VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
1	High Quality Design - The voting system is designed to accurately, completely, and robustly carry out election processes.					
1.1	The voting system is designed using commonly accepted election process specifications.					
1.1.1	Election Definition					
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:		VxSuite supports importing an election definition in the common data format defined by any external toolset including VotingWorks' VxDesign. Exporting of this ballot definition takes place as part of saving an election package for programming precinct components.	VotingWorks testing staff manually tests importing election definitions into VxAdmin and exporting them from VxAdmin as part of functional QA testing. Test fixtures of these types of definitions are also used in automated testing.	System Overview > Election Package
1.1.1-A.1		election districts				
1.1.1-A.2		contests and ballot measures				
1.1.1-A.3		candidates				
1.1.1-A.4		ballot style information				
D	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.				
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:		VxSuite supports multiple election districts and precinct splits as part of compatibility with the ballot definition CDF whose specification supports serving multiple or split precincts and districts.	VotingWorks testing staff manually tests the system end-to-end with ballot definitions that include two or more election districts and/or combinations of precincts and split precincts. Test fixtures of these types of definitions are also used in automated testing.	System Overview > Election Package
1.1.1-B.1		two or more election districts; and/or				
1.1.1-B.2		combinations of precincts and split precincts.				
D	Discussion	This requirement addresses the capability to accommodate multiple ballot styles depending on the political geography being served by a polling place.				
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:		VxSuite supports importing ballot definitions per the ballot definition CDF that include multiple identifiers for cross-referencing of subdivisions, districts, etc.	VotingWorks testing staff manually tests ballot definitions that include multiple identifiers as part of functional QA testing. Test fixtures of these types of definitions are also used in automated testing.	System Overview > Election Package
1.1.1-C.1		locally defined identifiers				
1.1.1-C.2		state-wide-defined identifiers				
1.1.1-C.3		open civic data identifiers [OCD-ID]				
D	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.				
1.1.1-D	Definition of parties and contests	The voting system must allow for:		VxSuite supports definition of parties and contests per this requirement as part of compatibility with the ballot definition CDF whose specification supports serving multiple or split precincts and districts.	VotingWorks testing staff manually tests ballot definitions that include definitions of parties and contests per this requirement as part of functional QA testing. Test fixtures of these types of definitions are also used in automated testing.	System Overview > Election Package
1.1.1-D.1		the definition of political parties and indicate the affiliation or endorsements of each contest option				
1.1.1-D.2		information on both party-specific and non-party specific contests, with the capability to include both contests on the same ballot				
1.1.1-D.3		contests that include ballot positions with write-in opportunities.				
1.1.1-E	Voting variation	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.		VxSuite supports this capability for all of the voting variations specified in the implementation statement in the TDP.	VotingWorks testing staff manually tests ballot definitions for each voting variation in the implementation as part of functional QA testing to confirm the system functions properly end-to-end. Test fixtures of these types of definitions are also used in automated testing.	System Overview > Election Package
D	Discussion	See requirements in sections 1.1.4 – Casting and 1.1.8 – Tabulation for voting variations most commonly used in the U.S.				
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.		After loading the election definition onto a given VxSuite component, the recording is confirmed by showing the associated election definition hash and summary metadata on screen and in readiness reports.	VotingWorks testing staff manually confirms the expected election definition hash is shown on a given component after loading the package.	User Manual > Configure [Component]
D	Discussion	Persistent storage includes storage systems such as non-volatile memory, hard disks, and optical disks.				
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.		VxAdmin saves a digitally signed election definition to USB drives that are used to program each voting device.	VotingWorks testing staff manually exports signed election definitions from VxAdmin and imports to voting devices confirming they are successfully imported and authenticated.	User Manual > Save Election Package; System Overview > VxAdmin Function
1.1.1-H	Jurisdiction definition distribution	The voting system must enable election officials to update jurisdiction-dependent text, line art, logos, and images to ballot styles.		VxSuite supports any jurisdiction-dependent, text, line art, logos and images on ballot styles if the accompanying ballot definition is provided in a grid-based common data format specification.	VotingWorks testing staff manually creates ballot styles with custom text, line art, logos and images to confirm all voting system functionality properly functions end-to-end.	System Overview > Election Package
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.		VxSuite only provides the voter access to contests included in a ballot style per the election definition ballot style <> contest mapping.	VotingWorks testing staff confirms during functional testing that ballot styles only including contests specified in the election definitions ballot style <> contest mapping.	System Overview > Election Package
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.		VxSuite does not provide the voter access to any contests not included in their ballot style per the election definition <> contest mapping .	VotingWorks testing staff confirms during functional testing that ballot styles do not include any contests not specified in the election definitions ballot style <> contest mapping.	System Overview > Election Package
D	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.				
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.		VxSuite supports election definitions with contests mapped to different political parties as specified in the ballot definition CDF.	VotingWorks testing staff confirms during functional testing that contests are associated with the proper party.	System Overview > Election Package
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.		VxSuite supports election definitions with specified ballot rotation per the ballot definition CDF specification.	VotingWorks testing staff confirms during functional testing that ballots are rotated per the election definition specification.	System Overview > Election Package
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.		VxSuite supports multiple ballot styles for a given polling place per the ballot definition CDF specification.	VotingWorks testing staff confirms during functional testing that multiple ballot styles for a given polling can be created, marked, and tabulated properly.	System Overview > Election Package

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
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.		VxSuite encodes ballot style in the QR code on every ballot used by the system. Ballot styles are also presented visually on ballots in a manner that can be customized.	VotingWorks testing staff confirms during functional testing that QR codes on ballots uniquely identify the ballot style associated with ballots.	System Overview > Election Package
1.1.2	Pre-Election Testing					
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.		Every VxSuite component includes system diagnostics that test all key functions to produce a component readiness report during pre-election testing.	VotingWorks testing staff perform all system diagnostics during functional testing to confirm component readiness reports are produced that reflect the state of the system's readiness.	System Overview > Diagnostics; User Manual > [Component] Diagnostics
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.		Every VxSuite component validates the complete election definition is loaded upon import and provides a notification upon failed import if any issues arise. A log with the LogEventId "election-configured" will be made, if there was an error it will have the disposition "failure" and a description of the error.	VotingWorks testing staff import correctly formatted and inaccurately formatted ballot packages into all system components during functional testing to confirm they are accepted/rejected as expected with error messaging and logging in place.	User Manual > Configure [Component]; System Security, Auditing, Logging > Logging
D	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.				
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.		VxSuite supports the production of test ballots that can be used within a test mode across all system components.	VotingWorks functional testing staff perform end-to-end testing of the system in test mode.	User Manual > Logic & Accuracy Pre-Election Testing
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.		VxSuite vote capture devices can scan ballots that reflect all positions during testing. The ballots can be manually marked or produced as part of automated test deck generation.	VotingWorks functional testing staff performs scanning and tabulation of all ballot positions for various election definitions.	User Manual > Logic & Accuracy Pre-Election Testing
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.		VxSuite supports saving digitally signed CVRs to USB drives from tabulators that election officials can compare to the test ballots directly. Tabulators also prepare a result reports that can be compared in aggregate to the expected test ballot counts.	VotingWorks functional testing staff performs scanning and tabulation of all ballot positions for various election definitions and compares the tabulated summary & CVRs to the test ballots used.	System Overview > Cast Vote Records
D	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.				
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.	1.1.2-C – Use of test ballots	VotingWorks publicly publishes the format of BMD QR codes that include voter selections for election officials to use to decode the QR code value and compare to the text on the printed ballot or corresponding ballot image. During pre-election testing, election officials can also compare the interpreted values of these QR codes on tabulator tally reports to the expected values printed as the voter-verifiable text on the BMD ballot. Cast vote records have a shared unique identifier between the interpreted data and the ballot images for manual comparison.	VotingWorks functional testing staff compares the encoded values in BMD QR codes manually to the voter-verifiable text on the ballot. Testing also manually compares the ballot images and to the interpreted values in the cast vote record files.	System Overview > Hand Marked Ballots; System Overview > Machine Marked Ballots
D	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. and that the ballot was created accurately. will include such as provided by a ballot marking device (BMD) using QR codes and gain assurance that the QR codes and any encoded data represented by the QR codes contains the voter's selections exactly as made. Likewise, 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.				
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).		System settings in the election packages enable customization of mark thresholds on the tabulators to determine what is considered a valid mark when interpreting the ballot image.	VotingWorks functional testing staff tests various mark thresholds in system settings files and compares that the expected changes to tabulated values are applied in cast vote record files for given ballot images.	System Overview > Election Package
1.1.2-H	No side-effects from pre-election testing	Pre-election testing must introduce no lasting effects in regard to the operation of the voting system during the election other than:		Pre-Election testing maintains no lasting effects to all VxSuite applications other then audit log entries, status changes reflecting any calibration or hardware diagnostic tests that have been run.	VotingWorks functional testing staff tests regular pre-election testing procedures and verifies that there are no unexpected lasting changes to the system.	User Manual > Logic & Accuracy Pre-Election Testing
1.1.2-H.1		audit log entries				
1.1.2-H.2		status changes to note that the tests have been run with a successful or failed result				
1.1.2-H.3		separate storage of test results				
1.1.2-H.4		changes in counters that record ballots cast				
1.1.2-H.5		normal wear and tear				
D	Discussion	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.				
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:		All VotingWorks components provide the ability to create an equipment readiness report that reports on the status of any pieces of hardware associated with that application.	VotingWorks functional testing staff tests producing an equipment readiness report on each application and verifying its accuracy before and after performing various actions such as calibration, refilling toner and paper, etc.	System Overview > Diagnostics; User Manual > [Component] Diagnostics
1.1.2-I.1		whether calibration is needed				
1.1.2-I.2		consumable supplies such as toner or paper are sufficient for use				
1.1.2-I.3		batteries are fully charged				
1.1.2-I.4		the status of other election-sensitive aspects of the equipment				
1.1.2-J	Ballot style readiness report	The voting system must provide the capability to produce pre-election reports that include:		VxAdmin includes a readiness report with this information when configured for an election.	VotingWorks functional testing confirms VxAdmin provides accurate and complete information in the readiness report when configured.	User Manual > VxAdmin Diagnostics
1.1.2-J.1		the allowable number of votes in each contest				
1.1.2-J.2		the tabulation method for each contest				
1.1.2-J.3		the inclusion or exclusion of contests as the result of precinct splits				
1.1.2-J.4		samples of all final ballot styles				
1.1.2-K	Precinct-based voting devices readiness reports	Precinct-based voting devices must have the capability of generating readiness reports that include:		VxScan and VxMark, the precinct based voting devices, provide readiness reports that include an ID identifying the election configured, the currently configured precinct(s) and currently configured ballot style(s)	VotingWorks functional testing staff generates readiness reports on precinct-based devices configured for a specific precinct and verifies this information is listed as expected.	System Overview > Diagnostics; User Manual > [Component] Diagnostics
1.1.2-K.1		the election's identification data				
1.1.2-K.2		the identification of the precinct and polling place				
1.1.2-K.3		the identification of all ballot styles used in that precinct				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
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:		Vote-capture devices, provide a readiness report that includes all of the listed information. The polls open and polls closed reports will include all of the current tabulation data and can be used in combination with the readiness report to confirm all zero contest data upon polls opening. 1.1.2-L.2 is N/A to VxCentralScan as it is only programmed for all ballot styles within a jurisdiction for central scanning. 1.1.2-L.5 is N/A to any component as contest option registers are not part of the VotingWorks system archictecture.	VotingWorks functional testing staff generates readiness reports and polls open reports on all vote capture devices and ensures the expected information is present.	System Overview > Diagnostics; User Manual > [Component] Diagnostics
1.1.2-L.1		the election's identification data				
1.1.2-L.2		the identification of the precinct and polling place, if applicable				
1.1.2-L.3		the identification of the device				
1.1.2-L.4		the identification of all ballot styles loaded				
1.1.2-L.5		the contents of each active contest option register at all storage locations				
1.1.2-L.6		confirmation that no hardware or software failures were detected during setup and testing, or a record of those that occurred				
1.1.2-L.7		any other information needed to confirm the readiness of the equipment				
1.1.3	Opening the Polls					
1.1.3-A	Opening the polls	The voting system must provide functions to enter a mode in which voting is permitted.		Precinct-based systems, VxMark and VxScan, will be in a "closed" poll state when first configured for an election. Voting is not permitted in this state. Once authenticated with a poll worker smartcard, the poll worker will see on screen instructions to open the polls. can open the polls and move the machine into a "open" polls state. A polls open report will automatically print verifying the status of the polls, and "0" counts for all contest and ballot data. The screen will then additionally confirm in text that the Polls are Opened. Once polls are open, voting is permitted and ballots can be marked on VxMark or scanned on VxScan. The VotingWorks User Manual provides detailed instructions on opening and closing of polls.	VotingWorks functional testing involves opening and closing of polls through testing standard workflows.	User Manual > Opening Polls; System Overview > VxScan Function; System Overview > VxMark Function; User Manual > VxMark > Open and Close Polls
D	Discussion	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.				
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:		Whenever polls are opened, in either live or test mode, there is a check to make sure all data is zero. If it is not an error will be shown to the user. A PollsOpened log will be made to the audit log with the disposition of success if polls were successfully opened and failure if the "zero check" failed or the polls failed to open for any other reason. When any application is toggled between "live" and "test" mode all data is cleared. If there is an error in this process it will be shown to the user. The audit log will contain a "toggled-test-mode" log with the disposition success or failure as appropriate.	In practice it is impossible to have non-zero data when opening the polls, VotingWorks maintains automated testing of application logic to ensure that if there were somehow non-zero data there would be an error upon opening the polls and the appropriate log made. Automated testing is maintained to ensure that data is cleared when switching between live and test mode. VotingWorks staff performs functional testing to ensure that after completing L&A end to end in test mode that data is zeroed upon entering "live" mode, or configuring with a new election.	Security, Auditing, Logging > Logging; System Overview > VxScan Function
1.1.3-B.1		must be recorded in the audit log				
1.1.3-B.2		an election worker must be clearly notified of the event				
D	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, and 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.				
1.1.4	Casting - This section describes the requirements of the ballot issued to the voter and the types of contests that appear on the ballot. This includes characteristics that the voter must be aware of in order to accurately reflect the intent of their choices and the requirements of the voting system when the ballot is cast.					
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.		VxMark allows poll workers to select any ballot style configured for the precinct that VxMark is configured for to present to voters. This supports contests with the voting variations: N-of-M Contest and Ballot Measures for general elections and partisan closed primary elections as indicated in the implementation statement.		System Overview > Election Package; System Performance & Specifications > Supported Voting Variations
1.1.4-B	Control ballot configuration	The voting system must, where applicable:		When activated for a given ballot style VxMark will only show the contests appropriate for that ballot style. In a primary election the ballot style will be specific to the party affiliation declared by the voter and only include contests for that selection.	VotingWorks functional testing includes testing of all voting variations declared in the implementation statement. Automated testing of application logic ensures that the expected portions of the ballot are shown to a voter for their ballot style, including in a primary election.	User Manual > VxMark > Voting Sessions
1.1.4-B.1		activate all portions of the ballot the voter is entitled to vote on				
1.1.4-B.2		disable all portions of the ballot the voter is not entitled to vote on				
1.1.4-B.3		enable the selection of the ballot configuration that is appropriate to the party affiliation declared by the voter in a primary election				
D	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.				
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.		Ballot style to contest mapping is defined in the election definition per the Common Data Format specification.	VotingWorks functional testing confirms that a voter's ballot style only includes the contests explicitly mapped to the ballot style per the election definition.	System Overview > Election Package
D	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.				
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.		The order of contests on each ballot and ballot marking device follows the order prescribed in the election definition.	VotingWorks functional testing confirms that the order of ballots matches the order defined in the election definition.	System Overview > Election Package
D	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.				
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.		VxSuite supports partisan primary elections as an election type. Whether the primary is open or closed is dependent upon voter registration procedure outside of the voting system.	VotingWorks functional testing confirms that partisan primary type elections support all voting system functionality by party.	System Overview > Election Package; System Performance & Specifications > Supported Voting Variations
D	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).				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
1.1.4-F	Partisan open primary ballot	The voting system must provide a type of ballot, used in a partisan primary election, to the voter that contains partisan contests from all parties and any nonpartisan contests in which the voter is eligible to make choices. Only choices associated with one party will be permitted.		VxSuite supports partisan primary elections as an election type. Whether the primary is open or closed is dependent upon voter registration procedure outside of the voting system.	VotingWorks functional testing confirms that partisan primary type elections support all voting system functionality by party.	System Overview > Election Package; System Performance & Specifications > Supported Voting Variations
D	Discussion	This type of ballot is used in states that run open primary elections, where voters do not register by party but choose the party for which they wish to vote.				
1.1.4-G	Indicate party affiliations and endorsements	The voting system must provide a type of ballot associated with:		VxSuite supports these types of ballots as specified in the election definition.	VotingWorks functional testing confirms that party affiliations and endorsements are properly shown on ballots for primary or general election contests as specified in the election definition.	System Overview > Election Package; System Performance & Specifications > Supported Voting Variations
1.1.4-G.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)				
1.1.4-G.2		a partisan general election that identifies the affiliated/endorsing party of each contest choice.				
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.		Write-ins are enabled when specified in the election definition for a given contest.	VotingWorks functional testing that write-ins are properly tabulated for contests where write-ins are enabled.	System Overview > Election Package
D	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.				
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.		VxAdmin provides a workflow to adjudicate write-ins that allows an election official to adjudicate a write-in as a candidate alias. If the adjudication would create a double vote an error message is shown and the adjudication is not allowed.	VotingWorks functional testing confirms that VxAdmin write-in adjudication properly reconciles aliases and presents an error in the case of potential double votes.	User Manual > Write-in Adjudication; System Overview > VxAdmin Function
D	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.				
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.		VxMark supports displaying an N-of-M contest and will only allow the user to select up to N choices. If the user tries to select a N+1th choice they will be shown an error that they can not select another choice.	Automated tests of application logic ensure proper display and recording of N-of-M contests. VotingWorks functional testing ensures N-of-M contests can be voted on as expected.	System Overview > Election Package; System Performance & Specifications > Supported Voting Variations; System Overview > VxMark Function
D	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 1 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.				
1.1.4-K	Straight-party voting, Casting	For straight-party voting, the voting system must be able to provide a contest in which a voter may select political party contest choices that result in the selection of all partisan contests on their ballot. In this instance, a selection of a political party choice automatically selects all contest choices associated with that party. The voting system must be capable of gathering and recording votes for both this contest and all partisan contests associated with it.		N/A - Not included in implementation statement.		
D	Discussion	Straight-party voting is a voting variation used in a general election. It provides the voter with the ability to select all candidates affiliated with a desired party in all partisan contests on the ballot by selecting one contest option. When a party is selected, the system must not prevent the selection of individual candidate options that may negate the original straight-party choice, nor must it require that voters utilize the straight-party voting option. Rules for determining the candidate choices resulting from the combination of direct option selections and straight-party option selections are determined by the rules in states that use straight-party voting.				
1.1.4-L	Cumulative voting contest, Casting	For a cumulative voting contest, the voting system must be capable of gathering and recording votes in a contest where the voter may allocate no more than the allowed number of votes to one or more contest selections in whole vote increments.		N/A - Not included in implementation statement.		
D	Discussion	When a cumulative voting contest is on a ballot, the system must allow the voter to assign all allowed votes to any desired contest selection or to any set of contest selections in whole vote increments. The total of all selection assignments must not exceed the total votes allowed. (See 1.1.4-Q - Proportional voting contest (equal-and-even cumulative voting contest), Casting for an alternate method of assigning multiple votes to a candidate.)				
1.1.4-M	Ranked choice voting contest, Casting	For a ranked choice voting (RCV) contest, the voting system must be capable of gathering and recording votes in a contest where the voter must be able to rank contest selections in order of preference, as first choice, second choice, etc.		N/A - Not included in implementation statement.		
D	Discussion	The ballot presentation of a RCV contest is independent of the number of seats being elected. Depending on jurisdictional rules, the number of choice options provided may vary from a minimum of 3 to the number of contest choices on the ballot. Contest outcome determination requires cast vote records (CVR) to be processed post-election.				
1.1.4-N	Party preference contest	For a party preference contest, the voting system must be capable of gathering and recording votes for a contest containing a list of political party choices. In this instance, the voting system uses a valid selection of a party in the contest, which limits gathering and recording of votes in all partisan contests on the ballot to those associated with the selected party.		N/A - Not included in implementation statement.		
D	Discussion	A party preference contest only appears on an open primary ballot when required by state rules. Its purpose is to allow the voter to select the party they intend to vote contests for and prevent the voter from spoiling the partisan section of the ballot by, for example, marking contests in a different party's section of the ballot.				
1.1.4-O	Top-2 primary contest (blanket primary contest)	For a top-2 primary contest, the voting system must be capable of assigning candidates of all relevant parties to a single seat contest which is also assigned to all partisan ballots.		N/A - Not included in implementation statement.		
D	Discussion	In some states, this method is required to be used to fill designated partisan offices. The contest, also called a blanket primary contest, appears on all party-specific primary ballots. All candidates are listed as contest options including their party affiliation. The 2 candidates who receive the most votes will be on the general election ballot independent of their party affiliation.				
1.1.4-P	Presidential delegate contest, Casting	For a presidential delegate contest, the voting system must be capable of gathering and recording votes for only those delegates that are affiliated with the voter's choice in the presidential preference contest.		N/A - Not included in implementation statement.		
D	Discussion	Presidential delegate voting is a voting variation that only is used in a presidential primary election on a party-specific primary ballot where delegates to the convention are selected by the voter when the method is selected by a state's political party. With this method, only contest option selections in delegate contests that are pledged to the voter's presidential candidate selection will be recorded. If the voter does not make a selection in the presidential preference contest, selections for presidential delegates will not be recorded.				
1.1.4-Q	Proportional voting contest (equal-and-even cumulative voting contest), Casting	For a proportional voting contest, the voting system must be capable of gathering and recording votes for a contest which allow multiple votes to be assigned to a candidate. This is accomplished by prorating the number of allowed votes proportionally to the number of validly selected candidates.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
D	Discussion	Also known as equal-and-even cumulative voting, this contest is an alternative to a cumulative voting contest in allowing multiple votes to be assigned to selected candidates. Votes are assigned based on the votes allowed and the number of valid selections made by dividing the number of votes allowed by the number of options chosen. Marking fewer selections than the number of votes allowed may result in fractional votes being assigned to a contest option.		N/A - Not included in implementation statement.		
1.1.4-R	Group voting contest, Casting	For a group voting contest, the voting system must be capable of designating a group select contest choice that automatically selects, gathers and records all contest choices associated with the group. More than one contest group select contest choice must be provided if the contest contains more than one group of candidates.		N/A - Not included in implementation statement.		
D	Discussion	A group voting contest is used to enable the voter to select a large number of allowed candidate options associated with a single group, party or ideology with a single option selection. There may be multiple groups of contest choices each associated with a single selection. The system treats a group selection as if all candidates in the group are selected when determining the number of selections made. This voting variation is currently only used in the State of Massachusetts to select Ward and Town party committee persons and only appears on the ballot in the presidential preference primary.				
1.1.4-S	Top-2 IRV contest (supplementary or contingent vote contest)	For a top-2 instant runoff voting (IRV) contest, the voting system must be capable of gathering and recording votes in a contest where the voter must be able to rank contest options in order of preference as their first choice, second choice, etc.		N/A - Not included in implementation statement.		
D	Discussion	The top-2 IRV contest, also known as a supplementary or contingent vote contest, is an IRV type contest and provides the voter the ability to identify the contest options in order of preference in the same fashion as a standard IRV contest. Although voted the same as an IRV contest and requiring cast vote records to be processed post-election to determine outcome, only the top-2 candidates with the most votes are eligible to win.				
1.1.5	Recording Voter Choices					
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.		Cast vote records reflect the selections made by the voter.	VotingWorks functional testing confirms that cast vote records properly reflect selections made by the voter by comparing ballot images to cast vote record files.	System Overview > Cast Vote Records
1.1.5-B	Ballot orientation	The voting system, when using pre-printed ballots, must either:		All tabulating devices can accept pre-printed ballots in any orientation.	VotingWorks functional testing confirms that ballots are accepted and properly tabulated by ballot scanners in any orientation.	System Overview > Hand Marked Ballots
1.1.5-B.1		correctly mark pre-printed ballots regardless whether they are loaded upside down, right side up, forward, or reversed				
1.1.5-B.2		detect and reject pre-printed ballots that are oriented incorrectly				
1.1.5-C	Record contest selection information	The voting system must record contest selection information in the CVR that includes:		The CVR includes all contest selections and ballot positions made by the voter.	VotingWorks functional and automated testing confirms that CVR contest selections and ballot positions are properly recorded for given ballot images.	System Overview > Cast Vote Records
1.1.5-C.1		all contest selections made by the voter for all supported vote variations				
1.1.5-C.2		positions on the ballot associated with each contest selection made by the voter when multiple selections are permitted, if applicable				
D	Discussion	For item 2, some contests such as for RCV may place candidate choices on the same line of the ballot, therefore the positions of the candidates may need to be recorded.				
1.1.5-D	Record write-in information	The voting system must record write-in information in the CVR that includes:		CVRs include the contest selection and ballot position made by the voter for a given write-in selection associated with corresponding ballot images. Ballot marking devices additionally record the text of the write-in in the CVR. CVRs are exported in the CVR CDF which also includes the total number of write-ins.	VotingWorks functional and automated testing confirms that all write-in information is properly recorded in the CVR.	System Overview > Cast Vote Records
1.1.5-D.1		identification of write-in selections made by the voter				
1.1.5-D.2		the text of the write-in, when using a BMD or other device that marks the ballot for the voter				
1.1.5-D.3		an image or other indication of the voter's write-in markings				
1.1.5-D.4		the total number of write-ins in the CVR				
1.1.5-E	Record election and contest information	The voting system must record additional contest information in the CVR that includes:		CVRs include identification of all contests, all overvotes/undervotes, number of write-ins, and identification of the party per the CVR CDF specification.	VotingWorks functional and automated testing confirms that all contest information is properly recorded in the CVR per the CVR CDF specification.	System Overview > Cast Vote Records
1.1.5-E.1		identification of all contests in which a voter has made a contest selection				
1.1.5-E.2		identification of all overvoted and undervoted contests				
1.1.5-E.3		the number of write-ins recorded for the contest				
1.1.5-E.4		identification of the party for partisan ballots or partisan contests				
D	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.				
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:		VxSuite tabulators do not record voter selections differently than as marked, but support the future ability to do so based on CVR snapshots that represent the original and modified values.	VotingWorks functional testing confirms that voter selections are recorded as marked and that original and modified values in the CVR are properly recorded.	System Overview > Cast Vote Records
1.1.5-F.1		identification of the original ballot selections made by the voter				
1.1.5-F.2		identification of the changed voter selections				
1.1.5-F.3		identification of the reasons for the changes				
D	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.				
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:		Cast vote record report metadata contains the identification of all required audit information	VotingWork functional and automated testing confirms that all CVRs record all audit-related information.	System Overview > Cast Vote Records
1.1.5-G.1		identification of the specific creating device such as a serial number				
1.1.5-G.2		identification of the geographical location of the device				
1.1.5-G.3		identification of the ballot style corresponding to the CVR				
1.1.5-G.4		identification of the corresponding voted ballot				
1.1.5-G.5		for multi-sheet ballots, identification of the individual sheet corresponding to the CVR, along with the identification of the ballot style				
1.1.5-G.6		identification of the batch containing the corresponding voted ballot, when applicable				
1.1.5-G.7		sequence of the corresponding voted ballot in the batch, when applicable				
D	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.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
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.				
D	Discussion	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.		Cast vote records may include a corresponding ballot image with a shared unique identifier.	VotingWorks functional and automated testing confirms that the unique identifier shared between ballot images and CVRs corresponds to the same ballot.	System Overview > Cast Vote Records
1.1.6	Ballot Handling for Vote-Capture Devices					
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.				
D	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.		An error message is presented to the voter or election official when a ballot style is scanned that does not correspond with the ballot styles included in the scanner configuration.	VotingWorks functional and automated testing confirms that an error message is presented when a ballot style is scanned that is not included in the scanner configuration.	System Overview > Ballot Interpretation; User Manual > VxScan Error Messages; User Manual > VxMark Error Messages
1.1.6-B	Detect and reject ballots that are oriented incorrectly	The voting system must either:				
1.1.6-B.1		correctly count ballots regardless of whether they are fed upside down, right side up, forward, or reversed				
1.1.6-B.2		detect and reject ballots that are oriented incorrectly		VxSuite tabulators accept ballots in all orientations.	VotingWorks functional and automated testing confirms that ballots can be interpreted in all orientations.	System Overview > Ballot Interpretation
1.1.6-C	Ballot separation when batch feeding	Batch-fed scanners, in response to unreadable ballots, write-ins, and other designated conditions, must do one of the following:				
1.1.6-C.1		out stack the ballot (that is, divert to a stack separate from the ballots that were normally processed)				
1.1.6-C.2		stop the ballot reader and display a message prompting the election official to remove the ballot				
1.1.6-C.3		mark the ballot with an identifying mark to facilitate its later identification				
1.1.6-C.4		if the ballot image uniquely identifies its corresponding ballot, use electronic adjudication to segregate the ballot				
D	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.		VxCentralScan can be configured via system settings to stop in response to ballot adjudication conditions and prompts the election official to remove the ballot. An imprinter may also be used with VxCentralScan to facilitate its later identification. Write-in adjudication is later completed on VxAdmin through electronic adjudication as the ballot image uniquely identifies its corresponding ballot.	VotingWorks functional testing confirms that the VxCentralScan responds as expected based on the system settings configuration in the election package.	User Manual > Central Scanning; System Overview > VxCentralScan Function
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:	7.3-H - Overvotes; 7.3-I - Undervotes			
1.1.6-D.1		ballots containing overvotes in a designated contest				
1.1.6-D.2		ballots containing undervotes in a designated contest				
1.1.6-D.3		ballots containing contests that were not voted				
1.1.6-D.4		blank ballots		Voter facing scanners provide a message to voters in these conditions that enable the removal and correction of the ballot based on the adjudication reasons specified in the system settings within an election package.	VotingWorks functional and automated testing confirms that a message is presented in these conditions when the associated adjudication reason is enabled in the election package.	User Manual > Assisting Voters; System Overview > VxScan Function
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:				
1.1.6-E.1		segregate the ballot in a manner that facilitate its later identification				
1.1.6-E.2		if the ballot image uniquely identifies its corresponding ballot, use electronic adjudication to segregate the ballot				
D	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, and 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.		VotingWorks tabulators use electronic adjudication to segregate the ballot when a write-in vote is made. Write-in adjudication takes place on VxAdmin after CVR import.	VotingWorks functional testing confirms that all write-in selections are presented on screen for write-in adjudication on VxAdmin.	User Manual > Write-In Adjudication
1.1.6-F	Ability to clear mis-fed ballots	If multiple feed or misfeeding (jamming) occurs, batch-fed scanners must:				
1.1.6-F.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)				
1.1.6-F.2		prevent duplicate scanning of the ballots				
D	Discussion	Number 2 deals with whether CVRs have been created for the ballots that were jammed.		VxCentralScan presents an error message when a scan is unreadable due to misfeeding specifying that the ballot shown on screen has not been counted. An operator may then compare the ballot on screen to the misfed ballot to confirm it is not double counted when rescanned.	VotingWorks functional testing confirms that centrally scanned ballots are not duplicated when following instructions on screen in response to misfed or jammed ballots.	User Manual > Central Scanning; System Overview > VxCentralScan Function
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.				
D	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.		VxScan and VxCentralScan produce readiness reports that include the mark thresholds set on the scanner. This data is also included in the election package used to program the scanners.	VotingWorks functional testing confirms that the mark thresholds specified in the election package are reflected in readiness reports and the CVR produced for a given scanner.	System Overview > Diagnostics; User Manual > VxScan Diagnostics; User Manual > VxCentralScan Diagnostics
1.1.6-H	Accurately detect imperfect marks	The voting system must detect a 1 mm thick line that:				
1.1.6-H.1		is made with a #2 pencil that crosses the entirety of the contest option position on its long axis				
1.1.6-H.2		is centered on the contest option position				
1.1.6-H.3		is as dark as can practically be made with a #2 pencil				
D	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; 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.		Default mark thresholds accurately detect this type of mark and consider it a voting selection.	VotingWorks functional testing confirms that marks of this type are properly tabulated as votes when scanners are programmed with default mark threshold values.	System Performance & Specifications > Reliably Detectable Marks
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.	1.1.6-G – Scan to manufacturer specifications			System Performance & Specifications > Reliably Detectable Marks
D	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.		These types of insignificant marks are not considered votes when scanning ballots using default mark thresholds.	VotingWorks functional testing confirms that these types of insignificant marks are not considered votes when scanners are programmed with default mark threshold values.	
1.1.6-J	Marginal marks, without bias	The detection of marginal marks from manually marked paper ballots must not show a bias.				
D	Discussion	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.		Marks for all ballot positions are interpreted identically.	VotingWorks functional and automated testing confirms that the same mark for two given ballot positions are interpreted equivalently.	System Overview > Ballot Interpretation
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.				
D	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.		A given mark on a ballot will be interpreted identically on successive scans given the mark threshold value is not changed.	VotingWorks functional and automated testing confirms that a given ballot mark is repeatedly interpreted the same when the mark threshold for the scanner remains the same.	System Overview > Ballot Interpretation
1.1.7	Exiting or Suspending Voting					
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.				User Manual > Closing Polls; User Manual > Additional Poll Worker

