - Minimum permissions for each group or role 	
SMTTVS-435	11.2.2-D – Applying permissions	The voting system must be capable of applying assigned groups or roles and permissions to authorized users. **Discussion**	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		Once the user is assigned a group or role, the voting system needs to be capable of making the necessary changes to the user's permissions. The permissions are changed based on the assigned group or role.	
SMTTVS-437	11.3.1-A – Access control mechanism application	The voting system must use access control mechanisms to permit authorized access or prevent unauthorized access to the voting system. **Discussion** Access controls support the following concepts: • limiting the actions of users, groups or roles, and processes to those that are authorized; • limiting entities to the functions for which they are authorized; • limiting entities to the data for which they are authorized; and • accountability of actions by identifying and authenticating users. Most modern operating systems natively provide configurable access control mechanisms that the voting system application can use.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-439	11.3.1-B – Multi-factor authentication for critical operations	At a minimum, the voting system must be capable of using multi-factor authentication to verify a user has authorized access to perform critical operations, including: 1. runtime software updates to the certified voting system; 2. aggregation and tabulation; 3. enabling network functions;	BMD, CCOS, EMP, Integration, Security, TDP

Key	Summary	Description	Component/s
		4. changing device states, including opening and closing the polls; 5. deleting or modifying the CVRs and ballot images; and 6. modifying authentication mechanisms. **Discussion** *NIST SP 800-63-3, Digital Identity Guidelines [NIST17c]* provides additional information useful in meeting this requirement. *NIST SP 800-63-3* defines multi-factor authentication (MFA) as follows: "An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are. Multifactor authenticators include, but are not limited to the following: • Username and password • Smartcard (for example, voter access card) • iButton • Biometric authentication (for example, fingerprint)	

Key	Summary	Description	Component/s
		Multi-factor authenticators can be tested for usability to ensure an appropriate balance of security, usability, and functionality. A significant impact to usability may require revision of the multi-factor authenticator implementation.	
SMTTVS-440	11.3.1-C – Multi-factor authentication for administrators	The voting system must authenticate the administrator with a multi-factor authentication mechanism. **Discussion** This requirement extends *[VVSG2005] I.7.2.1.2-e* by requiring multi-factor authentication for the voting system administrator group or role.	BMD, CCOS, EMP, Integration, Security, TDP
SMTTVS-441	11.3.2-A – Username and password management	If the voting system uses a username and password authentication method, the voting system must allow only the administrator to enforce password strength, histories, and expiration. **Discussion** This requirement extends *[VVSG2005] I.7.2.1.2-e* by requiring strong passwords, password histories, and password expiration.	EMP, Security, TDP
SMTTVS-442	11.3.2-B – Password complexity	The voting system must, at minimum, meet the password complexity requirements within the latest version of *NIST SP 800-63B Digital Identity Guidelines* standards. **Discussion** *NIST SP 800-63B [NIST17d]* does not specify any additional password complexity requirements besides password length. At the time of this writing, the only recommended password complexity requirement is a minimum password length of 8	CCOS, EMP, Security, TDP

Key	Summary	Description	Component/s
		characters. *NIST SP 800-63B* also recommends that if a password is provided to the user, it may be six characters and all numeric. NIST's password complexity recommendations are meant to make it easier for users to memorize their passwords, while decreasing user frustration.	
SMTTVS-444	11.3.2-C – Secure storage of authentication data	The voting system must store authentication data in a way that ensures confidentiality and integrity are preserved. **Discussion** Ensuring the confidentiality of stored authentication data (such as passwords) may involve the use of cryptography. The best practice at the time of this writing is to store a salted, one-way hash of passwords. Additional guidance for protecting authentication data can be found in *NIST SP 800-63B, Digital Identity Guidelines [NIST17d].*	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-445	11.3.2-D – Password disallow list	The voting system must compare all passwords against a manufacturer-specified list of well-known weak passwords and disallow the use of these weak passwords. **Discussion** Examples of common weak passwords include 0000, 1111, 1234.	EMP, Security, TDP
SMTTVS-446	11.3.2-E – Usernames within passwords	The voting system must ensure that the username is not used in the password. **Discussion** This requirement extends security by restricting the use of usernames and related information in passwords.	EMP, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-447	11.4-A – Least privilege for access policies	By default, the voting system must implement the principle of least privilege including denying access to functions and data unless explicitly permitted. **Discussion** This requirement extends *[VVSG2005] I.7.2.1.2-a* by requiring explicit authorization of subjects based on access control policies. At the time of this writing, *NIST SP 800-12 [NIST17e]* defines "least privilege" as "the principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function." Network access will also follow the principle of least privilege to ensure that devices only receive as much access as is necessary to perform the desired function.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-449	11.4-B – Separation of duties	Voting system documentation must include suggested practices for dispersing critical operations across multiple groups or roles. **Discussion** Guidance for implementing separation of duties within the voting system is imperative to implement the separation of duties principle. Separation of duties is meant to divide user functions and roles so that there is no conflict of interest.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-453	11.5-A – Session time limits	The voting system must enable an administrator the ability to do the following: 1. set the maximum time limit for a user's session, and 2. set the maximum time limit for user inactivity.	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		Discussion *NIST SP 800-63B [NIST17d]* recommends a max session time of 12 hours regardless of inactivity and a max inactivity time of 30 minutes. Elections consist of temporary employees and user access may only be required during an election. A user's access may expire and terminate automatically at the end of an election.	
SMTTVS-454	11.5-B – Reauthentication	The voting system must require reauthentication of an authorized user after the administrator-specified time limit for the user's session or for user inactivity. **Discussion** After authentication, a user's access to a voting system will time-out after a specified period of time. This will avoid unauthorized access to the voting system by unauthorized users. Once a user's access has timed-out, the user will have to re-authenticate to continue using the voting system. For voters, session times are specified under requirement *7.2-O – Inactivity alerts*. For more information, see *NIST SP 800-63B [NIST17d]*.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-455	11.5-C – Account lockout	The voting system must lockout roles or individuals after an administrator-specified number of consecutive failed authentications attempts. **Discussion** This requirement prevents certain classes of password guessing attacks. This requirement can be implemented using a technique such as exponential backoff. *NIST SP800-63B* recommends allowing 5-10 attempts before starting exponential backoff.	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		Exponential backoff requires that after each unsuccessful authentication attempt, the time period before another authentication attempt can be made grows exponentially. For instance: • The wait after 1 unsuccessful authentication attempt is 0 seconds • The wait after 2 unsuccessful attempts is 2 seconds • The wait after 3 unsuccessful attempts is 4 seconds, and so on	
SMTTVS-456	11.5-D – Lockout time duration	The voting system must allow only an administrator to define the lockout duration. **Discussion** This requirement extends *[VVSG2005] I.7.2.1.2* by allowing the administrator flexibility in configuring the account lockout policy. The lockout policy should not lockout voters.	CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-174	12.1-A – Unauthorized physical access	Any unauthorized physical access to voting systems must leave physical evidence that an unauthorized event has taken place. **Discussion** Access points such as covers and panels need to be secured by locks or other mechanisms that leave physical evidence in case of tampering or unauthorized access. Manufacturers can provide for and recommend a combination of procedures and	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		physical measures that allow election officials to differentiate authorized from unauthorized access during all modes of operation, such as a system that relies on tamper evident tape, seals, or tags coded with consecutive serial numbers. Other systems might use seals incorporating radio frequency identification devices with physically unclonable functions or other technology in the future. This requirement extends [VVSG2005] I.7.3.1 by requiring that any tampering with a device leave physical evidence. [VVSG2005] I.7.3.1 states that any tampering should be detectable using manufacturer-specified procedures and measures.	
SMTTVS-175	12.1-B – Unauthorized physical access alert	Voter-facing scanners and electronic BMDs must produce an alert if access to a restricted voting device component is detected during the activated voting stage. **Discussion** This alert is meant to call attention to election workers in the polling place. More information about the activated stage is defined in Table 11-1. **Related requirements** 11.2.1-C – Access control by voting stage	BMD, PCOS, Security, TDP
SMTTVS-176	12.1-C – Disconnecting a physical device	Voter-facing scanners and electronic BMDs must produce an alert if a connected component is physically disconnected during the activated voting stage. **Discussion** An alert can be provided in the form of an alarm to provide an audible and/or visual alert. Examples of connected components include printers, removable storage	BMD, PCOS, Security, TDP