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
D	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.		Authenticated poll workers can "close polls" to exit or "pause polls" to suspend voting.	VotingWorks functional testing confirms that voting is not permitted when polls are closed or suspended by a poll worker.	Actions; System Overview > VxMark Function; System Overview > VxScan Function; User Manual > VxMark > Open and Close Polls
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.				
D	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.		Ballots cannot be marked on VxMark nor cast on VxScan when polls are closed or suspended.	VotingWorks functional testing confirms that voting is not permitted when polls are closed or suspended by a poll worker.	System Overview > VxMark; System Overview > VxScan
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.		VxSuite software verifies that the polls report is printed, cast vote records are exported to the USB drive, and the internal state has been updated after a poll worker selects the function on screen.	VotingWorks functional testing and automated testing confirms that voting is not permitted when polls are closed or suspended by a poll worker.	User Manual > Closing Polls
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.		A polls closed and polls open report is generated when voting is stopped.	VotingWorks functional testing confirms that this report is generated when voting is stopped.	User Manual > Opening Polls; User Manual > Closing Polls; System Overview > VxScan Polls Reports
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.	11.3.1-B – Multi-factor authentication for critical operations			
D	Discussion	When early voting is conducted across multiple days, this requirement does not prevent reopening of the polls on the following day.		The voting system does not enable re-opening polls once closed other than providing a system administrator the ability to reset the polls to a paused state.	VotingWorks functional testing confirms that the only means of voting after closing polls is after a system administrator resets the polls to a paused state.	User Manual > Additional VxScan Settings; System Overview > VxScan Function; System Overview > VxMark Function
1.1.8	Tabulation					
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:				
1.1.8-A.1		extracting the valid votes from each ballot cast according to the defined rules				
1.1.8-A.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				
1.1.8-A.3		accumulation and aggregation of contest results and ballot statistics				
D	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.		Tabulation on VxScan and VxCentralScan and aggregation on VxAdmin is supported for all voting variations in the implementation statement.	VotingWorks functional and automated testing confirms that all votes are tabulated and aggregated as expected.	System Performance and Specifications > Supported Voting Variations
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.				
D	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 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.		All primary election tabulation reports and broken down by party.	VotingWorks functional and automated testing confirms that all primary reports and broken down by party.	System Overview > VxScan Polls Reports; System Overview > VxAdmin Results Exports > Tally Reports
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.		For ballots specific to one party (but are inclusive of nonpartisan contests), the voting system reports on the combined totals of nonpartisan contests across all party ballots.	VotingWorks functional and automated testing confirms nonpartisan contests across primary ballot styles are tabulated and aggregated properly.	System Overview > VxScan Polls Reports; System Overview > VxAdmin Results Exports > Tally Reports
1.1.8-B.2	Tabulation of an open primary ballot	When tabulating ballots from an open primary, the voting system must limit tabulation of votes to contests of one political party.				
D	Discussion	In an open primary, a voter may select partisan contest choices that are associated with more than one political party. Therefore, tabulation of a ballot during an open primary will void the partisan content of the ballot and only contest selections in nonpartisan contests are tabulated. The ballot is treated like a nonpartisan ballot.		In a primary election on VxSuite, ballots are specific to a given party and VxSuite assumes that election officials are procedurally limiting voter access to one party ballot to support open primaries.		
1.1.8-B.3	Open primary ballot with party preference contest	If the ballot contains a party preference contest and a party preference contest choice is selected, the voting system must only tabulate partisan contest option selections from contests that are of the same party as is selected in the party preference contest.	1.1.4-N – Party preference contest	N/A - not included in implementation statement		
D	Discussion	A party preference contest provides the voter with the ability to select their intended party and avoid cross-party selections voiding the partisan selection of the ballot. If a party preference contest option is not selected, partisan contests on the ballot are tabulated as if the party preference contest was not present.				
1.1.8-C	Write-ins, Tabulation	The voting system must be capable of				
1.1.8.C.1		tabulating votes for write-in candidates with separate totals for each contest choice				
1.1.8.C.2		tabulating valid individual write-in candidate totals in each contest				
D	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 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.		VxSuite tabulates write-in votes for each contest choice and provides a write-in adjudication interface on VxAdmin to tabulate valid individual write-in candidate totals in each contest.	VotingWorks functional and automated testing confirms that write-in votes are tabulated properly post-adjudication.	User Manual > Write-In Adjudication; System Overview > VxAdmin Function; System Overview > VxAdmin Results Exports
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.		Ballot rotation does not impact tabulation in VxSuite.	VotingWorks functional and automated testing confirms that votes are counted accurately regardless of rotation.	System Overview > Election Package
1.1.8-E	Straight-party voting, Tabulation	When tabulating a partisan general election ballot, which includes a validly selected straight-party contest option in a straight-party contest, the voting system must select each candidate contest choice that is endorsed by the selected party in every contest on the ballot unless the contest is specifically exempted.				
D	Discussion	There are currently two different tabulation rule sets for handling a ballot with both a straight-party selection and a selection in a contest of a candidate not endorsed by the selected party, known as party crossover. In one, any selection of a contest choice in a partisan contest eliminates any straight-party selection in that contest. In the other, straight-party option selections in a contest are eliminated if the number of candidates selected exceeds the allowed number, whether directly selected by the voter or automatically selected by the straight-party. Other rules are possible as well. Note that some states explicitly indicate that certain contests will not be affected by a straight-party selection.		N/A - not included in implementation statement		