Key	Summary	Description	Component/s
		devices, and mechanisms used for networking. If a token is necessary for normal operation, such as a memory card or other device granting a voter access to the voting system, it is not necessary to trigger the alert. More information on the activated stage is defined in Table 11-1.	
SMTTVS-177	12.1-D – Logging of physical connections and disconnections	The voting system must log when a voter-facing scanner, electronic BMD, or other component is connected or disconnected during the activated voting stage. **Discussion** Logging of the devices is vital for determining cause and providing incident information if a physical security event occurs. **Related requirements** 11.2.1-C – Access control by voting stage 15.1-D – Logging event types	BMD, CCOS, PCOS, Security, TDP
SMTTVS-178	12.1-E – Secure containers	Unauthorized physical access to a container that stores or transports voting system records must result in physical evidence that an unauthorized event has taken place. **Discussion** The goal is to ensure that election workers or observers would easily notice if someone has tampered with the container. This requirement can be achieved through locks or seals as a part of tamper evidence and tamper resistance countermeasures described by the use procedures and supplied by the manufacturer.	BMD, CCOS, PCOS, Security, TDP

Key	Summary	Description	Component/s
		Additionally, to support the requirements in *Principle 9-Auditable*, containers which hold either paper or electronic voting system records needed for audits need to be secure against physical access. An example of a physical container includes ballot boxes integrated and sold as part of the voting system. **Applies to:** Voter-facing scanners, BMDs	
SMTTVS-179	12.1-F – Secure locking systems	If the voting system uses locks, it must support locking systems for securing voting devices that are flexible enough to support different keying schemes, including a scheme that can make use of keys that are unique to each owner. **Discussion** A lock used on the voting system can be evaluated against UL437 door locks and locking cylinders requirements. See [UL13] for UL listing for door locks and locking cylinders within the standard to review requirements for lockpicking and the attack resistance tests. The use of a single key used to unlock thousands of precinct-based voting devices makes for a challenging security situation, as copies of this single key design are distributed to a large number of individuals. This creates a situation in which the key can be easily lost or stolen, and subsequently copied. At the same time, this situation does make key management significantly easier for election officials. To alleviate this situation, election officials might want keying schemes that are more or less restrictive in accordance with their election management practices and needs. This system can	BMD, PCOS, Security, TDP

Key	Summary	Description	Component/s
		make use of replicable locks or cylinders, mechanisms which allow for rekeying of locks, or other technologies. The requirement does not mandate a unique key for each piece of voting equipment but requires manufacturers to be able to provide unique keys for the voting equipment if requested by election officials. System owners need to establish procedures for issues such as key reproduction, use, and storage.	
SMTTVS-180	12.1-G – Backup power for power-reliant countermeasures	If the voting system uses a powered physical security countermeasure, that physical countermeasure must maintain its state when power is removed and must have a backup power supply. In addition, switching from primary power supply to backup power supply: 1. produces an alert; 2. happens automatically when primary power is unavailable; and 3. generates an event log entry, if possible. **Discussion** This ensures that the countermeasure isn't disabled or intentionally circumvented by a power failure. Switching to the backup power supply triggers an alarm that alerts an election worker to the issue so that any problem can be further diagnosed and eventually resolved. The alarm can be visible and audible. Once primary power is unavailable, the switch to back up power should be automatic to avoid any gaps in functionality if the switch must be done manually.	CCOS, Integration, PCOS, Security, TDP