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
1.1.8-F	Cross-party endorsement with straight-party voting	For straight-party tabulation, if a listed candidate option is endorsed by more than one political party, the voting system must be capable of tabulating votes for that candidate independent of which party option is validly selected.		N/A - not included in implementation statement		
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.		VxSuite supports precinct splits as modeled in the election definition and tabulation is not affected by variation of contest selection locations from one ballot or another.	VotingWorks functional and automated testing confirms that tabulation of precincts split ballots is accurate.	System Overview > Election Package
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.		N-of-M tabulation follows the tabulation rules for votes, overvotes, and undervotes as described in the discussion of this requirement.	VotingWorks functional and automated testing confirms that tabulation of N-of-M contests follows these rules.	System Performance and Specifications > Supported Voting Variations
D	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 (1 vote for 1 contest or typically a measure) or any larger 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 is used for top-2 primary contests (blanket primary contests), where N is always 1 but the 2 candidates with the most votes will be on the general election ballot.				
1.1.8-I	Cumulative voting contest, Tabulation	For cumulative voting, the voting system must be capable of tabulating votes, overvotes, and undervotes in contests where the voter may allocate up to a specified number of votes over a list of contest choices in any manner they choose. This may result in possibly giving more than one vote to a given contest selection.		N/A - not included in implementation statement		
1.1.8-J	Ranked choice voting contest, Tabulation	For ranked choice voting (RCV), the voting system must		N/A - not included in implementation statement		
1.1.8-J.1		capture the voter's ranking of each contest selection and store it in the CVR associated with the ballot style				
1.1.8-J.2		aggregate 1st choice totals of each contest selection				
1.1.8-J.3		process the collection of CVRs round-by-round according to the method specified in the implementation statement				
D	Discussion	Ranked choice voting (RCV) tabulation methods are different for single seat and multi-seat contests. Jurisdictional rules vary even when using the same basic method. A voting unit or precinct tabulating unit cannot perform RCV tabulation. RCV tabulation requires the concurrent availability of all CVRs associated with an RCV contest and is a post-voting accumulation/aggregation process. Some jurisdictional rules may only require use of the RCV tabulation process if aggregated first choice selections do not produce the total needed to exceed the threshold of votes required to win. Other jurisdictional rules do not use tabulated and aggregated 1st choice selections and require the RCV tabulation process to be used for all winners. Single winner RCV is also known as IRV (Instant Runoff Voting). STV (Single Transferable Vote) is a method used for multi-winner RCV. Another multi-winner process (Sequential At-Large IRV) uses successive IRV passes, one pass to determine each winner.				
1.1.8-K	Group voting contest, Tabulation	When tabulating group voting contest choices, the voting system must automatically select each contest choice that is affiliated with the selected group as if the voter manually selected each of those candidate choices. Any selection of a contest choice outside of the group will constitute as an overvote if the number of candidates in the group selected is equal to the votes allowed.		N/A - not included in implementation statement		
D	Discussion	There may be multiple candidate groups in a contest. The ballot normally places contest options for all candidates in a group sequentially, with the group contest option first. If a contest is not fully voted by utilizing the group voting contest option, a voter can select additional contest options outside of the group, as long as the total does not exceed the votes allowed.				
1.1.8-L	Presidential delegate contest, Tabulation	When tabulating a presidential delegate contest, the voting system must prevent votes for any delegate in the contest that is not representing the president candidate chosen by the voter's contest option selection in the presidential contest.		N/A - not included in implementation statement		
D	Discussion	Most states that directly elect presidential delegates do not have a tabulation associated with the presidential candidate selection. However, as of 2020, Alabama has included this association on both the democratic and republican ballots, while Rhode Island has the association on the democratic ballot. When used, if there is no presidential candidate selection or the presidential candidate and no affiliated delegate in the contest, no vote will be counted for any delegate contest option selection.				
1.1.8-M	Recall contest pair	When tabulating a recall/replace contest pair, the voting system must only tabulate the replace contest (controlled contest) if there is a vote selection in the recall contest (controlling contest).		N/A - not included in implementation statement		
	Discussion	The recall contest in the contest pair is typically a question used to determine whether an elected official should be recalled and the replace contest allows selection of the desired replacement. If the question is not voted, the replacement contest is not processed. However, the contest pair has been used for other purposes such as annexations and determination of tax rates.				
1.1.8-N	Proportional voting contest (equal-and-even cumulative voting contest), Tabulation	Votes selections in a proportional voting contest (also known as an equal-and-even cumulative voting contest) must be tabulated for the selected contest option or options by dividing the allowed votes by the number of contest option selections; this may occur as long as the number of selections do not exceed the number of allowed votes.		N/A - not included in implementation statement		
D	Discussion	This may produce a fractional number of votes tabulated for a candidate. However, it is not possible to tabulate undervotes in this contest.				
1.1.9	Reporting Results					
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.		VxAdmin reports contain cast ballot counts and vote counts for ballots from precincts or split precincts.	VotingWorks functional and automated testing confirms cast ballot counts and vote counts in VxAdmin contain accurate cast ballot counts and vote counts.	System Overview > VxAdmin Results Exports; System Overview > VxAdmin Function
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:		VxAdmin reports have the capability to report on number of ballots cast in total and broken down by ballot style, district (political geography), sheet, ballot type (absentee vs. precinct) amongst other possible reports. VxAdmin also reports on the total number of blank ballots.	VotingWorks functional and automated testing confirms these types of reports are available for generation in VxAdmin and that the reports are accurate.	System Overview > VxAdmin Results Exports; System Overview > VxAdmin Function
1.1.9-B.1		All read ballots and all counted ballots				
1.1.9-B.2		For multi-page ballots, the number of different pages read, and number counted				
1.1.9-B.3		Read ballots and counted ballots that require review				
1.1.9-B.4		Absentee read and counted ballots				
1.1.9-B.5		Blank ballots (ballots containing no votes)				
D	Discussion	Associated units of political geography may also include state, county, city, town or township, ward, and districts.				
1.1.9-C	Report categories of votes	The voting system must have the capability to report the following categories of votes:				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
1.1.9-C.1		in-person voting		VxAdmin provides reports for in-person voting (precinct ballots), absentee voting (absentee ballots), write-ins, as well as the result of adjudicated write-in ballots. VxSuite does not have a concept of a "rejected" ballot, but write-in marks can be deemed invalid during write-in adjudication.	VotingWorks functional and automated testing confirms that VxAdmin properly reports on these categories of votes with correct expected values.	System Overview > VxAdmin Results Exports; System Overview > VxAdmin Function
1.1.9-C.2		absentee voting				
1.1.9-C.3		write-ins				
1.1.9-C.4		accepted reviewed ballots				
1.1.9-C.5		rejected reviewed ballots				
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.		VxAdmin tally reports consolidate vote data from all precincts included in the report filter.	VotingWorks functional and automated testing confirms that CVRs are properly aggregated across multiple precincts.	System Overview > VxAdmin Results Exports; System Overview > VxAdmin Function
D	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.				
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.		Tally reports include the ballot count for each N-of-M contest.	VotingWorks functional and automated testing confirms that ballot count reports provide ballot counts for each contest.	System Overview > VxAdmin Results Exports
D	Discussion	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.				
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.		Tally reports include the vote totals for each option in an N-of-M contest.	VotingWorks functional and automated testing confirms the vote count reports provide accurate vote counts for each contest.	System Overview > VxAdmin Results Exports
D	Discussion	N-of-M in this requirement includes the most common type of contest, 1-of-M.				
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.		Tally reports include the number of overvotes for each N-of-M contest.	VotingWorks functional and automated testing confirms the report of overvotes provide accurate vote counts for each contest.	System Overview > VxAdmin Results Exports
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.		Tally reports include the number of undervotes for each N-of-M contest.	VotingWorks functional and automated testing confirms the report of undervotes provide accurate vote counts for each contest.	System Overview > VxAdmin Results Exports
D	Discussion	Counting ballots containing undervotes instead of votes lost to undervoting is insufficient.				
1.1.9-I	Ranked choice voting, report results	The voting system must have the capability to report the contest choice vote totals for each ranked choice contest and for each round of tabulation.		N/A - not included in implementation statement		
D	Discussion	This requirement is minimal. Since ranked choice voting is not currently in wide use, it is not clear what needs to be reported, how bogus orderings are reported, or how it would be done in multiple reporting contexts.				
1.1.9-J	Precinct reporting devices, reporting device consolidation	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.		VxAdmin aggregates CVRs from multiple vote-capture devices used in a single polling place and can create a consolidated report for the entire polling place.	VotingWorks functional and automated testing confirms that results are properly aggregated for CVRs aggregated from devices configured for the same polling place.	System Overview > VxAdmin Results Exports; System Overview > VxAdmin Function
D	Discussion	This requirement essentially requires precinct-based vote-capture devices to be able to consolidate voting data for the purposes of issuing one consolidated report.				
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.		Tally reports on VxScan with vote data are unavailable to print until polls are closed.	VotingWorks functional and automated testing confirms that tally reports with vote data are unavailable to print until polls are closed.	System Overview > VxScan Polls Reports; System Overview > VxScan Function
D	Discussion	Providing ballot counts does not violate this requirement. The prohibition is against providing vote totals for ballot contests.				
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.		Primary election reports separate totals for each party.	VotingWorks functional and automated testing confirms that primary elections properly report separate and accurate totals for each party.	System Overview > VxAdmin Results Exports
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.		All reports generated by the voting system are timestamped with date and time.	VotingWorks functional and automated testing confirms that all reports are timestamped.	System Overview > VxAdmin Results Exports; System Overview > VxScan Polls Reports; User Manual > [Component] Diagnostics
1.2	The voting system is designed to function correctly under real-world operating conditions					
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:		All votes are tabulated and reported accurately. All VVSG requirements applicable to the implementation statement are met.	VotingWorks functional and automated testing confirms that all votes are tabulated accurately and that all applicable VVSG requirements are met.	Quality Assurance Manual
1.2-A.1		A measurement of how accurately voter marks are recognized as valid or not valid according to manufacturer specifications				
1.2-A.2		A measurement of how accurately voter marks are tabulated and reported as results				
1.2-A.3		An assessment of whether the remaining VVSG requirements are satisfied				
D	Discussion	The data collected during the testing of this requirement contributes substantially to the evaluations of reliability, accuracy, and misfeed rate.				
1.2-B	Reliability 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.		The voting system detects marks consistent with mark specifications in the TDP.	VotingWorks functional and automated testing confirms that the system reliably detects marks consistent with specifications in the TDP.	System Performance and Specifications > Reliably Detectable Marks
D	Discussion	The specification may have parameters for different configuration values. It should also state the degree of uncertainty.				
1.2-C	Minimum ballot positions	A minimum of 10,000,000 ballot positions must be read by the voting system and tabulated accurately.		All votes are tabulated accurately.	VotingWorks functional testing tests tabulation accuracy above 10,000,000 ballot positions.	Quality Assurance Manual
D	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.				
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.		The voting system handles the maximum volume of activities according to system limits specified in the TDP.	VotingWorks functional testing tests the complete system at the volume limits defined in the TDP system limits.	System Performance and Specifications > System Limits
D	Discussion	This requirement should be verified through operational testing if the limit is practically testable.				
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.		Every voting system component fails gracefully in response to conditions when system limits are exceeded.	VotingWorks functional testing exceeds system limits to confirm all components always fail gracefully and can recover.	System Performance and Specifications > System Limits
D	Discussion	This requirement should be verified through operational testing if the limit is practically testable.				
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.		The voting system prevents against a single point of failure in several ways including: redundant data storage, continuously writing cast ballots to external disk, uninterruptible power supplies, and hardware features for emergency casting of ballots.	VotingWorks functional testing confirms that ballots may be continued in the event of various system failures.	System Security, Auditing & Logging
D	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.				
1.2-G	Misfeed rate benchmark	The voting system misfeed rate must not exceed 0.002 (1 / 500).			VotingWorks manual functional testing and automated	

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
D	Discussion	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.		tem	robotic feeding confirms that the misfeed rate does not exceed 1/500.	Quality Assurance Manual
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.				
D	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.		The voting system prevents the loss of data without recasting ballots by continuously exporting CVRs on VxScan to external disk while saving a redundant copy on internal disk.	VotingWorks functional testing confirms that no cast voter record data is lost due to the failure of any disk.	System Overview > VxScan Function
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].				
1.2-I.1		Voting devices located in polling places must minimally comply with Class B requirements				
1.2-I.2		Voting devices located in non-polling place settings such as back offices must minimally comply with Class A requirements		Voting devices comply the FCC requirements related to their intended usage location.	Central system voting devices all have FCC compliant labels. Precinct system voting devices are independently tested by NRTLs to confirm compliance.	hardware-assets/cots-documentation
1.2-J	Power supply from energy service provider	Voting devices located in polling places must be powered by a 120 V, single phase power supply derived from typical energy service providers.		All voting devices are powered by 120V single phase power supply as shown on nameplates.	VotingWorks functional testing confirms all voting devices are properly powered by normal 120V single phase outlets.	Defined on hardware nameplates.
D	Discussion	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.				
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.				
D	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.		VxScan and VxMark comply with Class B emission limits.	VxScan and VxMark are independently tested by NRTLs to confirm compliance.	hardware-assets/tests
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.		N/A - GFCIs are not present		
D	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), 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.)				
1.3	Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not					
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:				
1.3-A.1		requirement(s) under test;				
1.3-A.2		items under test to exercise a given requirement				
1.3-A.3		pass-fail criteria necessary to determine whether or not a requirement has passed the test of conformity to the requirement				
1.3-A.4		evidence (observations, data) expected to provide justification for satisfying or failing a given pass-fail condition				
1.3-A.5		test procedures necessary to provide, observe, record, analyze, and interpret this evidence relative to pass-fail criteria				
1.3-A.6		where applicable, descriptions of the causes of variation, ambiguity, noise, or observed errors in observed and recorded evidence during tested procedures				
1.3-A.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				
1.3-A.8		report of actual tests performed and their results				
1.3-A.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		The Quality Assurance Manual in the TDP, internal testing documents in docs-vxsuite-v4, and this document collectively report on manufacturer-performed tests.	VotingWorks functional and automated testing confirms that each VVSG requirement is met and documented via assets in the TDP.	Quality Assurance Manual
D	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.				
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.		The Quality Assurance Manual in the TDP, internal testing documents in docs-vxsuite-v4, and this document collectively report on manufacturer-performed tests.	VotingWorks functional and automated testing confirms that each VVSG requirement is met and documented via assets in the TDP.	Quality Assurance Manual
D	Discussion	This requirement is to ensure that all requirements identified in the respective implementation and conformance statements are covered by the submitted test-plan.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
2	High Quality Implementation - The voting system is implemented using high quality best practices					
2.1	The voting system and its software are implemented using trustworthy materials and best practices in software development					
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:				
2.1-A.1		sequence				
2.1-A.2		loop with exit condition (for example, for, while, or do-loops)				
2.1-A.3		if/then/else conditional				
2.1-A.4		case conditional				
2.1-A.5		block-structured exception handling (for example, try/throw/catch)				
D	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. 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 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).		The VotingWorks codebase is written in TypeScript and Rust, two widely used languages that have all of the listed control constructs.	We put significant consideration into the introduction of new languages to our codebase.	System Overview > Software Overview > Software Best Practices
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.		N/A - We meet requirement 2.1-A without the need for this extension.		
D	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.				
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.		The VotingWorks codebase is written in TypeScript and Rust, two widely used languages with well established coding conventions. We make use of automatic code linters to enforce these conventions. We also require peer code review of every change. Details about our best practices and tooling used to enforce those best practices can be found here: https://github.com/votingworks/vxsuite/blob/main/docs/best_practices/typescript.md; https://github.com/votingworks/vxsuite/blob/main/docs/best_practices/rust.md	We make use of automatic code linters to enforce best practices and also require peer code review of every change, during which we check for issues like this. If a code linter finds an issue with a code change, our continuous integration tool, CircleCI, fails and prevents the code from being merged until the issue is addressed.	System Overview > Software Overview > Software Best Practices
D	Discussion	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. 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.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
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.		VxSuite hardware can withstand these conditions.	Internal hardware testing has confirmed that our hardware can withstand these conditions.	Quality Assurance; quality-assurance/testing
2.1.1	Workmanship					
2.1.1-A	General build quality	All manufacturers of voting systems must practice proper workmanship by:		VotingWorks employs thorough quality assurance checks on all components and software	VotingWorks tests and iterates on QA checklists until they are thorough enough to capture all issues	Quality Assurance
2.1.1-A.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				
2.1.1-A.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				
2.1.1-B	Durability estimation	A manufacturer must submit a warranty model to the EAC, testing labs, and customers, that includes for each product, its relevant components, and associated consumables:		The documentation includes our warranty model.	VotingWorks staff reviews documentation.	Warranty Model
2.1.1-B.1		estimated replacement rates (e.g., 3 years, 10 years)				
2.1.1-B.2		estimated costs per replacement				
2.1.1-B.3		estimated warranty types and costs				
2.1.1-B.4		associated replacement policies, services, and available maintenance agreements				
2.1.1-B.5		plans for collecting, maintaining, and reporting data to the EAC to support and validate estimates				
D	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).				
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.		VxSuite paper specifications conform with the applicable specifications in GPSS.	VotingWorks staff reviews documentation and compares to applicable standards.	System Performance & Specifications > Paper Ballot Specifications
D	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 different kinds of paper. As of 2020-02-29, the Government Paper Specification Standards, February 1999 No. 11 [GPO19].				
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.		Ink marking devices specified in the User Manual are compatible with paper specified.	VotingWorks functional testing confirms ink specified is compatible with paper specified and has no negative side-effects.	User Manual > Approved Parts
D	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).				
2.1.2	Maintainability					
2.1.2-A	Electronic device maintainability	Electronic devices must exhibit the following physical attributes:				
2.1.2-A.1		labels and the identification of test points				
2.1.2-A.2		built-in test and diagnostic circuitry or physical indicators of condition				
2.1.2-A.3		labels and alarms related to failures				
2.1.2-B	System maintainability	Voting systems must allow for:				
2.1.2-B.1		a non-technician to easily detect that the equipment has failed		VxSuite components detect hardware malfunctions, like disconnected peripherals, and surfaces specific error messages for these cases.	VotingWorks functional and automated testing confirms that each critical hardware failure results in an error message surfaced to the user.	User Manual; User Manual > VxMark Error Messages; User Manual > VxScan Error Messages
2.1.2-B.2		a trained technician to easily diagnose problems		Component diagnostic screens allow for testing and diagnosing problems.	VotingWorks functional and automated testing confirms that diagnostic features allow diagnosing issues.	User Manual > [Component] Diagnostics; System Overview > Diagnostics
2.1.2-B.3		easy access to components for replacement		All subcomponents requiring replacement are easy to access such as: batch scanner rollers; precinct scanner thermal paper; report printer toner; report printer paper.	VotingWorks functional testing confirms that the hardware enables easy access for replacing consumables.	User Manual > System Maintenance
2.1.2-B.4		easy adjustment, alignment, and tuning of components		All scanners can be easily opened for cleaning. The batch scanner paper paths are easily adjustable.	VotingWorks functional testing confirms that the hardware can be easily cleaned or adjusted.	User Manual > System Maintenance
2.1.2-B.5		low false alarm rates (that is, indications of problems that do not exist)		VxSuite components have a low hardware failure false alarm rate.	VotingWorks functional and automated testing confirms that VxSuite components have a low hardware failure false alarm rate.	Quality Assurance
2.1.2-C	Nameplate and labels	All voting devices must:		All VxSuite components have a permanently affixed nameplate. For VxMark & VxScan, this a custom VotingWorks nameplate. For other COTS components, the OEM permanent nameplate meets this requirement.	VotingWorks quality assurance ensures permanent nameplates are present on all voting devices.	System Overview
2.1.2-C.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				
2.1.2-C.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				
2.1.2-C.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				
2.2	The voting system is implemented using best practice user-centered design methods that consider a wide range of representative voters, including those with and without disabilities, and election workers					
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:	8.3-A – Usability tests with voters; 8.4-A – Usability tests with election workers	VotingWorks completed usability and accessibility testing and the report is included in the		
2.1-A.1		a listing of user-centered design methods used				
2.1-A.2		the types of voters and election workers included in those methods				
2.1-A.3		how those methods were integrated into the overall implementation process				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
2.1-A.4		how the results of those methods contributed to developing the final features and design of the voting system		documentation.	VotingWorks staff reviews all documentation.	Usability and Accessibility Test Reports
D	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]•ISO/IEC 25062:2006: Usability test reports [ISO06b] ISO/IEC 25064:2013: User needs report [ISO13b] ISO/IEC 25066:2016 Evaluation report [ISO16]				
2.3	Voting system logic is clear, meaningful, and well-structured					
2.3-A	Block-structured exception handling	Application logic must handle exceptions using block-structured exception handling constructs.		VxSuite application logic handles exceptions using block-structured exception handling contructs in TypeScript and Rust code.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
D	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. 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].				
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.		VotingWorks application logic that calls third-party libraries or hardware drivers is wrapped in callable units that check for relevant error conditions and translate them appropriately.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
D	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 through the use of a COTS package that retrofits block-structured exception handling onto the previous language with minimal changes. While the latter path may at first appear to be less work, it should be noted that many library functions may need to be adapted to throw exceptions when exceptional conditions arise, whereas in a programming environment that had exceptions to begin with the analogous library functions would already do this.				
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.		VotingWorks application logic does not compile or interpret configuration data or other input data as a programming language, and makes sure to properly escape input data to avoid any possible risks like SQL injection.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
D	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 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.				
2.3-D	Hard-coded passwords and keys	Voting system software must not contain hard-coded, including the use of:		VotingWorks application logic does not use or reference any hard coded passwords or cryptographic keys.	We require peer code review of every change, during which we check for issues like this. We have also had external parties conduct penetration tests of our system.	System Overview > Software Overview > Software Best Practices; System Security, Auditing, & Logging > System Security Architecture
2.3-D.1		passwords				
2.3-D.2		cryptographic keys				
D	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].				
2.3.1	Software flow					
2.3.1-A	Unstructured control flow	Application logic must contain no unstructured control constructs.		VotingWorks application logic does not contain any unstructured control constructs. Application logic is written in TypeScript and Rust which are structured languages that do not use unstructured control constructs.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
D	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 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.				
2.3.1-B	Goto	Arbitrary branches (also known as gotos) must not be used.		VotingWorks application logic does not contain any gotos. Application logic is written in TypeScript and Rust which are structured languages that do not support gotos.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
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.		VotingWorks application logic does not use exceptions to redirect the flow of control.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
D	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.				
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.		VotingWorks application logic does not use unstructured exception handling. Application logic is written in TypeScript and Rust which are structured languages that do not support unstructured exception handling.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
D	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 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.				
2.4	Voting system structure is modular, scalable, and robust					
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:		VotingWorks application logic is designed in a modular fashion.	We require peer code review of every change, during which we encourage modular design and appropriate abstractions. For larger changes and features, we hold architecture discussions as a team.	System Overview > Software Overview > Software Best Practices
2.4-A.1		It must be a structural unit of software or analogous logical design.				
2.4-A.2		If it contains callable units, those callable units must be tightly coupled.				
2.4-A.3		Coupling between modules ("inter-module coupling") must:				
2.4-A.3.a		be loose, and				
2.4-A.3.b		occur over defined interfaces.				
2.4-A.4		It must contain all elements needed to compile or interpret successfully.				
2.4-A.5		It must have limited access to data in other modules.				
2.4-A.6		It must be substitutable with another module whose interfaces match the original module.				
D	Discussion	The modularity rules described here apply to the component submodules of a library.				
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.		VotingWorks application logic is written with testability in mind.	Code coverage tooling ensures that our code is thoroughly tested.	Quality Assurance Manual > Quality Assurance Protocols – Software
D	Discussion	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.				
2.4-C	Module size and identification	Modules must be small and easily identifiable, such as being:		VotingWorks application logic is broken up into small digestible modules.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
2.4-C.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				
2.4-C.2		no more than 5% of all callable units SHOULD exceed 60 lines in length				
2.4-C.3		no callable units SHOULD exceed 180 lines in length				
D	Discussion	"Lines," in this context, are defined as executable statements or flow control statements with suitable formatting.				
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.		VotingWorks application logic separates out large data structures and generally avoids large in-code data structures by using SQLite databases.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
D	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.				
2.5	The voting system supports system processes and data with integrity					
2.5-A	Self-modifying code	Application logic must not be self-modifying.		VotingWorks application logic is not self-modifying.	If our code was self-modifying and was somehow modified, our system integrity / Secure Boot checks would fail, and a machine would not boot, alerting us to the issue.	System Security, Auditing, & Logging > System Security Architecture > System Integrity
2.5-B	Unsafe concurrency	Application logic must be free of race conditions, deadlocks, livelocks, and resource starvation.		VotingWorks application logic has no known instances of race conditions, deadlocks, livelocks, or resource starvation.	We write automated tests and perform manual tests to identify concurrency issues.	Quality Assurance Manual > Quality Assurance Protocols – Software > Safe Concurrency
D	Discussion	In addressing this requirement, information should be provided in the TDP describing the means by which safe concurrency was ensured relative to the design, implementation, and testing of the application logic.				
2.5.1	Code Integrity					
2.5.1-A	COTS compilers	If compiled code is used, it must only be compiled using a COTS compiler.		The VotingWorks application is built using the COTS TypeScript and Rust compilers. TypeScript is compiled to JavaScript, which is itself just-in-time compiled by the COTS Chromium and Node.js engines.		System Overview > Software Overview > Software Best Practices

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
D	Discussion	This prohibits the use of arbitrary, nonstandard compilers and, consequently, the invention of new programming languages.				
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.		N/A - VotingWorks application logic does not use any traditionally interpreted languages.		
D	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.				
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.		Our system integrity mechanism prevent this.	If our code was self-modifying and was somehow modified, our system integrity / Secure Boot checks would fail, and a machine would not boot, alerting us to the issue.	System Security, Auditing, & Logging > System Security Architecture > System Integrity
D	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.				
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.		We have multiple layers of protection here: 1) artifact authentication, which prevents modification of records on USB drives, 2) authenticated encryption of the /var partition, which prevents modification of records on disk, including if the drive is removed from the machine, and 3) a strict system user setup that limits which system users have write access.		System Security, Auditing, & Logging > System Security Architecture > Artifact Authentication; System Security, Auditing, & Logging > System Security Architecture > System Integrity > Protecting Critical Read-Write Data; System Security, Auditing, & Logging > System Security Architecture > Defense-in-Depth and Least Privilege
D	Discussion	This requirement can be satisfied through a combination of: the memory protection implemented by most popular COTS operating systems, error checking, and 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.				
2.5.2	Input/output errors					
2.5.2-A	Input validation and error defense	The voting system must:		VotingWorks application logic validates inputs. Inputs that fail validation trigger a warning to the user.	VotingWorks functional and automated testing confirms that I/O operations are validated and failed validation results in a warning.	System Overview > Election Package; System Overview > Cast Vote Records; System Overview > VxAdmin Function; System Security, Auditing, & Logging > Artifact Authentication
2.5.2-A.1		monitor I/O operations				
2.5.2-A.2		validate all input against expected parameters, such as data presence, length, type, format, uniqueness, or inclusion in a set of whitelisted values				
2.5.2-A.3		report any input errors and how they were corrected				
2.5.2-A.4		check information inputs to ensure that incomplete or invalid inputs do not lead to irreversible error.				
D	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.				
2.5.3	Output protection			VotingWorks application logic sanitizes output.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
2.5.3-A	Escaping and encoding output	Software output must be properly encoded, escaped, and sanitized.				
D	Discussion	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].				
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.				
D	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).				
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.				
D	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.				
2.5.4	Error Handling					
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:		VotingWorks application logic performs these checks and exits quickly when these checks fail.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
2.5.4-A.1		common memory management errors, such as out-of-bounds accesses of arrays, strings, and buffers used to manage data				
2.5.4-A.2		uncontrolled format strings				
2.5.4-A.3		CPU-level exceptions such as address and bus errors, dividing by zero, and the like				
2.5.4-A.4		variables that are not appropriately handled when out of expected boundaries				
2.5.4-A.5		numeric and integer overflows				
2.5.4-A.6		validation of array indices				
2.5.4-A.7		known programming language specific vulnerabilities				
D	Discussion	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.				
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.		VotingWorks application logic performs these checks and exits quickly when these checks fail.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
D	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 index do not form a contiguous range, a map structure can be more appropriate than a vector.				
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.		N/A - An overflow will automatically result in an exception.		
2.5.4-D	CPU traps	The application logic must implement such handlers as needed to detect and respond to CPU-level exceptions.		VotingWorks application logic handles CPU-level exceptions.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
D	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.				
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.		VotingWorks application logic performs these checks and exits quickly when these checks fail.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
D	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 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.				
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.		VotingWorks application logic performs these checks and exits quickly when these checks fail.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
D	Discussion	Encapsulate overflow checking as much as possible.				
2.5.4-G	Uncontrolled format strings	Voting system software must not contain uncontrolled format strings.		VotingWorks application logic does not contain uncontrolled format strings.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
D	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].				
2.5.4-H	Recommended 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:				
2.5.4-H.1		pointer variable errors				
2.5.4-H.2		dynamic memory allocation and management errors				
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.		VotingWorks application logic performs these checks and exits quickly when these checks fail.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
D	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.				
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.		TypeScript does not support dynamic memory allocation. Rust does but also has an ownership model that ensures memory safety.		System Overview > Software Overview > Software Best Practices
D	Discussion	Dynamic memory allocation that is fully encapsulated within a standard platform library is treated as COTS software.				
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).		TypeScript does not support dynamic memory allocation. Rust does but also has an ownership model that ensures memory safety.		System Overview > Software Overview > Software Best Practices
D	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.				
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.		VotingWorks application logic performs these checks and exits quickly when these checks fail.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
2.5.4-L.1		An appropriate exception must be thrown				
2.5.4-L.2		Control must pass out of the unit immediately				
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.				
D	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.				
2.5.4-N	SQL injection	The voting system application must defend against SQL injection.		VotingWorks application logic defends against SQL injection.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
D	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].				
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).		VotingWorks application logic uses parameterized queries.	We make use of automatic code linters to enforce best practices and also require peer code review of every change.	System Overview > Software Overview > Software Best Practices
D	Discussion	Parameterized queries are a common defense against this class of software weakness.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
2.6	The voting system handles errors robustly and gracefully recovers from failure					
2.6-A	Surviving device failure	All systems must be capable of resuming normal operation following the correction of a failure:		The VotingWorks system resumes normal operation after recovery from a software or hardware failure.	We make use of automatic code linters to enforce best practices and also require peer code review of every change, during which we audit failure handling and recovery. We also have automated tests and steps during internal manual QA that cover these recovery mechanisms.	System Overview > Software Overview > Software Best Practices > Failure Recovery
2.6-A.1		in any device				
2.6-A.2		in any component (for example, memory, CPU, ballot reader, or printer) provided that catastrophic electrical or mechanical damage has not occurred				
2.6-A.3		in a controlled fashion so that system status can be restored to the initial state existing before the error occurred				
D	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.				
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.		The VotingWorks codebase uses database transactions to ensure that only complete and consistent (and not partial) updates are persisted. For data synced across a machine's internal drive and a connected USB drive, namely CVRs, we detect when data has fallen out of sync after a failure using the Merkle tree hash of the data and re-sync data as needed.	We make use of automatic code linters to enforce best practices and also require peer code review of every change, during which we audit failure handling and recovery. We also have automated tests and steps during internal manual QA that cover these recovery mechanisms.	System Overview > Software Overview > Software Best Practices > Failure Recovery
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.				
D	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.				
2.7	The voting system performs reliably in anticipated physical environments - Requirements in this section deal with voting system reliability with regard to environmental conditions and electrical surges and interference					
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:		VotingWorks internal and external testing as part of quality assurance processes tests the continuous operation across defined ranges and the resistance to electrical disturbances.	VotingWorks internal and external testing as part of quality assurance processes tests the continuous operation across defined ranges and the resistance to electrical disturbances.	Quality Assurance; quality-assurance > testing; User Manual > Operating Environment
2.7-A.1		continuous operation of the voting system under typical environmental conditions				
2.7-A.2		continuous operation of the voting system under varied environmental conditions across defined ranges				
2.7-A.3		resistance of the voting system to electrical surges, interference, and loss of power				
D	Discussion	As with accuracy, reliability cannot be positively ascertained; a judgment of reliability has to 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.				
2.7-B	Continuous operation - typical environment 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.		VotingWorks internal and external testing as part of quality assurance processes tests the continuous operation across defined ranges and the resistance to electrical circumstances.	VotingWorks internal and external testing as part of quality assurance processes tests the continuous operation across defined ranges and the resistance to electrical disturbances.	Quality Assurance; quality-assurance > testing; User Manual > Operating Environment
2.7-C	Continuous operation - varied environment 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.				
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.				
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.				
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.				
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.				
D	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 causing disruption to other devices and people due to electrical emanations from the devices.				
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.		keep the voting system operational for a minimum of two hours.	these components are able to operate on the provided backup power for a minimum of two hours.	System Overview; User Manual > System Inspection; quality-assurance > testing
D	Discussion	Essentially, battery backup must keep the voting system operational so that voting can continue for a minimum of two hours.				
2.7-I	Withstand conducted electrical disturbances	All electronic voting systems must withstand conducted electrical disturbances that affect the power ports of the system.		VotingWorks contracts with NRTLs to confirm VotingWorks manufactured devices can withstand electrical disturbances.	VotingWorks contracts with NRTLs to confirm VotingWorks manufactured devices can withstand electrical disturbances.	quality-assurance > external-testing
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.		VotingWorks contracts with NRTLs to confirm VotingWorks manufactured devices can withstand conducted emissions.	VotingWorks contracts with NRTLs to confirm VotingWorks manufactured devices can withstand conducted emissions.	quality-assurance > external-testing
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).		VotingWorks contracts with NRTLs to confirm VotingWorks manufactured devices can withstand electrostatic discharges.	VotingWorks contracts with NRTLs to confirm VotingWorks manufactured devices can withstand electrostatic discharges.	quality-assurance > external-testing
D	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.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
3	Transparent - The voting system and voting process are designed to provide the transparency					
3.1	The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood					
3.1.1	System overview documentation					
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.				
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.				
D	Discussion	The diagrams could be engineering renderings or photographs.		This documentation is included in System Overview.	VotingWorks staff reviews documentation.	System Overview
3.1.1-C	System description	System overview documentation must include written descriptions and diagrams that present the following, as applicable:				
3.1.1-C.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)				
3.1.1-C.2		a description of the operational environment of the system that provides an overview of the hardware, firmware, software, and communications structure				
3.1.1-C.3		a concept of operations that explains each system function and how the function is achieved in the design				
3.1.1-C.4		descriptions of the functional and physical interfaces between components				
3.1.1-C.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				
3.1.1-C.6		communications (dial-up, network) software				
3.1.1-C.7		interfaces among internal components and interfaces with external systems				
3.1.1-C.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				
3.1.1-C.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				
D	Discussion	The diagrams could be engineering renderings or photographs.		This documentation is included in System Overview	VotingWorks staff reviews documentation.	System Overview
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:				
3.1.1-D.1		written in-house including subcontracted				
3.1.1-D.2		procured as COTS, unmodified				
3.1.1-D.3		procured as COTS and modified, including descriptions of the modifications to the software or firmware and to the default configuration options				
D	Discussion	Full identification would include authorship, version numbers, where procured, and other items to positively identify the COTs or in-house developed software		This documentation is included in System Overview.	VotingWorks staff reviews documentation.	System Overview > Software Overview
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.				
D	Discussion	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.		This documentation is included in System Overview.	VotingWorks staff reviews documentation.	System Overview > Software Overview
3.1.2-A	System performance documentation	The manufacturer must provide system performance documentation that includes:				
3.1.2-A.1		device capacities and limits that were stated in the implementation statement				
3.1.2-A.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				
3.1.2-A.3		quality attributes such as reliability, maintainability, availability, usability, and portability				
3.1.2-A.4		provisions for safety, security, privacy, and continuity of operation				
3.1.2-A.5		design constraints, applicable standards, and compatibility requirements		This documentation is included in System Performances & Specifications.	VotingWorks staff reviews documentation.	System Performance & Specifications
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.				
D	Discussion	The capacity to convert the marks on individual ballots into signals is uniquely important to central count systems.		This documentation is included in System Performances & Specifications.	VotingWorks staff reviews documentation.	System Performance & Specifications > System Limits > Maximum Tabulation Rate
3.1.2-C	Reliably detectable marks	System performance documentation must include, for all types of optical scanners:				
3.1.2-C.1		what constitutes a mark that is tabulatable				
3.1.2-C.2		what constitutes a mark that is ambiguous and may require adjudication				
3.1.2-C.3		what constitutes a marginal mark that would not be tabulatable				
D	Discussion	Marginal marks could include those marks considered as stray or caused by defects or folds on the ballot.		This documentation is included in System Performances & Specifications.	VotingWorks staff reviews documentation.	System Performance & Specifications > Reliably Detectable Marks
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:				
3.1.2-D.1		an explanation regarding the capabilities of the system that were declared in the implementation statement				
3.1.2-D.2		additional capabilities (extensions) must be clearly indicated				
3.1.2-D.3		required capabilities that may be bypassed or deactivated during installation or operation by the user must be clearly indicated				
3.1.2-D.4		additional capabilities that function only when activated during installation or operation by the user must be clearly indicated				
3.1.2-D.5		additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user must be clearly indicated		This documentation is included in System Performance & Specifications.	VotingWorks staff reviews documentation.	System Performance & Specifications > Processing Capabilities
3.1.3	System security documentation					
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.				
D	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, pollworker, etc.		This documentation is included in System Security, Auditing & Logging.	VotingWorks staff reviews documentation.	System Security, Auditing & Logging > System Security Architecture
3.1.3-B	Access control implementation	The system security document must include:				
3.1.3-B.1		guidelines and usage instructions on implementing, configuring, and managing access control capabilities				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
3.1.3-B.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				
3.1.3-B.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				
3.1.3-B.4		information on all privileged accounts included on the voting system				
D	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.		This documentation is included in System Security, Auditing & Logging.	VotingWorks staff reviews documentation.	System Security, Auditing & Logging > System Security Architecture > Access Control; System Overview > User Roles
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.		This documentation is included in System Security, Auditing & Logging.	VotingWorks staff reviews documentation.	System Security, Auditing & Logging > Physical Security; System Security, Auditing & Logging > Procedural and Operational Security
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.		This documentation is included in System Security, Auditing & Logging.	VotingWorks staff reviews documentation.	System Security, Auditing & Logging > Audit Procedure
3.1.4	Software installation documentation					
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.				
D	Discussion	Software to be installed on programmed devices of the voting system includes executable code, configuration files, data files, and election specific software.		This documentation is included in Software Installation.	VotingWorks staff reviews documentation.	Software Installation
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:				
3.1.4-B.1		software product name				
3.1.4-B.2		software version number				
3.1.4-B.3		software manufacturer name				
3.1.4-B.4		software manufacturer contact information				
3.1.4-B.5		type of software (application logic, border logic, third party logic, COTS software, or installation software)				
3.1.4-B.6		list of software documentation				
3.1.4-B.7		component identifiers (such as filenames) of the software, and type of software component (executable code, source code, or data)				
3.1.4-B.8		flag to indicate whether or not 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)		This documentation is included in Software Installation.	VotingWorks staff reviews documentation.	Software Installation
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.				
D	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.		N/A - software installation process writes over the entire disk. This is explained in Software Installation.	VotingWorks staff reviews documentation.	Software Installation
3.1.4-D	Election specific software identification	Software installation documentation must identify election specific software in the user documentation.				
D	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 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).		N/A - there is no election specific software. This is explained in Software Installation.	VotingWorks staff reviews documentation.	Software Installation
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.		This documentation is included in Software Installation.	VotingWorks staff reviews documentation.	Software Installation
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.		This documentation is included in Software Installation.	VotingWorks staff reviews documentation.	Software Installation
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.		This documentation is included in Software Installation.	VotingWorks staff reviews documentation.	Software Installation > Trusted Build
3.1.4-H	Programmed device configuration replication	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.				
D	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 mechanisms for installation and signature verification provided, signed, and validated from the beginning.		This documentation is included in Software Installation.	VotingWorks staff reviews documentation.	Software Installation
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:	3.1.4-H - Programmed device configuration replication			
3.1.4-I.1		a unique identifier (such as a serial number) for the record				
3.1.4-I.2		a list of unique identifiers of storage media associated with the record				
3.1.4-I.3		the time, date, and location of the software installation				
3.1.4-I.4		names, affiliations, and signatures of all people present				
3.1.4-I.5		copies of the procedures used to install the software on the programmed devices of the voting system				
3.1.4-I.6		the certification number of the voting system				
3.1.4-I.7		list of the software installed as well as associated digital signatures and mechanisms for installation and verification on programmed devices of the voting system				
3.1.4-I.8		a unique identifier (such as a serial number) of the vote-capture device or election management system (EMS) which the software is installed				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
D	Discussion	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 have 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.		This documentation is included in Software Installation.	VotingWorks staff reviews documentation.	Software Installation
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.		This documentation is included in Software Installation.	VotingWorks staff reviews documentation.	Software Installation > Trusted Build
3.1.4-K	Open market procurement of COTS software	Software installation documentation must include that COTS software be obtained from the open market.		This documentation is included in Software Installation.	VotingWorks staff reviews documentation.	Software Installation > Trusted Build
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.				
D	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.		This documentation is included in Software Installation.	VotingWorks staff reviews documentation.	Software Installation
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.	3.1.4-H – Programmed device configuration replication; 3.1.4-I – Software installation record creation			
D	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.		This documentation is included in Software Installation.	VotingWorks staff reviews documentation.	Software Installation
3.1.5	System operations documentation					
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:		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual
3.1.5-A.1		provide a detailed description of procedures required to initiate, control, and verify proper system operation		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual
3.1.5-A.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)		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual
3.1.5-A.3		provide procedures that clearly enable the administrator to intervene in system operations to recover from an abnormal system state		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > VxScan Error Messages; User Manual > VxMark Error Messages
3.1.5-A.4		define and illustrate the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Configure [Component]
3.1.5-A.5		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.)		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual
3.1.5-A.6		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		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual
3.1.5-A.7		support successful election definition and software installation and control by central election officials		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Configure [Component]
3.1.5-A.8		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		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Checklists
3.1.5-A.9		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		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > [Component] Diagnostics
D	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.				
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Smart Cards and User Roles
3.1.5-E	Conditional actions	The operations document must describe decision criteria and conditional operator functions such as error and failure recovery actions.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual
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:				
3.1.5-G.1		environmental protection				
3.1.5-G.2		electrical service				
3.1.5-G.3		recommended auxiliary power				
3.1.5-G.4		telecommunications service				
3.1.5-G.5		any other facility or resource required for the proper installation and operation of the system		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Operational Environment
3.1.5-H	Readiness testing	The operations document must include specifications for testing system installation and readiness.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > [Component] Diagnostics
D	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.				
3.1.5-I	Features	The operations document must include documentation of system operating features that includes:		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual
3.1.5-I.1		detailed descriptions of all input, output, control, and display features accessible to the operator or voter		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual
3.1.5-I.2		examples of simulated interactions to facilitate understanding of the system and its capabilities		The user manual uses screenshots and images to simulate user flows.	VotingWorks staff reviews documentation.	User Manual
3.1.5-I.3		sample data formats and output reports		The user manual includes sample reports for common exports. For greater detail on VxAdmin reports, which are too numerous to enumerate in the user manual, see VxAdmin Result Exports in the System Overview	VotingWorks staff reviews documentation.	User Manual; System Overview > VxAdmin Results Exports
3.1.5-I.4		illustration and description of all status indicators and information messages		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
3.1.5-J	Support	The operations document must include documentation of system operating procedures that:		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual
3.1.5-J.1		describes procedures for providing technical support, system maintenance, and correction of defects, and for incorporating hardware upgrades and new software releases		The user manual describes what maintenance is expected of the end user and what should be escalated to VotingWorks.	VotingWorks staff reviews documentation.	User Manual
3.1.5-J.2		defines the procedures required to support system installation and readiness testing		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > [Component] Diagnostics
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:		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual
3.1.5-K.1		shipment		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > [Component] Hardware Setup; User Manual > Operational Environment
3.1.5-K.2		storage		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Operational Environment
3.1.5-K.3		archiving information		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Retaining & Removing Files
3.1.6	System maintenance documentation					
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.				
D	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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
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 recording, tabulation, and reporting in sufficient detail to provide an overview of the system for maintaining and identifying faulty hardware or software.		Documentation is included in the user manual and contains links to the system overview when additional context is needed.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
3.1.6-D	Equipment overview details	Maintenance documentation must include a concept of operations that fully describes such items as:				
3.1.6-D.1		electrical and mechanical functions of the equipment				
3.1.6-D.2		for paper-based systems, how ballot handling and reading processes are performed				
3.1.6-D.3		for electronic vote-capture devices, how vote selection and ballot casting are performed				
3.1.6-D.4		how data transmission over a network is performed (if applicable)				
3.1.6-D.5		how data are handled in memory units				
3.1.6-D.6		how data output is initiated and controlled				
3.1.6-D.7		how power is converted or conditioned				
3.1.6-D.8		how test and diagnostic information is acquired and used				
D	Discussion	The documentation should indicate how and when information is written from volatile to non-volatile memory, including redundant storage.		Documentation is included in the user manual and contains links to the system overview when additional context is needed.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
3.1.6-E	Maintenance procedures	Maintenance documentation must include preventive and corrective maintenance procedures for hardware, firmware, and software.		Documentation is included in the user manual for corrective hardware maintenance procedures. End users are not responsible for software or firmware maintenance procedures.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
3.1.6-F	Preventive maintenance procedures	Maintenance documentation must identify and describe:		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
3.1.6-F.1		all required and recommended preventive maintenance tasks, including software and data backup, database performance analysis, and database tuning		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
3.1.6-F.2		the number and skill levels of personnel required for each task		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
3.1.6-F.3		the parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Approved Parts
3.1.6-F.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)		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
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:		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > System Maintenance; User Manual > [Component] Diagnostics
3.1.6-G.1		steps to replace failed or deficient equipment		The end user is not responsible for replacing failed or deficient equipment.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
3.1.6-G.2		steps to correct deficiencies or faulty operations in software or firmware		The end user is not responsible for correcting faulty software or firmware.		
3.1.6-G.3		modifications that are necessary to coordinate any modified or upgraded software or firmware with other modules		The end user is not responsible for correcting faulty software or firmware.		
3.1.6-G.4		number and skill levels of personnel needed to accomplish each procedure		The necessary roles or skill level are called out in the documentation.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
3.1.6-G.5		special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Approved Parts
3.1.6-G.6		any coordination required with the manufacturer, or other party, for COTS		Situations that require escalating to VotingWorks are called out in the documentation.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
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.		There is no special purpose test or maintenance equipment required.		
3.1.6-I	Parts and materials	Maintenance documentation must include detailed documentation of parts and materials needed to operate and maintain the system.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Supply List; User Manual > Approved Parts
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:				
3.1.6-J.1		type				
3.1.6-J.2		size				
3.1.6-J.3		value or range				
3.1.6-J.4		manufacturer's designation				
3.1.6-J.5		individual quantities needed				
3.1.6-J.6		sources from which they may be obtained		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Supply List; User Manual > Approved Parts
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Approved Parts
D	Discussion	Includes pens or pencils and possibly a compatible ballot marking device (BMD).				
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Approved Parts