Key	Summary	Description	Component/s
		If the physical countermeasure leverages the voting system's operating system, it can create an event log entry when it is switched to backup power. The log entry information is security relevant, especially once a security incident has occurred, and would be useful when determining cause. Alternatively, the voting system should log when there is a switch from backup power to the primary power supply.	
SMTTVS-181	12.2-A – Physical port and access least functionality	The voting system must only expose physical ports and access points that are essential to voting operations, testing, and auditing. **Discussion** Examples of ports are USB and RJ45 physical network interfaces. Examples of access points are doors, and panels, and vents. Voting operations include voting device upgrades and maintenance.	BMD, CCOS, PCOS, Security, TDP
SMTTVS-182	12.2-B – Physical port auto-disable	If a physical connection that supports digital communication between voting system components is broken during an activated or suspended state, the affected voting system port must be automatically disabled. **Discussion** Automatically disabling will require an election worker's attention to re-enable and re-attach any cabling. This remediation is required for continuity and to address any tampering. An added feature could be that the specific election worker performing maintenance is uniquely identified within the logs, but this is not required. This	BMD, CCOS, PCOS, Security, TDP

Key	Summary	Description	Component/s
		requirement does not include power cabling with a backup power supply or analog accessibility device ports that are used during the activated voting stage.	
SMTTVS-183	12.2-C - Physical port restriction	Voting systems must restrict physical access to voting system ports that accommodate removable media, with the exception of ports used to activate a voting session. **Discussion** Physical port access needs to be restricted when not in use. This requirement is not meant to impede the use of accessible technology. This requirement assists in restricting adversaries from adding wireless adapters or other malicious adapters to the voting system. Although voting systems can have ports dedicated to voting operations outside of election day activities, those ports need not be exposed while balloting is in progress. Removable media (such as Floppy, CD or DVD drives, thumb drives, and memory cards) might be essential to voting operations during pre-voting and post-voting phases of the voting cycle, such as machine upgrade, maintenance, and testing. Therefore, all removable media should be accessible only to authorized personnel. They should not be accessible to voters during activated and suspended phases of the voting cycle. It is essential that any removable drives, whether or not they are used by the system, are not accessed without detection.	BMD, CCOS, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-184	12.2-D – Disabling ports	Voting systems must allow authorized administrators to logically put physical ports into a disabled state. **Discussion** Logically disabling ports prevents unused ports from being used as a staging point for an attack on the voting system.	CCOS, EMP, PCOS, Security, TDP
SMTTVS-185	12.2-E – Logging enabled and disabled ports	An event log entry that identifies the name of the affected device must be generated when physical ports are enabled or disabled. **Discussion** Whether a port is disabled or not is security relevant, especially once a security incident has occurred, and this information would be useful when determining cause. *12.2-C – Physical port restriction* applies to physical restrictions, whereas *12.2-D – Disabling ports* discusses logical disabling of ports.	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-373	13.1.1-A – Authentication to access configuration file	The voting system must allow only authenticated system administrators to access and modify voting device configuration files. **Discussion** Voting system configuration files can include operating system and voting system application configuration files. These files can have a large impact on how the voting	CCOS, EMP, Integration, PCOS, Security, TDP

Key	Summary	Description	Component/s
		system functions and what election logic is being used. Therefore, accidental or malicious modification can have a large impact on the system and access to these files should be restricted to authorized individuals.	
SMTTVS-374	13.1.1-B – Authentication to access configuration file on EMS	The EMS must uniquely authenticate individuals associated with the role of system administrator before allowing them to access and modify EMS configuration files. **Discussion** EMS configuration files can include operating system and voting system application configuration files. These files can have a large impact on how an EMS tabulates and reports election results. Therefore, accidental or malicious modification can have a large impact on the system and access to these files should be restricted to authorized individuals.	EMP, Integration, Security, TDP
SMTTVS-375	13.1.1-C – Authentication to access configuration file for network appliances	Network appliances must uniquely authenticate individuals before allowing them to access and modify configuration files. **Discussion** Network appliances, such as firewalls, routers, switches, and VPN gateways are generally configurable. Individually authenticating users to the device, in lieu of using a shared password, is a standard practice for restricting access to these devices.	EMP, Security, TDP
SMTTVS-376	13.1.2-A – Integrity	The voting system integrity must prevent modification of CVRs and ballot images when they are stored anywhere within the voting system.	CCOS, Security, TDP

Key	Summary	Description	Component/s
	protection for election records	**Discussion** Applying access control can help prevent any unauthorized modifications to CVRs and ballot images. Applying integrity protection ensures that any unauthorized modifications to CVRs and ballot images can be detected. For example, ballot images can be integrity protected using a private key maintained in a Hardware Security Module and a cryptographic signature of the image.	
SMTTVS-378	13.2-A – Signing stored election records	Cast vote records and ballot images must be digitally signed when stored and before being transmitted. **Discussion** Digital signatures address the threat that the records might be tampered with when stored or transmitted. Cryptographic hashes do not sufficiently mitigate this threat, as election records could be altered and then re-hashed. Digital signatures also allow verification of the source of any created or modified records. Additional information can be found in *FIPS 186-4 Digital Signature Standard [NIST13c]*.	CCOS, EMP, Integration, Security, TDP
SMTTVS-379	13.2-B – Verification of election records	A voting system must: 1. cryptographically verify the integrity and authenticity of all election data received; 2. immediately log any verification error of received election results;	BMD, CCOS, EMP, Integration, Security, TDP

Key	Summary	Description	Component/s
		3. immediately present on-screen any verification errors; and 4. not tabulate or aggregate any data that fails verification. **Discussion** This process of verifying election data and results is a defense in depth measure against accidental errors or a malicious incident regarding modified or false election records. For example, checking the cryptographic integrity of received election results prevents modified election results from being maliciously modified and reported on election night.	
SMTTVS-381	13.3-A – Cryptographic module validation	Cryptographic functionality must be implemented in a cryptographic module that meets current FIPS 140 validation, operating in FIPS mode. This applies to: 1. software cryptographic modules, and 2. hardware cryptographic modules. **Discussion** Use of cryptographic modules validated at level 1 or above ensures that the cryptographic algorithms used are secure and correctly implemented. The current version of *FIPS 140[NIST01, NIST19a]* and information about the *NIST Cryptographic Module Validation Program* are available under *[NIST20e]* in Appendix C: References. Note that a voting device can use more than one cryptographic module,	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		and quite commonly can use a software module for some functions and a hardware module for other functions.	
SMTTVS-383	13.3-C – Cryptographic strength	Devices using cryptography must employ NIST approved algorithms with a security strength of at least 112-bits. **Discussion** At the time of this writing, NIST specifies the security strength of algorithms in SP 800- 57, Part 1 *[NIST20a].* 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. The specified strength should be sufficient for several decades. This requirement is not intended to forbid all incidental use of non-approved algorithms by OS software or standardized network security protocols.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-384	13.3-D – MAC cryptographic strength	The key used with Message Authentication Codes must also have a security strength of at least 112 bits and use a 96-bit tag length. **Discussion** Message authentication codes of 96-bits are conventional in standardized secure communications protocols, and acceptable to protect voting records and systems.	CCOS, EMP, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-385	13.3-E – Cryptographic key management documentation	The voting system documentation must describe how key management is to be performed. **Discussion** This document provides procedural steps that can be taken to ease the burden of key management and safely perform these operations.	Security, TDP
SMTTVS-387	13.4-A – Confidentiality and integrity protection of transmitted data	The voting system must: 1. mutually authenticate all network connections; 2. cryptographically protect the confidentiality of all data sent over a network; and 3. cryptographically protect the integrity of all election data sent over the network. **Discussion** Mutual authentication provides assurance that each electronic device is legitimate. Mutual authentication can be performed using various protocols, such as IPsec and SSL/TLS. Only wired local area network (LAN) communication, such as ethernet, is possible for *VVSG 2.0* voting systems. This requirement includes network appliances such as switches, firewalls, and routers within its scope.	CCOS, EMP, Security, TDP

Key	Summary	Description	Component/s
		This does not prevent the use of “double encrypted” connections employing cryptography at multiple layers of the network stack. Data, such as ballot images, must be encrypted before transmission. Integrity protection ensures that any inadvertent or intentional alterations to data are detected by the recipient. Integrity protection for data in transit can be provided through the use of various protocols, such as IPsec VPNs and SSL/TLS. For more information about TLS implementations, see *NIST SP 800-52 rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations [NIST19b].*	

Key	Summary	Description	Component/s
SMTTVS-137	14.1-A – Risk assessment documentation	The voting system’s documentation must contain a risk assessment **Discussion** Risk assessments are a foundation of effective risk management. Additionally, they help to facilitate decision making at the organization, business process, and information system levels. Some decisions may include prioritizing the mitigation or prevention of high risks that are likely to have a high impact an election. Many methods of conducting risk assessments exist, including *NIST SP 800-30-1: Guide for Conducting Risk*	Security, TDP

Key	Summary	Description	Component/s
		Assessments [NIST12] or ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management [ISO18d].	
SMTTVS-138	14.1-B – Addressing and accepting risk	The voting system's risk assessment documentation must provide technical controls or a notation showing the acceptance of risk for each documented threat to voting system integrity. **Discussion** Assigning controls or accepting risk is a key part of the risk assessment process. This requirement assists in providing the evidence that a manufacturer has gone through the risk determination process. *NIST SP 800-53* revision 5 *Security and Privacy Controls for Information Systems and Organizations [NIST20h]* can be useful to identify controls that can assist with addressing any identified threats.	Security, TDP
SMTTVS-139	14.1-C – System security architecture description	The voting system's risk assessment documentation must describe how physical, technical, and operational controls work together to prevent, mitigate, and respond to attacks on the voting system. This includes the use of: 1. cryptography, 2. malware protection, 3. firewall access control lists, rules, and configurations, and 4. system configurations. **Discussion** Risk assessments can be large, complicated documents. This requirement ensures that a	Security, TDP

Key	Summary	Description	Component/s
		single narrative exists to explain to election officials and other system owners how the overall security operates for the voting system. **Related requirements** 3.1.3-C – Physical security	
SMTTVS-140	14.1-D – Procedural and operational security	The voting system must document necessary procedural and operational processes that need to occur to ensure integrity of the system. **Discussion** Procedural and operational security processes play a key role in overall system security. If any of these procedures are necessary to ensure system integrity or system security, these practices need to be well documented and explained.	Integration, Security, TDP
SMTTVS-141	14.2-A – Non-essential networking interfaces	The voting system must disable networking and other features that are non-essential to the function of the voting system by default. **Discussion** When the voting system is booted, networking and other functions are prohibited from running. For instance, networking interfaces such as Wi-Fi and Bluetooth should be disabled. By disabling features that are non-essential to the voting system, this decreases the attack surface by limiting the functionality and decreasing the entry points that may be accessed by unauthorized users.	CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-142	14.2-B – Network status indicator	If a voting system has network functionality, the voting system application must visually show an indicator within the management interface when networking functionality is enabled and disabled. **Discussion** This helps to ensure that network functionality is not enabled by accident.	CCOS, EMP, Security, TDP
SMTTVS-143	14.2-C – Wireless communication restrictions	Voting systems must not be capable of establishing wireless connections as provided in this section. **Discussion** Wireless connections can expand the attack surface of the voting system by opening it up to over-the-air attacks. Over-the-air access can allow for adversaries to attack remotely without physical access to the voting system. Disallowing wireless capabilities in the voting system limits the attack surface and restricts any network connections to be hardwired. Examples of how wireless can be disabled may include the following: • a system configuration process that disables wireless networking devices, • disconnecting/unplugging wireless device antennas, or • removing wireless hardware within the voting system. This requirement does not prohibit wireless hardware within the voting system so long as the hardware cannot be used, e.g. no wireless drivers present. This requirement applies solely to voting systems that are within the scope of the VVSG. It is not a prohibition on wireless technology within election systems overall. This	CCOS, PCOS, Security, TDP