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
3.1.6-M	Ballot stock specification	Maintenance documentation must:				
3.1.6-M.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		Documentation is included in the technical data package.	VotingWorks staff reviews documentation.	System Performance Specifications > Paper Ballot Specifications
3.1.6-M.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		Documentation is included in the technical data package.	VotingWorks staff reviews documentation.	System Overview > Hand Marked Ballots
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.		Documentation is included in the technical data package.	VotingWorks staff reviews documentation.	System Performance Specifications > Paper Ballot Specifications
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > System Maintenance; System Performance Specifications > Paper Ballot Specifications
D	Discussion	This requirement covers all printers, either stand-alone or integrated with another device, regardless whether they are used for reporting, for logging, for voter verified paper records (VVPR), etc.				
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
3.1.6-Q	System maintenance, maintenance support and spares	Maintenance documentation must identify:				
3.1.6-Q.1		recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation				
3.1.6-Q.2		recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation				
3.1.6-Q.3		organizational affiliation (for example, jurisdiction, manufacturer) of qualified maintenance personnel		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > System Maintenance
3.1.7	Training Documentation					
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Smart Cards and User Roles
3.1.7-B	Personnel	The manufacturer must specify the number of personnel and skill levels required to perform each of the following functions:				
3.1.7-B.1		pre-election or election preparation functions (such as, entering an election, contest and candidate information, designing a ballot, and generating pre-election reports)				
3.1.7-B.2		system operations for voting system functions performed at the polling place				
3.1.7-B.3		system operations for voting system functions performed at the central count facility				
3.1.7-B.4		preventive maintenance tasks				
3.1.7-B.5		diagnosis of faulty hardware, firmware, or software				
3.1.7-B.6		corrective maintenance tasks				
3.1.7-B.7		testing to verify the correction of problems		When tasks are described in the user manual, the necessary role (implying skill level) is indicated.	VotingWorks staff reviews documentation.	User Manual
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.		The user manual indicates when issues must be escalated to VotingWorks.	VotingWorks staff reviews documentation.	User Manual
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Smart Cards and User Roles
3.2	The process and transactions, both physical and digital, associated with the voting system are readily available for inspection					
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection
D	Discussion	The setup inspection process provides a means to inspect various properties of voting devices as needed during the election process.				
3.2-B	Minimum properties included in the setup inspection process	Setup inspection process documentation must at a minimum include:				
3.2-B.1		inspecting voting system software		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection
3.2-B.2		inspecting storage locations that hold election information that changes during an election		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection
3.2-B.3		inspecting other voting device properties		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection
3.2-B.4		executing logic and accuracy testing related to readiness of use in an election		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Logic & Accuracy Pre-Election Testing
3.2-C	Setup inspection record generation	Setup inspection process documentation must describe the records that result from performing the setup inspection process.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection; User Manual > [Component] Diagnostics
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection; User Manual > Signed Hash Validation
D	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.				
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection; User Manual > Signed Hash Validation
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection
3.2-L	Communications operational status inspection procedure	Setup inspection process documentation must include the procedures to inspect the operational status of the communications capabilities of the voting device.		N/A - There are no communications capabilities.		
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.		N/A - There are no communications capabilities.		
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection; User Manual > Supply List; User Manual > Approved Parts

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
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.		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection
3.2-P	Calibration of voting device components	Setup inspection process documentation must include:				
3.2-P.1		a list of components associated with the voting device that require calibration				
3.2-P.2		the nominal operating ranges for each component				
3.2-P.3		the procedures to inspect the calibration of each component				
3.2-P.4		the procedures to adjust the calibration of each component		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection
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:				
3.2-Q.1		a description of the risks of not performing each documented inspection				
3.2-Q.2		power sources				
3.2-Q.3		cabling for communications				
3.2-Q.4		capabilities				
3.2-Q.5		consumables				
3.2-Q.6		calibration of voting device components				
3.2-Q.7		general physical features of the voting device				
3.2-Q.8		securing external interfaces of the voting device not being used		Documentation is included in the user manual.	VotingWorks staff reviews documentation.	User Manual > Setup Inspection
3.3	The public can understand and verify the operations of the voting system throughout the entirety of the election					
3.3-A	System security, system event logging	Manufacturers must provide publicly available documentation that:				
3.3-A.1		describes system event logging capabilities and usage				
3.3-A.2		fully documents the log format information				
D	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.				
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:				
3.3-B.1		descriptions of how elements and attributes are used				
3.3-B.2		constraints on data elements				
3.3-B.3		extensions as well as any constraints				
D	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].				
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.				
D	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.				
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.				
D	Discussion	Codes that represent a voter's ballot selections are commonly used within barcodes and CVRs so as 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 includes other information within the barcode generally found on clear-text ballots to identify the ballot style.		All VotinWorks documentation is public. This specific documentation is also available in Public Documents.	VotingWorks staff reviews documentation.	Public Documents

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
4	Interoperable - The voting system is designed to support interoperability in its interface to external systems, its interfaces to internal components, its data, and its peripherals					
4.1	Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.					
4.1-A	Election programming data input and output	The voting system must include support for CDF specification(s) regarding:				
4.1-A.1		import and export of election programming data				
4.1-A.2		import and export of ballot programming data.				
D	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].		VotingWorks supports importing and exporting election definition data in the ballot definition CDF.	VotingWorks functional and automated testing confirms all functionality performs as expected when using definitions in the publicly available format.	System Overview > Ballot Definition CDF
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.				
D	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].		VotingWorks supports importing and exporting election result data in the election results reporting CDF.	VotingWorks functional and automated testing confirms that election results can be exported and imported in the ERR CDF.	System Overview > VxAdmin Results Exports > CDF ERR Export
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).				
D	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].		VotingWorks tabulators export CVRs in the CDF and VxAdmin imports CDF CVRs.	VotingWorks functional and automated testing confirms that the CVR CDF can be exported and imported as expected.	System Overview > Cast Vote Records
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.				
D	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].		VotingWorks devices can export logs in the CDF.	VotingWorks functional and automated testing confirms all log data can be exported in the CDF.	System Security, Auditing and Logging > Logging
4.1-E	Voting device event code documentation	Manufacturers must provide a publicly available specification for event codes used in their equipment.				
D	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.		All logs are publicly documented.	VotingWorks functional and automated testing confirms logs are exported in the publicly documented format.	System Security, Auditing and Logging > Logging
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.				
D	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.		All CDF implementation specifications are publicly available.	VotingWorks functional and automated testing confirms that all functions perform as expected per publicly available specifications.	Public Documents
4.2	Standard, publicly available formats for other types of data not addressed by CDF specifications are used					
4.2-A	Standard formats	Publicly available non-proprietary formats must be used, where possible, for exchanging data.				
D	Discussion	Examples include the use of common data encodings such as bar or QR codes.		All barcode encoding is publicly available.	testing confirms that all functions perform as expected per publicly available specifications.	Public Documents
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.				
D	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.		All barcode encoding is publicly available.	VotingWorks functional and automated testing confirms that all functions perform as expected per publicly available specifications.	Public Documents
4.3	Widely-used hardware interfaces and communications protocols are used					
4.3	Interfaces and Communication Protocols					
4.3-A	Standard device interfaces	Standard, common hardware interfaces and protocols must be used to connect devices.				
D	Discussion	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.		All interfaces between devices are over USB.	VotingWorks functional testing confirms all functions perform as expected between device interfaces over USB.	System Overview
4.4	Commercial-off-the-shelf (COTS) devices can be used if they meet all applicable VSG requirements					
4.4-A	COTS devices meet applicable requirements	COTS devices, if used, must satisfy all applicable VVSG requirements.				
D	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.		All COTS devices meet all applicable VVSG requirements.	VotingWorks functional testing confirms all COTS devices meet all applicable VVSG requirements.	System Overview > [Component] Hardware

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
5	Equivalent and Consistent Voter Access - All voters can access and use the voting system regardless of their abilities					
5.1	Voters have a consistent experience throughout the voting process within any method of voting					
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.				
D	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. 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].		All interaction modes on VxMark have access to the same functionality as visual-touch.	VotingWorks functional and automated testing confirms that the same voting, verification, and casting functionality is available in all interaction modes on VxMark.	System Overview > VxMark Function
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.				
D	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].		All voter facing material is translated for additional languages.	VotingWorks functional testing confirms that all voter facing material is translated for non-English languages in a given election package.	System Performance & Specifications > Supported Languages
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.				
D	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 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.		All voter-verifiable paper ballots have voter selections presented in English even when the primary ballot language is translated to a non-English language.	VotingWorks functional testing confirms that all non-English voter verifiable ballots have English values for auditing purposes.	System Overview > Machine Marked Ballots
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.	6.1-B - Warnings			
D	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].		VxMark provides support for visual-touch, audio-tactile, and limited-dexterity interaction modes for marking, verifying, and casting a ballot.	VotingWorks functional testing confirms that accessibility features are supported throughout the voter experience on VxMark.	System Overview > VxMark Function
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.	7.1-I - Text size (paper)			
D	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].		VxMark plays the values interpreted from the voter-verifiable paper ballot scan over headphones when a voter is confirming their ballot selections in the audio-tactile interaction mode.	VotingWorks functional and automated testing confirms that the values played over headphones in audio-tactile mode are the same selections as the interpreted from the voter-verifiable paper ballot scan on VxMark.	System Overview > VxMark Function
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:	7.3-N - Instructions for voters; 7.3-O Instructions for election workers			
5.1-F.1		recommended procedures that fully implement accessibility for voters with disabilities				
5.1-F.2		how the voting system supports those procedures				
D	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].		The user manual provides instructions for voters & election workers for all accessibility features.	VotingWorks functional testing confirms that all accessibility features are documented in the user manual.	User Manual > VxMark
5.2	Voters receive equivalent information and options in all modes of voting					
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.				
D	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.		All ballot options are presented in an equivalent manner for a given interaction mode / voter setting on VxMark.	VotingWorks functional and automated testing confirms that all ballot options on VxMark are presented in an equivalent manner for a given interaction mode or voter setting.	System Overview > VxMark Function
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.				
D	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].		All voter facing material is translated for additional languages.	VotingWorks functional testing confirms that all voter facing material is translated for non-English languages in a given election package.	User Manual > VxMark; System Performance and Specifications > Supported Languages
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.				
D	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].		All voter information is presented in all display formats and interactions modes.	VotingWorks functional and automated testing confirms that all voter information is presented in all display formats and interaction modes.	User Manual > VxMark
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.		The audio over headphones in the VxMark audio-tactile interaction mode conveys the same		

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
D	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].		information that is displayed visually to the voter. Some additional content presented over headphones to guide the user in the audio-tactile interface.	VotingWorks functional testing confirms that the audio in audio-tactile mode is synchronized with the visual interface.	User Manual > VxMark
5.2-E	Sound cues	Sound and visual cues must be coordinated so that:				
5.2-E.1		sound cues are accompanied by visual cues unless the system is set to audio-only				
5.2-E.2		visual cues are accompanied by sound cues unless the system is set to visual-only				
D	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].		Audio and visual cues are synced with the exception of when audio or visual-only mode is set by a voter in the voter settings.	VotingWorks functional testing confirms that audio and visual cues are synced with the exception of when VxMark is in audio or visual only mode.	User Manual > Voting Session Language & Settings; System Overview > VxMark Function
5.2-F	Presenting 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.				
D	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].		A voter may change any voter facing settings during a voting session on VxMark and all voting state is preserved.	VotingWorks functional testing confirms that voter session state is preserved when changing voter facing settings.	User Manual > Voting Session Language & Settings; System Overview > VxMark Function