Key	Summary	Description	Component/s
		requirement does not impact or restrict the use of assistive technology (AT) within the polling place. Voters with wireless AT may have to use an adapter that leverages the 3.5 mm headphone jack. **Related requirements** 15.4-C – Documentation for disabled wireless 8.1-E – Standard audio connectors	
SMTTVS-144	14.2-D – Wireless network status indicator	If a voting system has network functionality, the voting system application must visually show an indicator within the management interface to confirm that wireless networking functionality is disabled. **Discussion** Note that this is in addition to the networking identifier. Wireless is a significant avenue for system compromise. This indicator ensures that wireless functionality is not enabled by accident.	CCOS, Security, TDP
SMTTVS-145	14.2-E – External network restrictions	A voting system must not be configured to: 1. establish a connection to an external network, or 2. connect to any device external to the voting system. **Discussion** The basic instructions provided by a vendor should clearly indicate that the intended use and installation of voting systems implements an air gap between the voting system and external networks or external devices. This requirement is intended to limit the voting	CCOS, EMP, Security, TDP

Key	Summary	Description	Component/s
		systems attack surface and disallow connections of the voting system to technologies such as: • e-pollbooks, • public switched telephone networks (PSTNs), and • cellular modems. In particular, connections to the internet expand the attack surface even further than other wireless technologies because the data traverses over the internet, which reaches all over the world. This type of access allows a malicious actor to attack from various distances, meaning they do not have to be in close proximity of a polling place or near a specific jurisdiction. Exposure to the internet could allow nation-state attackers to gain remote access to the voting system. With remote access an attacker may be able to view all files within a voting system and make modifications to files within the voting system. These files may include election results and ballot records. This type of exposure could also make voting systems vulnerable to ransomware. Ransomware is a type of malware that could deny access to election data or functionality, usually by encrypting the data with a key known only to the hacker who deployed the malware. Ultimately an attacker could render a voting system non-operational until a ransom is paid. **Related requirements** 15.4-B – Secure configuration documentation	

Key	Summary	Description	Component/s
SMTTVS-146	14.2-F – Secure configuration and hardening documentation	The voting system must follow a secure configuration guide for all underlying operating systems and other voting system components, with any deviations from the secure configuration guidance documented and justified. **Discussion** Properly configuring an operating system is a difficult and complex task, with small settings potentially causing a large impact. Industry, NIST, and various agencies within the DoD offer guidance for specific operating systems, as do OS and component manufacturers. Some examples include Security Technical Implementation Guides (STIGs) *[__DISA20]* and the Center for Internet Security (CIS) benchmarks. Documenting deviations ensures that important settings are not overlooked and decisions to deviate are properly considered. **Related requirements** 15.4-B – Secure network configuration documentation	Integration, Security, TDP
SMTTVS-147	14.2-G – Unused code	The voting system software must not contain unused or dead code. **Discussion** An attacker may be able to take advantage of the unused code and introduce software bugs/exploits that can be used to make the voting system vulnerable. Dead code is source code that can never be executed in a running program because the surrounding code makes it impossible for a section of code to ever be executed.	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		See *MITRE CWE-561 [MITRE20]*. Software with dead code is considered poor quality and reduces maintainability. This requirement does not restrict the use of defensive code, such as exception handling to prevent failures because this code is still traversed to check conditions.	
SMTTVS-148	14.2-H – Use of exploit mitigation technologies	The voting system must use exploit mitigation technologies including data execution prevention (DEP) and address space layout randomization (ASLR), or equivalent mitigations. **Discussion** DEP and ASLR are commonplace exploit mitigation technologies that can help prevent a variety of vulnerability types, including memory corruption errors like buffer overflows. If the voting system does not use DEP and ASLR, the equivalent mitigation technologies used must be identified. Applications need to be written and compiled in such a way as to make use of underlying exploit mitigation technologies. See the *OWASP Application Security Verification Standard [OWASP19]* for more information about exploit mitigation.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-149	14.2-I – Importing software libraries	The voting system software must import only library components that are necessary. **Discussion** Importing entire software libraries significantly increases the attack surface of the software. Importing only the components of a library, such as modules, functions, or	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		classes needed is a useful attack surface minimization strategy. Following the language's intended import design, such as importing only the specific module needed from a more general "standard" library, will also help with this goal. This requirement is not intended to encourage developers to avoid the import process by copying code directly to software, which would greatly complicate the update process. Not all 3rd party libraries are easily modifiable, making this attack surface reduction strategy impractical.	
SMTTVS-150	14.2-J – Vulnerability management plan	The voting system documentation must include the plan for how to address vulnerabilities found in the voting system and at minimum include the following: 1. how the voting system design process identifies and addresses well-known vulnerabilities; 2. disclosure of all known vulnerabilities within the system, 3. a patch management plan; and 4. the method to receive and send reports of vulnerabilities. **Discussion** This requirement informs how a voting system vendor is able to manage verified vulnerabilities to their voting system. Certain information can also be included for each vulnerability, such as any severity, impact, or exploitability scores. Tools like the Common Vulnerability Scoring System	Security, TDP

Key	Summary	Description	Component/s
		(CVSS) can be used to communicate the metrics (including the severity) of software vulnerabilities. For more information about vulnerability and patch management, see *NISTIR 8011 Volume 4, Automation Support for Security Control Assessments: Software Vulnerability Management [NIST20c]* and *NIST SP 800-40, Guide to Enterprise Patch Management Technologies [NIST13b].* *[NISTIR 8011 Vol. 4, Automation Support for Security Control Assessments: VUL | CSRC|https://csrc.nist.gov/publications/detail/nistir/8011/vol-4/final]* *[SP 800-40 Rev. 3, Guide to Enterprise Patch Management Technologies | CSRC|https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final]*	
SMTTVS-151	14.2-K – Known vulnerabilities	The underlying voting system platform must be free of well-known vulnerabilities as identified in the vulnerability management plan. **Discussion** Vulnerability scanning tools can be used to identify known vulnerabilities in software and firmware. *The U.S. National Vulnerability Database (NVD)* is one resource that can be useful for identifying known vulnerabilities. Other vulnerability databases also exist and can be leveraged for full vulnerability coverage that might not be identified by automated scanning tools.	BMD, CCOS, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-152	14.3-A – Supply chain risk management strategy	The voting system's documentation must contain a supply chain risk management strategy that at minimum includes the following: 1. a reference to the template or standard used, if any, to develop the supply chain risk management strategy; 2. the assurance requirements to mitigate supply chain risks; 3. the contract language that requires suppliers and partners to provide the appropriate information to meet the assurance requirements of the supply chain risk management strategy; 4. the plan for reviewing and auditing suppliers and partners; and 5. the response and recovery plan for a supply chain risk incident. **Discussion** Supply chain risks may include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the technology supply chain. These risks are associated with an organization's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. These risks can be managed by…	Security, TDP

Key	Summary	Description	Component/s
		• following *Appendix E* of *NIST SP 800-161 – Supply Chain Risk Management Practices [NIST15b] for Federal Information Systems and Organizations* guidance (Appendix E provides a supply chain management plan (strategy template). • utilizing the *NIST Cybersecurity Framework Version 1.1 [NIST18c]* by referencing the Supply Chain Risk Management category and subcategory, and • referencing the relevant security controls for supply chain in *NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations [NIST20b].* Contract language provided must include the products or services acquired from the suppliers/partners and any evidence or artifacts that attest to the required level of assurance.	
SMTTVS-153	14.3-B – Criticality analysis	The voting system's documentation must include a list of critical components and suppliers defined by a criticality analysis and supplier impact analysis. **Discussion** Defining the critical components and supplier of the voting system can assist in prioritizing their importance to the voting process and identifying the impact to security, privacy and performance for failure or compromise. This can be supplemented by following *NISTIR 8179 Criticality Analysis Process Model - Prioritizing Systems and Components [NIST18b]* and *NISTIR 8272, Impact Analysis Tool for Interdependent Cyber Supply Chain Risks [NIST20d].*	CCOS, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-154	14.3-C – Bill of materials	The voting system's documentation must include the hardware and software information for the critical components defined in the *14.3-B* and at minimum list the following information for each component: 1. component name; 2. manufacturer; 3. model or version; and 4. applicable platform for software (e.g., Windows or Linux). **Discussion** This requirement will use the critical components defined in the critical analysis of *14.3-B – Criticality analysis*. At minimum the bill of materials for critical components are required, but this does not restrict the voting system vendor from listing the bill of materials for other components. This is a common practice when providing a hardware bill of materials. It is not as common to produce a bill of materials for software and as standards/best practices are developed, they should be considered for inclusion in the software bill of materials. For more information about the risks of third-party components and developing software bills of materials, see *"Managing Security Risks Inherent in the Use of Third-party Components" [SAFECode19]* and resources from the *National Telecommunications and Information Administration about Software Bills of Materials [NTIA19].*	Security, TDP