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
6	Voter Privacy - Voters can mark, verify, and cast their ballot privately and independently					
6.1	The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections					
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.		A privacy shield is built into VxMark hardware. When using hand-marked paper ballots, it is expected that jurisdictions implement procedures at the polling place to preserve privacy in marking of the ballot and its transfer to VxScan for casting.	VotingWorks functional testing confirms that voter privacy is preserved when following procedural guidance.	System Overview > VxMark Hardware; User Manual > VxMark Hardware Setup
D	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 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].	7.2-F - Voter speech			
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.	7.3-K - Warnings, alerts, and instructions	Overvote and undervote notifications on VxScan do not present voter selections, only contest names.	VotingWorks functional and automated testing confirm that no voter selections are shown on screen for undervote or overvote warnings on VxScan.	User Manual > Assisting Voters
D	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.				
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.	7.2-A - Display and interaction options; 7.3-K - Warnings, alerts, and instructions	Voters on VxMark can independently navigate to settings that enable or disable audio or visual-only modes.	VotingWorks functional testing confirms that a voter can mute audio (visual-only) or hide visual presentation of the voter session (audio-only) on VxMark.	User Manual > Voting Session Language & Settings
D	Discussion	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].				
6.1-D	Audio privacy	Audio during the voting session must be audible only to the voter.	7.2-F - Voter speech; 8.1-J - Hearing aids	Headphones supplied with VxMark prevent sound leakage.	VotingWorks performs sound leakage tests when calibrating headphone volume to confirm only a voter can hear voting session audio.	System Overview > VxMark Hardware
D	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].				
6.2	Voters can mark, verify, and cast their ballot or other associated cast vote record without assistance from others.					
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.	2.2-A - User-centered design process; 5.1-D - Accessibility features; 5.1-E - Reading paper ballots; 8.2-A - Federal standards for accessibility	Using VxMark, voters can mark, verify and cast ballots privately and independently in all interaction modes: visual-touch, audio-tactile and limited-dexterity.	VotingWorks functional testing confirms that all interaction modes support marking, verifying, and casting of a ballot privately and independently using VxMark.	System Overview > VxMark Function
6.2-A.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.		N/A - no E2E verifiable system		
D	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.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
7	Marked, Verified, and Cast as Intended - Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters					
7.1	The default voting system settings present a ballot usable for the widest range of voters, and voters can adjust settings and preferences to meet their needs.					
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.	7.1-K - Audio settings	All voter settings are reset when the voting session ends on both VxMark & VxScan.	VotingWorks functional testing confirms all voter settings are reset after voting sessions end.	System Overview > VxMark Function; System Overview > VxScan Function
D	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				
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.	5.2-F - Preserving votes	All voter interface settings can be restored while preserving the state of a voter session by clicking "Reset" in the voter settings.	VotingWorks functional testing confirms that all voter session state is maintained when voter interface settings are reset.	User Manual > Voting Session Language & Settings
D	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, but still keeping what was selected thus far. Applies to: Electronic interfaces				
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.		The default contrast ratio is >= 10:1 for all elements.	VotingWorks functional & automated testing confirms that contrast ratios are maintained for all visual elements shown on screen.	System Overview > VxMark Function
7.1-C.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.				
7.1-C.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.				
D	Discussion	For example, this applies to: candidate names, 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				
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:		All voter facing screens (VxMark & VxScan) provide the ability to select alternative display contrast options that meet all these requirements.	VotingWorks automated testing confirms that contrast ratios are maintained for all contrast modes.	System Overview > VxMark Function; System Overview > VxScan Function
7.1-D.1		A high contrast option with a white background and dark text, with a luminosity contrast ratio of at least 20:1.				
7.1-D.2		A high contrast option with a black background (between #000000 and #111111) and one of the following foreground options, including:				
7.1-D.2.a		yellow text similar to #FFFF00, providing a contrast ratio of at least 17.5:1				
7.1-D.2.b		cyan text similar to #00FFFF, providing a contrast ratio of at least 15:1				
7.1-D.2.c		white text similar to #FAFAFA, providing a contrast ratio of at least 18:1				
7.1-D.3		A low contrast option, providing a contrast ratio in the range of 4.5:1 to 8:1				
D	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 a 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]. Applies to: Electronic interfaces				
7.1-E	Color conventions	The use of color by the voting system must follow these common conventions:		The use of color follows these conventions.	VotingWorks functional testing confirms that the use of color follows these conventions.	User Manual; System Overview > VxMark Function
7.1-E.1		Green, blue, or white is used for general information or as a normal status indicator				
7.1-E.2		Amber or yellow is used to indicate warnings or a marginal status				
7.1-E.3		Red is used to indicate error conditions or a problem requiring immediate attention				
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.		Text and iconography is used to convey information in addition to color.	VotingWorks functional testing confirms that color coding is not the only means of conveying information on screen.	User Manual; System Overview > VxMark Function
D	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].				
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 (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:	5.2-A - No bias; 5.2-F - Preserving votes; 7.2-D - Scrolling; 7.3-B - No split contests	VxMark and VxScan provide four discrete sizes that fall in these ranges.	VotingWorks functional testing confirms that these four settings sizes map to the expected mm size ranges on screen.	System Overview > VxMark Function; System Overview > VxScan Function
7.1-G.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				
7.1-G.2		Provide at least four discrete text sizes, in which the main ballot options fall within one of these ranges				
7.1-G.2.a		3.5-4.2 mm (10-12 points)				
7.1-G.2.b		4.8-5.6 mm (14-16 points)				
7.1-G.2.c		6.4-7.1 mm (18-20 points)				
7.1-G.2.d		8.5-9.0 mm (24-25 points)				
D	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. 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				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
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.	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; 7.1-G - Text size (electronic display); 7.2-D - Scrolling.			
7.1-H.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				
7.1-H.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				
D	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		All other information in the interface scales when text sizes are changed on screen on VxScan & VxMark.	VotingWorks functional testing confirms that all other information scales on screen when text sizes are changed.	System Overview > VxMark Function; System Overview > VxScan Function
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).	5.1-E - Reading paper ballots; 7.1-G - Text size (electronic display)	Paper ballots printed from VxMark have a default font size for voter selections of at least 3.5 mm. Hand marked paper ballot design can be performed outside of the system, but the system is capable of interpreting ballots with this minimum size.		
D	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			VotingWorks functional testing confirms paper ballots meet this minimum font size by manually measuring the height of an uppercase I.	System Overview > Machine Marked Ballots
7.1-J	Sans-serif font	The voting system must be capable of presenting text intended for the voter in a sans-serif font.				
D	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.		VxSuite font is Roboto, a sans-serif font.	VotingWorks functional and automated testing confirm all font is Roboto.	User Manual
7.1-K	Audio settings	The voting system's audio format interface must meet the following requirements:	7.1-A - Reset to default settings			
7.1-K.1		The settings for volume and rate of speech are followed regardless of the technical means of producing audio output				
7.1-K.2		The default volume for each voting session is set between 60 and 70 dB SPL.				
7.1-K.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.				
7.1-K.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.				
7.1-K.5		The default rate of speech is 120 to 125 words per minute (wpm).				
7.1-K.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.				
7.1-K.7		Adjusting the rate of speech does not affect the pitch of the voice		The VxMark audio interface meets all these requirements when using the system specified headphones. Rate of speech and volume is controlled in steps and increments as specified when using the attached accessible controller on VxMark.		
D	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].			VotingWorks functional testing confirms that audio volume & rate of speech meet these requirements when changing settings by using sound meters and measuring the words per minute.	System Overview > VxMark Function
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.		The headphones supplied with VxMark have a frequency range that reproduces frequencies over the audible speech range.		
D	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].			VotingWorks functional testing confirms the audible speech range is reproduced with the provided VxMark headphones.	System Overview > VxMark Hardware
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:				
7.1-M.1		proper enunciation, normal intonation, accurate pronunciation in the context of the information, and the capability to pronounce candidate names as intended				
7.1-M.2		low background noise				
7.1-M.3		recording or reproduction in dual-mono, with the same audio information in both ears				
D	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].		The election package supports any audio recording source for audio files imported into the system. VotingWorks internal tooling utilizes Google Cloud text-to-speech speech synthesis.	VotingWorks functional testing confirms that voter information presented over headphones on VxMark is accurately presented with low background noise and reproduction in dual mono.	System Overview > Election Package; System Overview > VxMark Function
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:	7.2-E - Touch screen gestures; 7.2-H - Accidental activation; 7.2-R - Control labels visible; 7.3-L - Icon labels			
7.1-N.1		be tactilely discernible without activating those controls or keys		The attached accessible controller on VxMark has tactilely discernible buttons (such as arrow keys) and includes braille labels. It		
7.1-N.2		include a Unified English Braille, Contracted label if there is a text label				
7.1-N.3		not require sequential, timed, or simultaneous presses or activations, unless using a full keyboard				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
D	Discussion	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].		does not require any sequential, timed, or simultaneous activations.	VotingWorks usability and accessibility testing confirms that a blind voter can operate the voting system by feel alone.	System Overview > VxMark Hardware; Usability and Accessibility
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.		N/A - these types of locking/toggle/keys do not exist in VxSuite.		
D	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].				
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.		All buttons on screen and in hardware are distinguishable by shape and color. A full alphabetic keyboard is used for write-in candidate entry.	VotingWorks functional testing confirms all voter facing controls are discernable by shape and color.	User Manual
D	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. 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].				
7.2	Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes					
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:	5.1-A - Voting methods and interaction modes; 5.2-A - No bias	All marking, verifying, and casting functionality on VxMark is supported in these display formats and interaction modes.	VotingWorks functional testing confirms marking, verifying, and casting is supported in all display formats and interaction modes.	System Overview > VxMark Function; User Manual > Voting Session Language & Settings
7.2-A.1		Visual format				
7.2-A.2		Enhanced visual format				
7.2-A.3		Audio format				
7.2-A.4		Touch mode				
7.2-A.5		Limited dexterity mode				
D	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. 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].				
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.	7.2-A - Display and interaction options	A voter on VxMark can navigate back and forth in all interaction modes without completing their vote.	VotingWorks functional testing confirms that voters may navigate back and forth across contests without completing votes for a given contest in all interaction modes.	System Overview > VxMark Function; User Manual > Voting Sessions
D	Discussion	For example, voters are not forced to proceed sequentially through all contests before going back to check their votes within a previous contest. 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.				
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:	7.2-A - Display interaction options; 7.3-E - Feedback; 7.3-F - Correcting the ballot	VxMark gives voters direct control over making or changing selections per these requirements.	VotingWorks functional and automated testing confirms VxMark navigation adheres to these requirements.	System Overview > VxMark Function; User Manual > Voting Sessions
7.2-C.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.				
7.2-C.2		In a vote-for-N-of-M contest, the system must not deselect any candidate automatically.				
7.2-C.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.				
7.2-C.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.		N/A - voting variation not supported		
7.2-C.5		Ballots with preferential or ranking voting methods must not re-order candidates except in response to an explicit voter command.		N/A - voting variation not supported		
D	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. 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.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
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.	7.1-G - Text size (electronic display); 7.1-H - Scaling and zooming (electronic display); 7.2-E - Touch screen gestures; 7.2-F - Voter speech; 7.2-H - Accidental activation; 7.2-I - Touch area size; 7.3-B - No split contests; 7.3-E - Feedback; 7.3-F - Correctin gthe ballot; 7.3-H - Overvotes; 7.3-I - Undervotes; 7.3-K - Warnings, alerts, and instructions			
7.2-D.1		The voting system may display the contest by:				
7.2-D.1.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				
7.2-D.1.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.				
7.2-D.2		For either display method, the voting system interface must:				
7.2-D.2.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				
7.2-D.2.b		include easily perceivable cues in every display format to indicate that there is more information or there are more contest options available				
7.2-D.2.c		include an option for an audio format and visual format that sync during scrolling				
7.2-D.3		The navigation method must ensure that the voting system:				
7.2-D.3.a		meets all requirements for providing feedback to the voter				
7.2-D.3.b		accurately issues all warnings and alerts including notifications of undervotes and overvotes				
7.2-D.3.c		meets all requirements for control size and interaction, and keeping all controls visible				
7.2-D.3.d		does not rely only on conventional platform scroll bars				
7.2-D.3.e		provides an opportunity to review and correct selections before leaving the contest				
D	Discussion	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. 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		If the content does not fit on a single screen for a given display setting, VxSuite presents a "more" button to scroll through the content.	VotingWorks functional and automated testing confirms that the "more" button is presented when content does not fit on a single screen.	System Overview > VxMark Function
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:	7.1-N - Tactile keys; 7.2-H - Accidental activation			
7.2-E.1		Gestures are offered as another way of interacting with a touch screen and an optional alternative to the other touch interactions.				
7.2-E.2		Gestures work consistently across the entire voting interaction.				
7.2-E.3		Gestures do not include navigation off the current contest.				
7.2-E.4		Gestures are used in a way that does not create accidental activation of an action through an unintended gesture				
7.2-E.5		Gestures are limited to simple, well-known gestures				
7.2-E.6		Gestures do not require sequential, timed or simultaneous actions				
D	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. 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		Swiping to scroll is the supported touch screen gesture and it meets these conditions.	VotingWorks functional testing confirms that scrolling meets these conditions.	System Overview > VxMark Function
7.2-F	Voter speech	If the voting system includes speech or human sounds as a way for voters to control the system:	6.1-A - Preserving privacy for voters; 6.1-D - Audio privacy			
7.2-F.1		it must not require the voter to speak recognizable voting selections out loud				
7.2-F.2		speech input must not be the only non-visual interaction mode				
D	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.		N/A - the voting system does not support speech or human sounds as a way for voters to control the system.		
7.2-G	Voter control of audio	The voting system must allow the voter to control the audio format including:				
7.2-G.1		pausing and resuming the audio				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
7.2-G.2		repeating any information		VxMark audio tactile interface supports all these audio controls and provides instructions as to how to use these controls at the start of a voting session.	VotingWorks functional testing confirms that audio format controls control audio as expected and instructions as to how to use them are presented to the voter.	System Overview > VxMark Function > Audio Format
7.2-G.3		skipping to the next or previous contest				
7.2-G.4		skipping over the reading of the ballot question text				
D	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				
7.2-H	Accidental activation	Both on-screen and physical controls on the voting system must be designed to prevent accidental activation.	7.1-N - Tactile keys; 7.2-E - Touch screen gestures	Placement and sensitivity of all controls are designed to prevent accidental activation.	VotingWorks functional and usability testing confirms that no controls can be accidentally activated.	System Overview > VxMark Function
D	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. 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.				
7.2-I	Touch area size	If the voting system has a touch screen, the touch target areas must:		All touch size areas on touch screens meet these size requirements.	VotingWorks functional and automated testing confirms touch size areas meet these size requirements.	System Overview > VxMark Function
7.2-I.1		be at least 12.7 mm (0.5 inches) in both vertical and horizontal dimensions				
7.2-I.2		be at least 2.54 mm (0.1 inches) away from adjacent touch areas				
7.2-I.3		not overlap another touch area				
D	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 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 10-14 mm and the average fingertip is 8-10 mm. Applies to: Touch screen interfaces				
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.		Hand marked paper ballot bubbles are .20"x.13"	VotingWorks functional and automated testing confirms bubbles on hand marked ballots are these dimensions.	System Overview > Hand Marked Ballots
D	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				
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).		Voter facing physical controls on VxScan & VxMark require no greater than 5 lbs.	VotingWorks functional testing measures the force required for all voter facing controls to confirm it does not require greater than 5 lbs.	System Overview > VxScan Hardware; System Overview > VxMark Hardware
D	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]. Applies to: Physical controls				
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.		All voter facing controls can be used without direct bodily contact.	VotingWorks functional testing confirms that voter facing controls can be made without direct bodily contact.	System Overview > VxScan Hardware; System Overview > VxMark Hardware
D	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. 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				
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.		All voter facing keys and controls have no repetitive effect when held.	VotingWorks functional testing confirms that voter facing keys and controls have no repetitive effect when held.	System Overview > VxScan; System Overview > VxMark
D	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].				
7.2-N	System response time	The voting system’s response time must meet the following response times:		VxMark & VxScan meet these system response times in response to voter action.	VotingWorks functional testing confirms that VxMark & VxScan response times to voter inputs meet these requirements.	User Manual
7.2-N.1		The system initially responds to a voter action in no more than:				
7.2-N.1.a		0.1 seconds for a visual change, and				
7.2-N.1.b		0.5 seconds for an audio response.				
7.2-N.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.				
7.2-N.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.				
D	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 detectable activity is taking place for several seconds. There need not be a specific "activity" icon, as long as some visual change is apparent (such as progressively "painting" a new screen or providing audio feedback). Applies to: Electronic interfaces				
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:		VxMark presents an inactivity alert after 5 minutes that once expired enables the voter to have additional time for 30 seconds. VxMark then clears the ballot data and requires poll worker intervention.	VotingWorks functional testing confirms the inactivity experience presents after the documented time periods and requires poll worker intervention after.	User Manual > Voting Sessions
7.2-O.1		The system must document the inactivity time.				
7.2-O.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.				
7.2-O.3		The alert time must be between 20 and 45 seconds.				
7.2-O.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				
D	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				
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:				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
7.2-P.1		providing a clear area for a wheelchair of 760 mm (30 inches) wide and 1220 mm (48 inches) deep, and		VxScan and VxMark accommodate floor space as specified.	VotingWorks functional and usability testing confirms that VxScan and VxMark accommodate floor space as specified.	System Overview > VxMark Hardware; System Overview > VxScan Hardware
7.2-P.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.				
D	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.				
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].		VxScan and VxMark physical dimensions meet the referenced U.S. Access Board requirements.	VotingWorks functional and usability testing confirms that VxScan and VxMark meet the referenced U.S. Access Board requirements.	System Overview > VxMark Hardware; System Overview > VxScan Hardware
D	Discussion	This requirement is part of Section 508 [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].				
7.2-R	Control labels visible	Labels for physical controls used by voters must be placed:	7.1-N - Tactile keys; 7.2-Q - Physical dimensions; 7.3-L - Icon labels	Labels for physical controls used by voters are only present on VxMark and are on a surface where voters can see them from seated or standing postures within the required physical dimensions.	VotingWorks functional testing confirms that physical controls are placed in accordance with the requirement.	System Overview > VxMark Hardware
7.2-R.1		on a surface of the voting system where voters can see them from a seated or standing posture, and				
7.2-R.2		within the dimensions required in 7.2-Q – Physical dimensions				
D	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.				
7.3	Voters can understand all information as it is presented, including instructions, messages from the system, and error messages					
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.		All features of the voting system are designed to help voters complete their ballots effectively.	Usability testing results demonstrate that the voting system has a low error rate and features of the system do not lead to voters making errors.	User Manual
D	Discussion	This requirement provides a general scope that supports the other requirements in 7.3. It is meant to encourage innovation in meeting this principle while ensuring that any new design features not covered explicitly in 7.3 help and not hinder voters in understanding and voting their ballots effectively.				
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.	7.2-D - Scrolling	VxMark employs a "more" button per 7.2-D to ensure a contest is not split into two groups of options. Hand-marked paper ballots that divide options across two columns or two pages are not supported.	VotingWorks functional and automated testing confirms that no contest is split into two groups of options for all types of election packages.	User Manual > VxMark; System Performance and Specifications > System Limits
7.3-B.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				
7.3-B.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 7.2-D – Scrolling for managing the way the list of options is displayed.				
D	Discussion	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.				
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.		All ballots indicate this information as specified in the election package.	VotingWorks functional and automated testing confirms that this information is provided for each contest.	System Overview > Election Package
7.3-C.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.		VxMark shows all this information in a consistent order across election packages.	VotingWorks functional and automated testing confirms VxMark presents this information on-screen and through the headphone audio interface consistently across election packages.	User Manual > VxMark Function
7.3-C.2		The maximum number of selections allowed in the contest.				
7.3-C.3		In the audio format only, the number of options or candidates.				
7.3-C.4		If any selections have already been made, the number of selections remaining.				
7.3-C.5		In the audio format only, if any selections have been made, the currently selected candidates or options.				
7.3-C.6		Any instructions or reminders of how to find marking instructions, placed visually and in audio after the contest information.				
D	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.				
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.	2.2-A - User-centered design process; 5.2-A - No bias; 7.3-N - Instructions for voters; 8.3-A - Usability tests with voters	The design presentation of a contest selection to the way the voter marks that selection is consistent across all ballots. Hand-marked paper spatial relationship to a bubble is consistent and contest selections on VxMark are always presented consistently where the way the voter marks the selection is by clicking on the option. The format of contest selections on BMD ballots is also consistent.	7.1-G - Text size (electronic display); 7.1-H - Scaling and zooming (electronic display); 7.2-E - Touch screen gestures; 7.2-F - Voter speech; 7.2-H - Accidental activation; 7.2-I - Touch area size; 7.3-B - No split contests; 7.3-E - Feedback; 7.3-F - Correcting the ballot; 7.3-H - Overvotes; 7.3-I - Undervotes; 7.3-K - Warnings, alerts, and instructions	System Overview > Hand Marked Paper Ballots; System Overview > Machine Marked Ballots; User Manual > VxMark Function
D	Discussion	A type of contest includes contests to: vote for one or more candidates, answer a ballot question, vote whether to retain a judge, 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.				
7.3-E	Feedback	The voting system must provide unambiguous feedback confirming the voter's selection.	7.2-C - Voter control; 7.3-G - Full ballot selections review			

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
D	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. 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		VxMark provides a visual and audio notification (over headphones) that unambiguously confirms the voter selections	VotingWorks functional and usability testing confirms that the presentation of visual and audio voter confirmation is unambiguous.	User Manual > VxMark > Voting Sessions; System Overview > VxMark Function
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:	5.2-F - Preserving votes; 7.3-H - Overvotes; 7.3-I - Undervotes	Voters casting ballots on VxScan are notified of overvotes and undervotes based on adjudication reasons set in the election package. The same warnings are presented during the marking experience on VxMark based on election package configuration.	VotingWorks functional and automated testing confirms that voters have the opportunity to correct the ballot before it is cast or printed based on the election package configuration.	User Manual > Assisting Voters; User Manual > VxMark > Voting Sessions; System Overview > VxMark Function; System Overview > VxScan Function
7.3-F.1		allow the voter to change a vote within a contest before advancing to the next contest				
7.3-F.2		provide the voter the opportunity to correct the ballot before it is cast or printed				
7.3-F.3		allow the voter to make these corrections without assistance				
D	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].				
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:	5.2-F - Preserving votes; 7.3-H - Overvotes; 7.3-I - Undervotes	VxMark provides this information on a review screen before printing the ballot and subsequently before casting the ballot. VxScan presents these notifications after a voter inserts their ballot into the scanner.	VotingWorks functional and automated testing confirms that voters are provided the opportunity to review their selections before printing or cast their ballot for all election packages based on their respective configurations.	User Manual > VxMark > Voting Sessions; System Overview > VxMark Function
7.3-G.1		displays all of the contests on the ballot with:				
7.3-G.1.a		the voter's selections for that contest				
7.3-G.1.b		a notification that they have not made a selection				
7.3-G.1.c		a notification that they have made fewer selections than allowed				
7.3-G.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				
7.3-G.3		allows the voter to continue to the function for casting the ballot without making a correction at any time in the review process				
7.3-G(cont.)		The review function may also be provided on a scanner or other device where the voter marks and casts a paper ballot.				
D	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. 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.				
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.	5.1-D - Accessibility features; 7.2-C - Voter control; 7.3-K - Warnings, alerts, and instructions	Voters casting ballots on VxScan are notified of overvotes based on adjudication reasons set in the election package. On VxMark, voters are prevented from selecting more than allowable number of options and are warned when they try.	VotingWorks functional and automated testing confirms that voters are notified of overvotes on VxScan based on the settings in the election package and are prevented from marking overvotes on VxMark.	User Manual > Assisting Voters; User Manual > VxMark > Voting Sessions; System Overview > VxScan Function; System Overview > VxMark Function
7.3-H.1		An electronic ballot interface must prevent voters from selecting more than the allowable number of options for each contest.				
7.3-H.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.				
D	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 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				
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).	7.2-C - Voter control; 7.3-K Warnings, alerts, and instructions	Voters casting ballots on VxScan are notified of undervotes based on adjudication reasons set in the election package. On VxMark, voters are warned in both visual and audio modes of undervotes during the review stage.	VotingWorks functional and automated testing confirms that voters are notified of undervotes on VxScan based on the settings in the election package and are warned of undervotes on VxMark.	User Manual > Assisting Voters; User Manual > VxMark > Voting Sessions; System Overview > VxScan Function; System Overview > VxMark Function
7.3-I.1		Both electronic interfaces and scanners must allow the voter to submit an undervoted ballot without correction.				
7.3-I.2		The voting system may allow election officials to disable the notification of undervotes on a scanner.				
D	Discussion	For electronic interfaces, this notification can be incorporated into the review feature. This requirement supports HAVA [HAVA02]. Applies to: Electronic interfaces and scanners				
7.3-J.1	Notification of casting	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.		VxMark provides on-screen and audio format (via headphone) confirmation of a cast ballot or an unsuccessfully cast ballot with the reason for failure. VxScan provides on-screen and audio (via speaker) confirmation of a cast ballot or an unsuccessfully cast ballot with the reason for failure. Blank ballots are detected and a warning is provided based on the election package configuration.	VotingWorks functional and usability testing confirms that unambiguous successful and unsuccessful casting notification is provided on all voter facing devices.	User Manual > Assisting Voters; User Manual > VxMark > Voting Sessions
7.3-J.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.				
D	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].				
7.3-K	Warnings, alerts, and instructions	Warning, alerts, and instructions issued by the voting system must be distinguishable from other information.		Warnings and alerts are visually distinct from other messages and clearly stated in plain language per the requirements in 7.3-K.	VotingWorks functional and usability testing confirms that all alerts are visually distinct from other messages and clearly stated in plain language.	User Manual > VxScan Error Messages; User Manual > VxMark Error Messages
7.3-K.1		Warnings and alerts must clearly state in plain language:				
7.3-K.1.a		the nature of the issue or problem				
7.3-K.1.b		whether the voter has performed or attempted an invalid operation or whether the voting system itself has malfunctioned in some way				
7.3-K.1.c		the responses available to the voter				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
7.3-K.2		Each step in an instruction or item in a list of instructions must be separated:		Sequences of instructions are separated as visually distinct list items and with pauses in audio mode.	VotingWorks functional and usability testing confirms that all instructions are clearly separated and stated in plain language.	User Manual > Assisting Voters; User Manual > VxMark > Voting Sessions
7.3-K.2.a		spatially in visual formats				
7.3-K.2.b		with a noticeable pause in audio formats				
D	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].				
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. 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 discernible 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.	7.1-N - Tactile keys; 7.2-R - Control labels visible; 8.1-E - Standard audio connectors; 8.1-I - Standard PAT jacks	All voter facing icons presented on screen are associated with a corresponding text label. Per the requirement, the input jacks on VxMark are an exception to this requirement.	VotingWorks functional and automated testing confirms all voter facing icons are accompanied with a text label.	User Manual > Assisting Voters; User Manual > VxMark > Voting Sessions
D	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].				
7.3-M	Identifying languages	A vote-capture device or other voting session device that offers language options to a voter must:		VxMark and VxScan have a language selection button shown on all voter facing screens with language selections translated as the native version of each language.	VotingWorks functional and automated testing confirms a language selection button is persistent on all voter facing screens with the language translated as the native version for all multi-language election packages.	User Manual > Assisting Voters; User Manual > VxMark > Voting Sessions
7.3-M.1		visibly present the controls to identify or change language on the screen at all times, not hidden within a help or settings feature,				
7.3-M.2		include the native version of each language name in the list of language options.				
D	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				
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.	5.1-F - Accessibility documentation	Voter facing screens provide clear language instructions for all steps of the voting process. Paper ballots support instructional text as part of the balot design.	VotingWorks functional and usability testing confirms clear language instructions are part of all steps of the voting process across all marking methods.	User Manual > Assisting Voters; User Manual > VxMark > Voting Sessions; System Overview > Hand Marked Ballots
7.3-N.1		For electronic interfaces, the voting system must provide a way for voters to get help directly from the system.				
7.3-N.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.				
7.3-N.3		Voting systems must present instructions near to where they are needed during the voting session.				
D	Discussion	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.				
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.	5.1-F - Accessibility documentation	Documentation is provided in the user manual.	VotingWorks staff reviews documentation.	User Manual
7.3-O.1		The documentation required for normal voting system operation must be:				
7.3-O.1.a		presented at a level appropriate for election workers who are not experts in voting system and computer technology				
7.3-O.1.b		in a format suitable for use in the polling place				
7.2-O.2		Printed procedural instructions, and on-screen instructions and messages must enable the election workers to verify that the voting system				
7.3-O.2.a		has been set up correctly (setup)				
7.3-O.2.b		is in correct working order to record votes (polling), and				
7.3-O.2.c		has been shut down correctly (shutdown).				
D	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 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.				
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.		All information presented in the product and product documentation is written in plain language.	VotingWorks functional and usability testing confirms that all information is in plain language.	User Manual
D	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. 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." 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.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
8	Robust, Safe, Usable, and Accessible - The voting system and voting processes provide a robust, safe, usable, and accessible experience					
8.1	The voting system's hardware, software, and accessories are robust and do not expose users to harmful conditions					
8.1-A	Electronic display screens	If the voting system uses an electronic display screen, the display must have the following characteristics:		All electronic screens used in the voting system exceed these minimum requirements. These specifications are published in the "Audio Visual & Display Screen Settings" document.	VotingWorks functional testing confirms that electronic displays meet manufacturer specifications and are configured for proper brightness.	Audio Visual & Display Screen Settings
8.1-A.1		For all electronic display screens:				
8.1-A.1.a		antiglare screen surface that shows no distinct virtual image of a light source or a means of physically shielding the display from such reflections				
8.1-A.1.b		minimum uniform diffuse ambient contrast ratio for 500 lx illuminance: 10:1.				
8.1-A.2		If the display is the primary visual interface for making vote selections:				
8.1-A.2.a		minimum diagonal display size: 12 inches, and				
8.1-A.2.b		minimum display resolution: 1920 x 1080 pixels.				
8.1-A.3		If the display screen is for messages to voters or poll workers:				
8.1-A.3.a		minimum diagonal display size: 7.9 inches, and				
8.1-A.3.b		minimum display resolution: 1024x768 pixels.				
D	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				
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.		N/A - the voting system does not emit lights in flashes		
	Discussion	This requirement has been updated to meet WCAG 2.0 [W3C10] and Section 508 [USAB18] software design issue standards. Applies to: Electronic interfaces				
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.		A voter's personal assistive device is not necessary to use VxMark.	VotingWorks functional and usability testing confirms that a voter's personal assistive device is not necessary to use the voting system.	System Overview > VxMark Function
D	Discussion	This requirement does not preclude the voting system from providing interfaces to assistive technology. (See definition of "personal assistive devices" in Appendix A - Glossary). Its purpose is to ensure that voters are not required to bring special devices with them in order 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.				
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.		N/A - no biometric capabilities		
D	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].				
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		VxMark and VxScan's headphone input is a standard 3.5mm stereo headphone jack.	VotingWorks functional and usability testing confirms that the VxMark & VxScan audio-tactile interface is supported through a standard 3.5mm headphone jack.	System Overview > VxMark Hardware; System Overview > VxScan Hardware
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.		VxMark's headphone input is located in the front left of the voting station that is discernible by touch standing in front of the unit.	VotingWorks functional and usability testing confirms that the headphone input is discernible through touch standing in front of the device.	System Overview > VxMark Hardware
D	Discussion	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.				
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].	6.1-D - Audio privacy; 8.1-J - Hearing aids	VxMark does not use telephone style handsets. VxMark's headphone interface supports a t-coil interface that can connect to the device over the standard 3.5 mm jack. VotingWorks recommends a specific compatible model as specified in System Overview > VxMark Hardware.	VotingWorks functional testing confirms that a wireless T-Coil performs as expected by connecting to the device over the standard 3.5mm headphone jack.	System Overview > VxMark Hardware
D	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].				
8.1-H	Sanitized headphones	The voting system must be supplied with a means to sanitize headphones or handsets and instructions for election workers on the procedure to ensure that a sanitized headphone or handset is available to each voter.		VotingWorks recommends headphone ear covers to be used to sanitize headsets. The recommendation is included in the User Manual.	VotingWorks functional testing confirms the recommended ear covers provide a sanitized headphone to all voters.	User Manual > Voting Sessions
D	Discussion	This requirement can be achieved in various ways, including the use of "throwaway" headphones or sanitary coverings.				
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 voters can use to connect their personal assistive technology switch to the system.	5.1-A - Voting methods and interaction modes; 7.2-A - Display and interaction options	VxMark supports any standard dual-switch input device over the standard 3.5mm PAT jack. All functionality is available in the limited-dexterity interaction mode.	VotingWorks functional and usability testing confirms that all dual-switch input devices are supported on VxMark through the 3.5mm PAT jack.	System Overview > VxMark Hardware
8.1-I.1		The jack must allow only switch activations to be transmitted to the system.				
8.1-I.2		The system must accept switch input that is functionally equivalent to other input methods.				
8.1-I.3		All the functionality of the voting system must be available through technology using this input mechanism.				
D	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. 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.				
8.1-J	Hearing aids	Voters who use assistive hearing devices must be able to use voting devices as intended:	8.1-G - Telephone style handset			
8.1-J.1		The voting device must not cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
8.1-J.2		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].				
D	Discussion	"Hearing devices" include hearing aids and cochlear implants. This requirement is based on WCAG 2.0 [W3C10] and Section 508 [USAB18].		Voters who use assistive hearing devices can use VxMark without any degraded experience.	VotingWorks hardware testing confirms that VxMark headphones do not interfere with assistive hearing devices.	Quality Assurance
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].				
D	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].		Voting system devices are all safety tested to UL 62368-1 by a NRTL.	VotingWorks contracts with NRTLs to test components that are not already tested to be in accordance with UL 62368-1.	Audio Visual & Display Screen Settings; Quality Assurance
8.2	The voting system mets currently accepted federal standards for accessibility					
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.				
D	Discussion	This applies to all parts of the voting system including the election management system (EMS). 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		All VxSuite components meet Section 508 and WCAG 2.0 Level AA checkpoints.	VotingWorks staff reviews these standards to implement functional and automated tests that confirm conformance with these standards.	Quality Assurance
8.3	The voting system is evaluated with a wide range of representative voters, including those with and without disabilities					
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:	2.2-A - User-centered design process; 5.1-D - Accessibility features			
8.3-A.1		General population, using the visual interface (without audio), including:				
8.3-A.1.a		voters who are native speakers of the language being tested for each language defined as supported in the technical data package (TDP)				
8.3-A.1.b		blind voters, using the audio format plus tactile controls				
8.3-A.1.c		voters with low vision, using the enhanced visual features with and without audio				
8.3-A.1.d		voters with limited dexterity, using the visual interface with low and no dexterity controls				
8.3-A.2		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].				
D	Discussion	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.		The report for this usability testing is included in the TDP.	VotingWorks staff conducts usability testing and reviews the report included in documentation.	Usability & Accessibility
8.4	The voting system is evaluated for usability with election workers					
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:	2.2-A - User-centered design process; 7.3-O - Instructions for election workers			
8.4-A.1		Setup and opening for voting, which involves:				
8.4-A.1.a		operation during voting				
8.4-A.1.b		use of assistive technology or language options that are part of the voting system				
8.4-A.1.c		shutdown at the end of a voting day during a multi-day early voting period, if supported by the voting system				
8.4-A.1.d		shutdown at the end of voting including running any reports				
8.4-A.1.e		providing ballots in different languages				
8.4-A.1.f		selecting the correct ballot type (for example, for vote centers)				
8.4-A.1.g		setting up the voting system to use different display formats and interaction modes				
8.4-A.2		The test participants must include election workers representing a range of experience				
8.4-A.3		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].				
D	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.		The report for this usability testing is included in the TDP.	VotingWorks staff conducts usability testing and reviews the report included in documentation.	Usability & Accessibility