Key	Summary	Description	Component/s
SMTTVS-155	14.3.1-A – Cryptographic boot verification	The voting system must cryptographically verify firmware and software integrity before the operating system is loaded into memory. **Discussion** This requirement does not mandate hardware support for cryptographic verification. This requirement could be met by trusted boot, but other software-based solutions exist. This includes a software bootloader cryptographically verifying the OS prior to execution. Verifying the bootloader itself is excluded from this requirement, but not prohibited. **Applies to:** Vote-capture and tabulation device, EMS	BMD, CCOS, EMP, Integration, PCOS, Security, TDP
SMTTVS-156	14.3.1-B – Preventing of boot on error	If the voting system fails boot validation, the voting system must not boot and provide an onscreen alert. **Discussion** System users need to be notified when the voting system is either corrupted or has been maliciously modified. Boot validation prevents unauthorized operating systems and software from being installed or run on a system. **Applies to:** Vote-capture and tabulation device, EMS	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-157	14.3.1-C – Notification of boot validation failure	If the voting system does not pass boot validation, it must present an on-screen alert and provide any other necessary information to understand the failure. **Discussion** Failure of boot validation needs to be provided to users so these errors can be further analyzed when needed. If the voting system is capable of pre-boot logging, failure information could be stored in a log for future analysis. **Applies to:** Vote-capture and tabulation device, EMS **Related requirements** 14.3.2 – Software integrity	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-158	14.3.2-A – Installing software	The voting system must only allow digitally signed software and firmware to be installed. **Discussion** Signed software and firmware ensures that it is not modified before installation, and that it is being distributed by the proper entity.	BMD, CCOS, EMP, Integration, PCOS, Security, TDP
SMTTVS-159	14.3.2-B – Software verification for installation	The voting system must cryptographically verify the digital signature of software and firmware before it is installed. **Discussion** The security properties of integrity and authenticity are not achieved unless the digital signature for the signed software and firmware is cryptographically verified.	BMD, CCOS, EMP, Integration, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-160	14.3.2-C – Application allowlisting	The voting system must only run applications that have been verified against an allowlist. **Discussion** This requirement helps ensure only authorized applications run on the voting system. **Applies to:** Vote-capture device	BMD, CCOS, Integration, PCOS, Security, TDP
SMTTVS-161	14.3.2-D – Integrity protection for software allowlists	The voting system must protect the integrity and authenticity of the allowlist configuration files. **Discussion** If the allowlist is improperly modified, the software allowlisting mitigation can be defeated. The most common way of providing allowlist configuration file protection could be a digital signature.	BMD, CCOS, EMP, Integration, PCOS, Security, TDP
SMTTVS-162	14.4-A – Authenticated operating system updates	The voting system must authenticate administrators before an operating system update is performed. **Discussion** Administrators are required to be authenticated before they can update the voting system, regardless of whether the updated done by a networked method or performed using physical media. **Related requirements** 11.3.1-B – Multi-factor authentication for critical operations	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		11.3.1-C – Multi-factor authentication for administrators	
SMTTVS-163	14.4-B – Authenticated application updates	The voting system must authenticate administrators before a software update to the voting system application and related software. **Discussion** Administrators are required to be authenticated before they can update the voting system, whether the update is applied by a network method or physical media. **Related requirements** 11.3.1-B – Multi-factor authentication for critical operations 11.3.1-C – Multi-factor authentication for administrators	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-164	14.4-C – Authenticated firmware updates	The voting system must authenticate administrators before a firmware or driver update. **Discussion** Administrators are required to be authenticated before they can update the voting system, regardless if network enabled update is performed or via physical media. **Related requirements** 11.3.1-B – Multi-factor authentication for critical operations 11.3.1-C – Multi-factor authentication for administrators	BMD, CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-458	15.1-A – Event logging	The voting system must be capable of logging events that occur in a voting system. **Discussion** The ability to log events within a system allows for continuous monitoring of the voting system. These logs provide a way for administrators to analyze the voting system's activities, diagnose issues, and perform necessary recovery and remediation actions.	BMD, CCOS, EMP, PCOS, Security
SMTTVS-459	15.1-B – Exporting logs	The voting system must be capable of exporting logs. **Discussion** Exporting logs offers the opportunity for external review, clearing storage, and a method to compare with future logs.	BMD, CCOS, EMP, Integration, PCOS
SMTTVS-460	15.1-C – Logging voter information	The voting system must not log any information: 1. identifying a specific voter, and 2. connecting a voter to a specific ballot. **Discussion** No voter information is stored anywhere within voting system logs. This would violate voter ballot secrecy because it can link a voter to their ballot selections.	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-461	15.1-D – Logging event types	At minimum, the voting system must log the events included in Table 15-1. **Discussion** *Table 15-1 – System events to log* provides a list of events that will be included in the voting system event logs. The voting system is not limited to the events in the table.	BMD, CCOS, EMP, PCOS

<table>
<tr><th>Key</th><th>Summary</th><th>Description</th><th>Component/s</th></tr>
<tr><td></td><td></td><td>Logging system events provides insight into general system metrics, errors, and vulnerabilities. Information gathered from logs can be used to improve system performance by preventing future errors/issues or automate issue handling.

Table 15-1:
<table><tr><th>System Event</th><th>Description</th></tr><tr><td>General system functions</td><td></td></tr><tr><td>Device generated error and exception messages</td><td>Includes but is 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.</td></tr></table></td><td></td></tr>
</table>

Key	Summary	Description		Component/s
			· All faults and the recovery actions taken. Device generated error and exception messages such as ordinary timer system interrupts and normal I/O system interrupts do not need to be logged.	
		Critical system status messages	Critical system status messages other than information messages displayed by the device during the course of normal operations. Includes but is 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 scanner and communications equipment operation · Printer errors · Detection or remediation of malware or other malicious software · Cryptographic boot validation success/failure	

Key	Summary	Description		Component/s
		Non-critical status messages	Non-critical status messages that are generated by the device'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.	
		Device shutdown and restarts	Both normal and abnormal device shutdowns and restarts.	
		Changes to system configuration settings	Configuration settings include but are not limited to registry keys, kernel settings, logging settings, and other voting device configuration settings.	
		Integrity checks for executables, configuration files, data, and logs	Integrity checks that can indicate possible tampering with files and data.	
		The addition and deletion of files	Files that are added or deleted from the voting device.	
		System readiness results	Includes but is not limited to: · System pass or fail of hardware and software test for system readiness · Identification of the software release, identification	

Key	Summary	Description		Component/s
			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	
		Removable media events	Removable media that is inserted into or removed from the voting device.	
		Backup and restore	Successful and failed attempts to perform backups and restores.	
SMTTVS-462	15.1-E – Configuration file access log	When a system administrator is accessing a configuration file, the voting system must log identifying information of the group or role accessing that file. **Discussion** A record of who modified a configuration file is important for auditing and accountability. The identifying information could include the username or the name of the user for improved traceability.		CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-464	15.2-A – Presentation of voting application errors	The voting system must provide immediate notification to the user when a voting application error occurs. **Discussion** Voting application errors can disrupt a voter's voting session. Immediate notification of an issue or an error allows for prompt recovery and remediation.	BMD, CCOS, PCOS, Security, TDP
SMTTVS-465	15.2-B – Voting application error handling documentation	The voting system documentation must include procedures for handling voting application errors. **Discussion** Documentation will assist election officials with steps to properly address errors.	CCOS, EMP, PCOS, Security, TDP
SMTTVS-466	15.2-C – Logging system errors	The voting system must log system errors. **Discussion** This requirement ensures that any system errors are logged for analysis and remediation. System errors do not include user errors, such as undervotes or overvotes	BMD, CCOS, EMP, PCOS, Security, TDP
SMTTVS-467	15.2-D – Creating error reports	The voting system must be capable of creating error reports. **Discussion** Error reports allow system administrators to easily analyze the errors that occurred within a system.	BMD, CCOS, EMP, PCOS, Security
SMTTVS-469	15.3-A – Malware	COTS workstations providing EMS functionality must deploy mechanisms to protect against malware.	EMP, Security, TDP

Key	Summary	Description	Component/s
	protection mechanisms	**Discussion** *NIST SP 800-83 Revision 1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops [NIST13a]* might be useful as supplemental guidance for protecting against malware. Malware protection mechanisms are not required for voter-facing scanners and electronic BMDs. Alternatively, voter-facing scanners and electronic BMDs are required to use protection mechanisms, such as digital signatures and allowlists. This requirement is focused on EMS COTS workstations and does not include peripherals devices (e.g., printers).	
SMTTVS-470	15.3-B – Updatable malware protection mechanisms	The malware protection mechanisms for COTS devices providing EMS functionality must be updatable. **Discussion** Malware protection mechanisms typically use software signatures to identify malware. As new malware signatures are received, the malware protection mechanism needs to be updated with the new signatures to ensure it is identifying all known malware.	CCOS, EMP, PCOS, Security
SMTTVS-471	15.3-C – Documenting malware protection mechanisms	The voting system documentation must include the process and procedures for updating malware protection mechanisms. **Discussion** Providing documentation of the procedures to configure the malware protection mechanisms assists with ensuring the malware protection mechanisms are properly updated to meet *15.3.B - Updatable malware protection mechanisms*	Security, TDP

Key	Summary	Description	Component/s
SMTTVS-472	15.3-D – Notification of malware detection	COTS workstations and servers providing EMS functionality must immediately notify an election official when malware is detected. **Discussion** Malware on an EMS device can disrupt the integrity of the data on the EMS device. Once malware is detected, immediate notification of malware detection allows election officials to promptly take the proper action to avoid data integrity issues. This requirement is focused on EMS COTS workstations and does not include peripheral devices (e.g., printers).	EMP, Security, TDP
SMTTVS-473	15.3-E – Logging malware detection	The voting system must log instances of detecting malware	EMP, Security, TDP
SMTTVS-474	15.3-F – Notification of malware remediation	COTS workstations and servers providing EMS functionality must provide a notification upon the removal or remediation of malware. **Discussion** Once malware it is identified on a device, operations can cease until the malware is remediated. This notification allows administrators and officials to know when it is safe to resume normal operations. This requirement is focused on EMS COTS workstations and does not include peripherals devices (e.g., printers)	EMP, Security, TDP

Key	Summary	Description	Component/s
SMTTVS-475	15.3-G – Logging malware remediation	The voting system must log malware remediation activities. **Discussion** Remediation that requires the reimaging or reinstallation of the OS may need to be logged external to the voting system. Prior to reimaging, the malware detection logs could be downloaded and stored on another system to capture the time stamp of the malware event and preserve the malware event log for further analysis.	EMP, Security, TDP
SMTTVS-477	15.4-A – Internal network architecture documentation	The voting system documentation must include the network architecture of any internal network used by any portion of the voting system. **Discussion** Documentation of the internal network architecture can assist with data flow analysis, proper network configuration, and architecture to properly support the voting system	Integration, Security, TDP
SMTTVS-478	15.4-B – Secure network configuration documentation	The voting system documentation must list security configurations and be accompanied by network security best practices. **Discussion** This documentation may include how external network services are not included as part of the voting system and are handled through a separate air-gapped process. For example, a sneaker-net process may be used to manually transfer elections results to another system that uses public telecommunications to transmit the unofficial election results to a central count center.	CCOS, EMP, PCOS, Security, TDP

Key	Summary	Description	Component/s
		A variety of documentation providing secure configurations for network devices is publicly available from the US government. If outside manufacturers provide guidance and best practices, these need to be documented and used to the extent practical. This documentation may also include the use of firewalls and intrusion detection systems (IDS). Firewalls and IDSs are typically used to control and monitor the boundary between a private network and the internet. Although the current requirements do not allow for internet connectivity, firewalls and IDSs may also be used for internal boundaries and monitoring inside a private network. Guidance for Intrusion Detection and prevention systems can be found in *NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems [NIST07].*	
SMTTVS-479	15.4-C – Documentation for disabled wireless	The voting system documentation must include information about how wireless is disabled within the voting system. **Discussion** Documentation for how the voting system is configured to disable wireless networking is important to meet requirement *14.2-D – Wireless network status indicator*, which disallows the use of any wireless connections. Example information for how wireless can be disabled may include the following: • a system configuration process that disables wireless networking devices, • disconnecting/unplugging wireless device antennas, and	EMP, Security, TDP

Key	Summary	Description	Component/s
		• removing wireless hardware within the voting system. A variety of documentation providing secure configurations for network devices is publicly available from the US government. If outside manufacturers provide guidance and best practices exist, these need to be documented and used to the extent practical.	
SMTTVS-480	15.4-D – Rule and policy updates	The voting system must be capable of updating rules and policies for network appliances. **Discussion** Network appliances and the voting system are constantly receiving improvements and information related to current threats. As this information is released, rules and policies might need to be modified to adjust to new capabilities.	CCOS, EMP, Security, TDP

www.smartmatic.com