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
9	Auditable - The voting system is auditable and enables evidence-based elections.					
9.1	An error or fault in the voting system software or hardware cannot cause an undetectable change in election results					
9.1.1	Software independence					
9.1.1-A	Software independence	The voting system must be software independent.	9.1.5 - Paper records; 9.1.6 - Cryptographic E2E verifiable	VxSuite has a paper-based system architecture as specified in the technical data package.	VotingWorks functional and automated testing confirms it is not possible to cast a ballot without a voter-verified paper trail, and ballots cannot be modified when cast.	System Overview > Software Overview > Software Independence
9.1.1-A.1		The voting system must meet the requirements within the Paper-based System Architectures or Cryptographic E2E Verifiable System Architectures section, or both.				
9.1.1-A.2		The voting system documentation must include the method used to provide software independence.				
D	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 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. However, a system that meets all of the paper-based requirements need not satisfy the E2E-requirements even if it incorporates E2E verifiable functionality. Knowing the specific mechanism used to achieve software independence assists with determining if the system is 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?				
9.1.2	Tamper Evidence					
9.1.2-A	Tamper-evident records	The voting system must produce tamper-evident records that enable detection of incorrect election outcomes, including:		Ballots on VxScan & VxMark are stored in a tamper-evident ballot box once cast. CVRs for ballots scanned on VxScan are continuously exported to external disks stored in a tamper-evident manner.	VotingWorks functional testing confirms all CVRs and ballot images are stored in a tamper evident manner.	System Security, Auditing, Logging > Physical Security; System Security, Auditing, Logging > Artifact Authentication
		capturing the contents of each vote at the time of each ballot's casting, and				
		recording detected errors in a tamper-evident manner.				
D	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.				
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.				
D	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. Applies to: Voter-facing scanners and electronic ballot markers				
9.1.3	Voter verification					
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.	7.3-G - Full ballot selections review	VxScan provides confirmation that a voter's ballot was correctly interpreted and an opportunity for second chance voting if errors or issues were detected. VxMark allows a voter to review their interpreted selections.	VotingWorks testing staff confirms during functional testing that voters receive confirmation of successfully cast ballots, rejected ballots, and ballots with adjudication issues on VxScan. VotingWorks testing staff confirms during functional testing staff that voters can review their interpreted ballot selections on VxMark	System Overview > VxScan Function; System Overview > VxMark Function; User Manual > Assisting Voters; User Manual > Voting Sessions
D	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. Applies to: Voter-facing scanners and electronic ballot markers				
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.	7.3-F - Correcting the ballot	On VxScan, the voter can return their ballot to spoil it if errors are detected. On VxMark, the voter can spoil their ballot after printing the ballot if they want to make a correction.	VotingWorks testing staff confirms during functional testing that voters can return ballots with issues on VxScan and can spoil printed ballots on VxMark.	System Overview > VxScan Function; System Overview > VxMark Function; User Manual > Assisting Voters; User Manual > Voting Sessions
D	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 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. Apples to: Paper-based system architectures				
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.		Voters are instructed on screen to ask a poll worker for help when errors are encountered.	VotingWorks testing staff confirms during functional testing that instructional messages are presented on screen.	User Manual > VxScan Error Messages; User Manual > VxMark Error Messages
D	Discussion	This can include a voter alerting an election worker or pressing a button on the machine to report detected errors or incorrect results.				
9.1.4	Auditable					
9.1.4-A	Auditor verification	Voting systems must generate records that would enable external auditors to verify that cast ballots were correctly tabulated.		Ballot images for each corresponding voter-verifiable paper ballot are saved as part of cast vote records.	VotingWorks functional and automated testing confirms a corresponding ballot image is stored with cast vote records for each voter verifiable paper ballot.	System Overview > Cast Vote Records; System Security, Auditing, Logging > Audit Procedure
D	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.				
9.1.4-B	Documented procedure	The voting system manufacturer must provide a documented procedure to verify that cast ballots were correctly tabulated.	9.1.1-A - Software independent	VxSuite supports a variety of post-election audit methods including: batch comparison, ballot comparison, and image audits. These methods are documented in the TDP.	VotingWorks functional testing confirms post-election audits may be performed per audit documentation.	System Security, Auditing, Logging > Audit Procedure
D	Discussion	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.				
9.1.5	Paper Records					

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
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.	3.3-C - Bar and other codes; 3.3-D - Ballot selection codes; 5.1-E - Reading paper ballots; 6.1-A - Preserving privacy for voters; 6.2-A - Voter independence; 9.1.5-C - Paper record intelligibility; 9.1.5-D - Matching selections	When hand marked paper ballots are used, the voter's ballot selections are inherently paper-based and voter-verified. When a voter uses VxMark, a machine marked paper ballot is printed and presented to the voter for verification.	VotingWorks testing staff confirms during functional testing that VxMark supports verification of a paper ballot by the voter.	System Overview > Software Overview > Software Independence; System Overview > Hand Marked Ballots; System Overview > Machine Marked Ballots
D	Discussion	Voting systems that use independent voter-verifiable records can satisfy the software independence requirement and achieve conformance to the VVSG.				
9.1.5-B	Paper record retention	A paper-based voting system must retain a paper record of the voter's ballot selections.		Ballot boxes on VxScan and VxMark retain a paper record of the voter's ballot selections.	VotingWorks functional testing confirms that paper records are retained.	System Overview > VxScan Function; System Overview > VxMark Function
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.		All voter-verifiable records are in a human readable format.	Functional and usability testing confirms that paper records are in a human readable format.	System Overview > Hand Marked Ballots; System Overview > Machine Marked Ballots
D	Discussion	The requirement ensures that a human-readable version of the data is also printed whenever a barcode is used to encode ballot selections.				
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. Applies to: Paper-based system architectures		Machine marked ballots are designed to clearly reflect the voter's selections.	Functional and usability testing confirms that a voter-verifiable paper record representing the voter's records is presented for voter confirmation before casting.	System Overview > Machine Marked Ballots; System Overview > VxMark Function
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.	3.3-C - Bar and other codes; 3.3-D Ballot selection codes	VxMark machine marked ballots have a publicly documented QR code format in the TDP.	VotingWorks staff reviews the publicly available documentation for completeness and accuracy.	System Overview > Machine Marked Ballots
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.	1.1.5-G - Record audit information; 9.4-A - Risk-limiting audit; 9.4-B - Random numbers supporting audit processes; 9.1.1-A - Software independent	VxCentralScan batch scanners support an imprinter attachment that prints a unique identifier on the ballot in a publicly documented format per the TDP.	VotingWorks functional testing confirms VxCentralScan imprints a unique identifier in the publicly documented format.	System Overview > VxCentralScan Function
D	Discussion	Although not all jurisdictions may use this feature, voting systems are required to have the capability to add a unique identifier to ballots. Applies to: Paper-based system architectures				
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.	9.1.1-A - Software independent	VxCentralScan imprinting cannot imprint in the ballot marking area when configured by the election official per the User Manual.	Functional testing confirms that VxCentralScan imprinting cannot imprinting the ballot marking area when configured per the instructions in the User Manual.	User Manual > VxCentralScan Hardware Setup
D	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 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.				
9.1.6	Cryptographic E2E Verifiable					
9.1.6-A	Verified cryptographic protocol	The E2E cryptographic protocol used by the cryptographic E2E verifiable voting system must be evaluated and approved through a public process established by the EAC.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
D	Discussion	Due to the lack of E2E verifiable voting systems available within the current market, there are no verified E2E cryptographic protocols. A standard public process for approval of the E2E cryptographic protocols will need to be established outside of the VVSG. Once this process is established, the VVSG requirements can point to the approved/verified cryptographic protocols as acceptable for use within an E2E verifiable voting system.				
9.1.6-B	Independent evaluation of E2E cryptographic protocol implementation	A cryptographic E2E verifiable voting system must undergo an independent evaluation to verify it correctly and securely implements an approved E2E cryptographic protocol.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
D	Discussion	An independent evaluation can be performed by any entity outside of the voting system manufacturer. Example best practices include using guidance from the FIPS 140 series [NIST01, NIST19a], NIST SP 800-133 Revision 2, Recommendation for Cryptographic Key Generation [NIST20f], or NIST SP 800-175B, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms [NIST20g]. The independent evaluation and cryptographic engineering best practices used can be documented and submitted. Lessons learned from the analysis of the source code of the Swiss Post system shows the value in making this code available for public review. See "How not to prove your election outcome" [Lewis19b], and "Ceci n'est pas une preuve" [Lewis19a].				
9.1.6-C	Cryptographic ballot selection verification by voter	A cryptographic E2E verifiable voting system must:	6.2-A - Voter independence; 7.3-G - Full ballot selections review; 9.1.6-E - Ballot receipt; 10.2-4-A - Voting information in receipts	N/A - VxSuite is not a cryptographic E2E verifiable voting system		
9.1.6-C.1		be capable of providing evidence that an individual voter can use to confirm that the voting system correctly interpreted their ballot selections, while in the polling place; and				
9.1.6-C.2		provide evidence such that if there is an error or flaw in the interpretation of the voters' selections, the evidence can be used for detection of the error or flaw.				
D	Discussion	This requirement addresses cast-as-intended verification, which is one of the principal components necessary to achieve end-to-end-verifiability [Benaloh14]. Interpretation is the process by which the voting system converts the voter's contest option selections into the format used to store these selections. Therefore, this evidence must sufficiently prove the representation of the voter's contest option selections in digital form matches the voter selections as provided to the system. Giving voters the opportunity to verify the voting system stored their ballot choices correctly is a fundamental building block in an end-to-end verifiable voting system. See "End-to-end verifiability" [Benaloh14] and "Usability is not Enough: Lessons Learned from 'Human Factors in Security' Research for Verifiability" [Kulyk18] for more information on the various implementations of this technique.				
9.1.6-D.1	Methods for cryptographic ballot selection verification	A cryptographic E2E verifiable voting system documentation must include: the method for the voter to use the evidence provided for ballot selection verification to verify the correct interpretation of their ballot; and				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
9.1.6-D.2		a list of known verification tools, their supplier, and how the verification tools are used.	9.1.6-C - Cryptographic ballot selection verification by voter			
D	Discussion	Voter intent verification often relies on external verification tools to assist voters in the verification step(s). These can be external verifiers, which is either a second device, a website of a trusted institution, or software running inside the polling location. The manufacturer must provide documentation explaining the verification options available to voters. If the jurisdiction is expected to provide the verification tool or service, this must also be documented.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
9.1.6-E	Ballot receipt	A cryptographic E2E verifiable voting system must provide a voter with a receipt that allows them to verify that their ballot has been correctly recorded and tallied by the system. These receipts	6.1-A - Preserving privacy for voters; 6.2-A - Voter independence; 7.3-G - Full ballot selections review; 8.3-A - Usability tests with voters; 10.2.4-A - Voting information in receipts			
9.1.6-E.1		must not display any ballot selections made by the voter				
9.1.6-E.2		must not enable the voter to prove their selections on the cast ballot to others				
9.1.6-E.3		must be represented in a publicly documented format				
9.1.6-E.4		may contain a unique identifier				
9.1.6-E.5		are accessible, verifiable, and preserve voter-privacy				
D	Discussion	This evidence should fail to confirm a voter's ballot has been correctly recorded and tallied by the system if the ballot has been removed, tampered with, or its selections altered, added to, or removed.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
9.1.6-F	Disputes involving ballot receipts	The cryptographic E2E verifiable voting system documentation must provide procedures for collecting, investigating, and adjudicating disputes from voters based on the contents of their ballot receipts.	9.1.6-E - Ballot receipt			
D	Discussion	This documentation will include a process to address the scenario where a voter attempts to verify with their ballot receipt and believes there is a problem with their ballot receipt				
9.1.6-G	Evidence export	A cryptographic E2E verifiable voting system must:				
9.1.6-G.1		be capable of exporting all evidence supporting ballot tabulation verification				
9.1.6-G.2		provide the export in an open and consumable format				
D	Discussion	Most recorded-as-cast verification approaches require the public posting of the evidence at some point after all ballots have been aggregated and tallied. As required in the previous requirement, the evidence must not reveal how voters voted.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
9.1.6-H	Mandatory ballot availability	A cryptographic E2E verifiable voting system must be capable of exporting all encoded ballots for public posting.				
D	Discussion	The public posting does not have to be provided by the voting system, but the voting system must provide the evidence such that it can be published, and the verification process made accessible to voters. The public posting of these exported encoded ballots is performed by election officials and is an essential part of the E2E verifiable process. It allows the public to verify the election results.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
9.1.6-I	Verification of encoded votes documentation	A cryptographic E2E verifiable voting system documentation must include:				
9.1.6-I.1		the expected method by which voters will perform the ballot tabulation verification, and				
9.1.6-I.2		how this method provides voters with the opportunity to verify that their ballots are included within the tabulation results.				
D	Discussion	For example, a common method is to publish the evidence to a public bulletin board. The manufacturer should document this method or its alternative. The bulletin board, itself, might not be included in the scope of the voting system but the voting system must provide an export of the evidence to be published on the bulletin board.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
9.1.6-J	Verifier reference implementation	A cryptographic E2E verifiable voting system documentation must include:	9.1.6-C - Cryptographic ballot selection verification by voter			
9.1.6-J.1		a free publicly available reference implementation of a tool which can be used:				
9.1.6-J.1.a		to verify evidence provided to a voter to prove that their ballot choices were correctly interpreted				
9.1.6-J.1.b		to verify the evidence reported for voters to perform ballot tabulation verification				
9.1.6-J.2		the build instructions for the reference implementation, along with the tool				
D	Discussion	For the system to support the cast-as-intended property of end-to-end verifiable systems there must be at least one tool available to voters to verify that their ballot selections have been correctly interpreted. Additionally, for a cryptographic E2E system be software independent, the voters need to have choices about what software use and trust when performing verification. By providing an open source reference implementation may facilitate development of third-party verification tools.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
9.1.6-K	Privacy preserving, universally verifiable ballot tabulation	A cryptographic E2E verifiable voting system tabulation process must preserve the privacy of every voter and provide a method for public verification.	6.1-A - Preserving privacy for voters			
D	Discussion	To be publicly verifiable, the approach provides a means for any auditor or observer to verify the correct decryption and tabulation of the votes (not necessarily in that order) using cryptographic proofs that are generated by the process.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
9.2	The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities					
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.	1.1.9-A - Post-election reports; 3.1.3-D - Audit procedures	VxSuite supports a variety of post-election audit methods including: batch comparison, ballot comparison, and image audits. These methods are documented in the TDP.	VotingWorks functional testing confirms post-election audits may be performed per audit documentation.	System Security, Auditing, Logging > Audit Procedure
D	Discussion	Ballots, CVRs, and ballot images are examples of artifacts that can support a post-election audit.				
9.3	Voting system records are resilient in the presence of intentional forms of tampering and accidental errors					
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.	13.1.2-A - Integrity protection for election records; 13.2-A - Signing stored election records; 13.2-B - Verification of election records	CVRs and ballot images are digitally signed and verified when	Functional testing confirms that all audit	System Security, Auditing, Logging >

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
D	Discussion	CVRs and ballot images need sufficient data protection because they are needed for audits.		imported into VxAdmin.	records are signed and verified.	Artification Authentication
9.4	The voting system supports efficient audits					
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.	4.1-C - Exchange of cast vote records (CVRs); 9.1.5 - Paper records; 9.2-A - Audit support documentation; 9.4-C - Unique ballot identifiers; 9.4-D - Multipage ballots			
D	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.		The artifacts required to support a batch-comparison or ballot-comparison risk-limiting audit are available as defined in the Audit Procedure in the TDP.	VotingWorks functional testing confirms post-election audits may be performed per audit documentation.	System Security, Auditing, Logging > Audit Procedure
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.	9.4-C - Unique ballot identifiers; 10.2.2-E - Randomly generated identifiers			
D	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].		Random unique identifiers used in cast vote records, ballot images, and imprinted values on ballots are publicly documented in the TDP.	VotingWorks staff reviews documentation for completeness and accuracy.	System Overview > Cast Vote Records; System Overview > VxCentralScan Function
9.4-C	Unique ballot identifiers	The voting system must enable election auditors to uniquely address individual ballots.				
D	Discussion	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		Unique ballot identifiers are available in the cast vote record, associated ballot images, and imprinted value (when imprinting on VxCentralScan).	Functional and automated testing confirms a unique ballot identifier is present in cast vote records, ballot images, and on imprinted ballots.	System Overview > Cast Vote Records; System Overview > VxCentralScan Function
9.4-D	Multipage ballots	The voting system must be able to account for multipage ballots.		VxSuite supports multi-page hand marked paper ballots.	Functional and automated testing confirms that multi-page hand marked paper ballots are supported throughout voting system functionality.	System Overview > Hand Marked Ballots

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
10	Ballot Secrecy - The voting system protects the secrecy of voters' ballot selections					
10.1	Ballot secrecy is maintained throughout the voting process					
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.	11.1-B - Voter information in log files	No personally identifiable information about a voter is ever inputted into VxSuite. Additionally, VxScan shuffles CVRs to preserve voter privacy and VxAdmin reporting flags reports that could violate voter privacy for an election official.	VotingWorks functional testing confirms that no information in the voting system can be associated with a specific voter.	System Security, Auditing, Logging > Preserving Voter Privacy; System Overview > VxAdmin Results Exports
D	Discussion	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.				
10.2	The voting system does not contain nor produce records, notification, information about the voter, or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.					
10.2.1	Voter associations					
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.				
D	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.)				
10.2.1-B	Indirect voter associations	Indirect voter associations must only be used to associate a voter with their encrypted ballot selections.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
D	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. 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. Applies to: Cryptographic E2E verifiable voting system architectures				
10.2.1-C	Use of indirect voter associations	The voting system must only use indirect voter associations when the option is selected at the beginning of a voting session for situations when a voter needs to fill out a ballot before their eligibility is determined.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
D	Discussion	Certain channels of voting require indirect associations so that ballots can be removed before casting for a variety of reasons including signature mismatch or death of a voter. These types of ballots are often considered provisional or recallable ballots. Applies to: Cryptographic E2E verifiable voting system				
10.2.1-D	Isolated storage location	Ballots that are not cast and contain an indirect association must be separated from cast ballots.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
D	Discussion	Ballots that contain an indirect association are not considered cast. Cast ballots and ballots having their eligibility considered need to be kept separate from each other. Although not the only way of meeting this requirement, one example would be storing cast ballots in a different directory from ballots not yet cast. Applies to: Cryptographic E2E verifiable voting architectures				
10.2.1-E	Removal of indirect voter associations	The voting system must be capable of removing the indirect voter association between a ballot and a voter once that voter is determined to be eligible.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
D	Discussion	Provisional or recallable ballots may require indirect associations so that ballots can be removed before casting. After a voter's eligibility is determined the indirect voter association can be removed and the ballot can be added to collection of cast ballots. In the case of electronic E2E systems, whatever data record provides this association must be removed from the system. Ballots with indirect associations are not considered cast until the association is removed. Best practice would ensure that indirect voter associations are only available to authorized election personnel. Applies to: Cryptographic E2E verifiable voting architectures				
10.2.1-F	Confidentiality for ballots with indirect voter associations	The voting system must only be capable of decrypting a ballot after any indirect voter association to it has been removed.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
D	Discussion	Encryption of the ballot preserves the confidentiality of the voter's ballot selections while the ballot is tied to an indirect association to the voter. The indirect voter association is not encrypted with the ballot. The voting system must not be capable of decrypting a ballot that still has an indirect association to a voter. A possible approach to implement this is by requiring that a decryption key (or set of keys) be entered to decrypt ballots but disallowing input until after all indirect associations have been removed. If the key is present on the system at the same time as indirect associations, it may be possible for malicious software to decrypt ballots and associate selections with voters. Applies to: Cryptographic E2E verifiable voting architectures				
10.2.2	Identification in vote records					
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.	9.1.5-F - Unique identifier	N/A - VxSuite does not use any indirect associations between the voter's identity and their ballot.		
D	Discussion	For the purpose of these requirements, associations between physical ballots and CVRs are not considered direct or indirect identifiers.				
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.		VxScan shuffles CVR order to preserve voter privacy.	Functional and automated testing confirms that CVR order has no association to a voter record.	System Security, Auditing, Logging > Preserving Voter Privacy
D	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 won't be a problem.				
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.		CVR and ballot image file names are based on random v4 UUIDs.	Functional and automated testing confirms no voter identifying information is in file names.	System Overview > Cast Vote Records
D	Discussion	This helps to ensure that information that could accidently be used to reference a voter is not used within a file name.				
10.2.2-D	Aggregating and ordering	Aggregated and final totals:		VxAdmin aggregated and final reports contain no voter identifying information and cannot recreate the order they were cast in. The reporting interface also highlights possible reporting conditions that could violate voter privacy based on small volume of votes cast.	Functional and automated testing confirms that aggregated and final totals preserve voter privacy.	System Overview > VxAdmin Results Exports
10.2.2-D.1		must not contain voter identifying information				
10.2.2-D.2		must not be able to recreate the order in which the ballots were cast				
D	Discussion	Voter identifying information includes social security number, voter identification number, or driver's license number.				
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.	9.4-B - Random numbers supporting audit processes; 10.2.2-D - Aggregating and ordering			

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Tests	TDP Reference
D	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. 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].		VxSuite utilizes the Node uuid library as a random bit generator, which leverages the operating system's FIPS-compliant OpenSSL implementation that meets NIST requirements.	VotingWorks software code review confirms NIST conforming random bit generation is used.	System Security, Auditing, Logging > System Security Architecture
10.2.3	Access to cast vote records (CVR)					
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.	11.3.1-B - Multi-factor authentication for critical operations; 11.3.1-C - Multi-factor authentication for administrators; 11.4-A - Least privilege for access policies; 11.4-B - Separation of duties	No VxSuite user role has access to the the directory or storage location of these records on a given device's internal disk. These records are redundantly stored on an external USB that is digitally signed and authenticated when imported into VxAdmin. Physical access to this USB drive is restricted by a tamper-evident seal.	Functional testing confirms that no user can access the directory or storage location of these records.	System Security, Auditing, Logging > Physical Security; System Security, Auditing, Logging > System Security Architecture
D	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.				
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.	11.1-A - Logging activities and resources access	The directory and storage location can not be accessed. The application logs when it accesses a storage location through various logs in particular those with a LogEventId starting with "database" and "file." More details on all log events can be found in the logging documentation.	Functional testing confirms that no user can access the directory or storage location of these records.	System Security, Auditing, Logging > Logging
D	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.				
10.2.4	Voter information in other devices in artifacts					
10.2.4-A	Voting information in receipts	Receipts produced by cryptographic E2E verifiable voting systems must not contain voter information.		N/A - VxSuite is not a cryptographic E2E verifiable voting system		
D	Discussion	The voting system must not issue a receipt to the voter that would provide proof to another of how the voter voted.				
10.2.4-B	Logging of ballot selections	Logs and other portions of the audit trail must not contain individual or aggregate ballot selections.		All logs produced by VotingWorks application do not contain individual or aggregate ballot selections.	VotingWorks staff manually audit all code changes to ensure that logs containing individual or aggregate ballot selections are not introduced to the system. A final code review audit was performed of all points in the code where a log is emitted to ensure that no ballot selection information could be recorded. Logs are exported from VotingWorks applications in functional testing and checked for unexpected selection information.	System Security, Auditing, Logging > Logging
D	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.				
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.		VxMark does not retain information about a voter's ballot. Their selections are are kept in temporary memory and cleared after each voting session.	Functional testing confirms that VxMark records do not include any information that would allow identifying a voter's ballot.	System Overview > VxMark Function
D	Discussion	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.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
11	Access Control - The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions					
11.1	The voting system enables logging, monitoring, reviewing, and modifying of access privileges, accounts, activities, and authorizations.					
11.1-A	Logging activities and resource access	The voting system must log any access to, and activities performed on, the voting system, including:		VxSuite logs any access to, and activities performed on, the voting system. A description of the logs and all of the events logged can be found in the logging documentation. The system does not allow access to the underlying operating system's access control system. Authentication related events that occur within the application result have logs beginning with "auth-" or "smart-card-". All logs have timestamps.	VotingWorks functional and automated testing confirms that log entries are created for all such events and the log entries are included in exported logs.	System Security, Auditing, & Logging > Logging
11.1-A.1		timestamps for all log entries				
11.1-A.2		all failed and successful attempts to access the voting system				
11.1-A.3		all events which change the access control system including policies, privileges, accounts, users, groups or roles, and authentication methods				
D	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.				
11.1-B	Voter information in log files	The voting system must not log any voter identifying information.	10.1-A - System use of voter information; 10.2.4-B - Logging of ballot selections	All logs produced by VxSuite applications do not contain any information that could identify a voter or tie a voter to a ballot.	performed of all points in the code where a log is emitted to ensure that no voter identifying information could be recorded. Logs are exported from VotingWorks applications in functional testing and checked for unexpected identifying information.	System Security, Auditing, & Logging > Logging
D	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.				
11.1-C	Preserving log integrity	The voting system must prevent:		The configuration of the system does not allow for changing the configuration of logging, or changing or deleting any existing log entries. The logging protocol, rsyslog, is configured such that logs are never deleted, other than in their original form when they are rotated after a compressed copy is created.	VotingWorks penetration testing confirms that the logging configuration cannot be modified on a locked down device.	System Security, Auditing, & Logging > Logging
11.1-C.1		the logging capability from being disabled				
11.1-C.2		the log entries from being modified in an undetectable manner				
11.1-C.3		The deletion of logs; with the exception of log rotation				
D	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 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.				
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.		on demand at any time. They can save all logs, only error logs, or the logs in a CDF format.	testing confirms that interfaces include an option to export logs and those logs are successfully exported.	System Security, Auditing, & Logging > Logging; User Manual > Retaining and Removing Files
D	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.				
11.2	The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.					
11.2.1	Authorized access					
11.2.1-A	Ensuring authorized access	The voting system must allow only authorized users to access the voting system.		VxSuite applications can only be accessed with the use of certified, programmed smart cards created by the system administrator. Modes in which voters can mark or cast ballots can only be enabled by an authorized poll worker.	VotingWorks functional and automated testing confirms that applications cannot be used without a smart card or with invalid smart cards.	System Security, Auditing, & Logging > System Security Architecture > Access Control
D	Discussion	Authorized users include voters, election officials, and election workers.				
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.		Only system administrators can program, unprogram, or modify smart cards for authentication.	VotingWorks functional and automated testing confirms options to manage smart cards are only exposed to system administrators.	System Security, Auditing, & Logging > System Security Architecture > Access Control; User Manual > Smart Cards and User Roles
D	Discussion	This requirement assists with ensuring only authorized users are given access to the voting system.				
11.2.1-C	Access control by voting stage (Table 11-1 - Voting Stage Descriptions)	The voting system access control mechanisms must distinguish at least the following voting stages from Table 11-1:		VxSuite user roles are given specific permissions by these voting stages that adhere to the	VotingWorks functional and automated testing confirms that user role permissions	
11.2.1-C.1		Pre-voting - Loading, and configuring device software, maintenance, loading election-specific files, preparing for election day usage				
11.2.1-C.2		Activated - Activating the ballot, printing, casting, spoiling the ballot				
11.2.1-C.3		Suspended - Occurring when an election official suspends voting				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
11.2.1-C.4		Post-voting - Closing polls, tabulating votes, printing records		voting stages that adhere to the access control requirements of 11.2.	testing confirms that user role permissions are distinguished by the steps associated with each voting stage.	Software Overview > User Roles; User Manual > Smart Cards and User Roles
D	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).				
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.		Only system administrators can create other system administrator cards, which allow programming other smart cards.	VotingWorks functional and automated testing confirms options to manage smart cards are only exposed to system administrators.	System Security, Auditing, & Logging > System Security Architecture > Access Control; User Manual > Smart Cards and User Roles
D	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 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.				
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.		Only system administrators can import a system settings file as part of an election package into VxAdmin, which is the only means to modify authentication settings.	VotingWorks functional and automated testing confirms that only system administrators can authenticate on VxAdmin before system settings are loaded.	System Security, Auditing, & Logging > System Security Architecture > Access Control; System Overview > Election Package
D	Discussion	The administrator's authority to create or modify permissions restricts users from gaining unauthorized permissions.				
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.	11.2.2-B - Minimum groups or roles	Only system administrators can program, unprogram, or modify smart cards for authentication.	VotingWorks functional and automated testing confirms options to manage smart cards are only exposed to system administrators.	System Security, Auditing, & Logging > System Security Architecture > Access Control; System Overview > User Roles; User Manual > Smart Cards and User Roles
D	Discussion	Table 2 is a list of groups or roles that need to be included within the voting system.				
11.2.2	Role-based access control					
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.		VxSuite's authentication model supports the recommendations in the referenced document in the following ways: maintaining a clear and simple mapping of users to roles based on their responsibilities; assigning permissions to roles and then users to roles, rather than assigning permissions directly to users; establishing a simple hierarchy where higher-level roles manage lower-level roles; preventing users from having multiple roles; limiting lower-level roles to specific contexts (elections) that expire; and providing simple user-management tools.	VotingWorks staff reviewed the authentication system in reference to the specified standard.	System Security, Auditing, & Logging > System Security Architecture > Access Control; System Overview > User Roles; User Manual > Smart Cards and User Roles
D	Discussion	This requirement extends [VVSG2005] I. 7.2.1.1-a by requiring role-based methods to follow ANSI INCITS 359-2004 [ANSI04].				
11.2.2-B	Minimum groups or roles (Table 11-2 - Minimum voting system groups or roles for RBAC)	At minimum, voting systems that implement RBAC must define groups or roles with the role descriptions within Table 11-2.				
11.2.2-B.1		Administrator - Can update and configure the voting devices and troubleshoots system problems.		The system administrator can configure VxAdmin and perform diagnostics on all machines.	VotingWorks functional and automated testing confirms that system administrators can authenticate and access diagnostics at any time.	System Overview > Diagnostics; System Overview > User Roles; User Manual > Smart Cards and User Roles; User Manual > [Component] Diagnostics
11.2.2-B.2		Voter - A restricted process in the vote-capture device. It allows the vote-capture device to enter the activated state for voting activities.		Voters can only use VxMark or VxScan when it the polls have been opened by an authenticated poll worker. Additionally, VxMark voting sessions must be activated by an authenticated poll worker.	VotingWorks functional and automated testing confirms that ballots cannot be cast when polls are not open.	System Overview > User Roles; System Overview > VxScan Function; System Overview > VxMark Function
11.2.2-B.3		Election Worker - 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.		The role "election worker" maps to VotingWorks "election manager" and "poll worker" because the two roles must be separated for finer access control. The poll worker can manage the polls, print poll reports, and recover from most errors. The election manager can load ballot definition files and perform setup and testing procedures.	VotingWorks functional and automated testing confirms that election managers can configure devices, print reports, and troubleshoot devices and poll workers can manage polls and print polls reports.	System Overview > User Roles; User Manual > Smart Cards and User Roles; User Manual
D	Discussion	Table 11-2 is a baseline list of groups or roles to be included in the voting system.				
11.2.2-C	Minimum group or role permissions	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.				
11.2.2-C.1		Administrator		The system administrator can access the device, remove the configuration, or perform	VotingWorks functional and automated testing confirms that system administrators can authenticate into any machine at any	System Overview > User Roles; User Manual > Smart Cards and User Roles;
11.2.2-C.1.a		System - EMS; Pre-Voting - Full Access; Activated - Full Access; Suspended - Full Access; Post-Voting - Full Access				
11.2.2-C.1.b		System - Electronic BMD; Pre-Voting - Full Access; Activated - Full Access; Suspended - Full Access; Post-Voting - Full Access				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
11.2.2-C.1.c		System - Voter-Facing Scanner; Pre-Voting - Full Access; Activated - Full Access; Suspended - Full Access; Post-Voting - Full Access		diagnostics at any time.	time to perform necessary functions.	User Manual
11.2.2-C.2		Voter				
11.2.2-C.2.a		System - EMS		There is no voter mode or poll worker access on VxAdmin.		
11.2.2-C.2.b		System - Electronic BMD; Activated - Vote and cast ballots		Voter modes are not authenticated but managed as application state. Entering voter modes requires poll worker authentication.	VotingWorks functional and automated testing confirms that voters are limited to interacting with precinct devices in voting modes enabled by an authenticated user.	System Overview > User Roles; User Manual > Smart Cards and User Roles; User Manual; System Overview > VxMark Function; System Overview > VxScan Function
11.2.2-C.2.c		System - Voter-Facing Scanner; Activated - Ballot submission				
11.2.2-C.3		Election Worker				
11.2.2-C.3.a		System - EMS; Pre-Voting - Define and load election programming; Post-voting - Reconcile provisional or challenged ballots, write-ins, generate reports		The election manager can adjudicate ballots, generate reports, and export election programming from VxAdmin to load on other devices.		
11.2.2-C.3.b		System - Electronic BMD; Pre-Voting - Open polls, L&A; Activated - Close or suspend polls, Recover from errors, Activate ballot and cancel unvoted ballots; Suspended - Exit suspended state; Post-Voting - Generate reports		The poll worker manages the polls and activating ballots. The election manager manages modes for L&A, and has access to diagnostics for additional troubleshooting.		
11.2.2-C.3.c		System - Voter-Facing Scanner; Pre-Voting - Open polls, L&A; Activated - Recover from errors; Suspended - Exit suspended state; Post-Voting - Generate reports		The poll worker manages the polls and activating ballots. The election manager manages modes for L&A, various configuration settings, and has access to diagnostics for additional troubleshooting.	VotingWorks functional and automated testing confirms that election managers and poll workers are can perform all listed functions.	System Overview > User Roles; User Manual > Smart Cards and User Roles; User Manual
D	Discussion	Table 11-3 – Minimum permissions for each group or role defines the minimum functions according to user, voting stage, and system. Other capabilities can be defined as needed by jurisdiction.				
11.2.2-D	Applying permissions	The voting system must be capable of applying assigned groups or roles and permissions to authorized users.		administrators to assign roles to authorized users by programming and providing smart cards.	VotingWorks functional and automated testing confirms that system administrators can create valid smart cards.	System Overview > User Roles; User Manual > Smart Cards and User Roles
D	Discussion	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.				
11.3	The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations					
11.3.1	Access control mechanisms					
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.		VxSuite uses an access control system to prevent unauthorized access to the voting system.	VotingWorks functional and automated testing confirms that critical aspects of the system cannot be accessed without valid authentication in the form of a smart card programmed by VxAdmin.	System Security, Auditing, & Logging > System Security Architecture > Access Control
D	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.				
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:	8.4-A - Usability testing with election workers			
11.3.1-B.1		runtime software updates to the certified voting system		N/A - VxSuite does not support runtime software updates so the requirement does not apply.		
11.3.1-B.2		aggregation and tabulation		Aggregation and tabulation require multi-factor election manager authentication.	VotingWorks functional and automated testing confirms that MFA is required for election managers to log in for aggregation and tabulation at VxAdmin.	System Overview > User Roles; User Manual > Smart Cards and User Roles
11.3.1-B.3		enabling network functions		N/A - This requirement does not apply because network functions cannot be enabled.		
11.3.1-B.4		changing device states, including opening and closing the polls		Opening or closing the polls requires poll worker authentication, which can be multi-factor if set in the system settings by the system administrator.	VotingWorks functional and automated testing confirms that MFA is required for poll workers to open or close polls if arePollWorkerCardPinsEnabled is true in the system settings.	System Overview > User Roles; User Manual > Smart Cards and User Roles; System Overview > Election Package
11.3.1-B.5		deleting or modifying the CVRs and ballot images		Deleting or modifying the CVRs and ballot images requires multi-factor election manager or system administrator authentication.	VotingWorks functional and automated testing confirms that MFA is required for election managers or system administrators to clear any election data.	System Overview > User Roles; User Manual > Smart Cards and User Roles
11.3.1-B.6		modifying authentication mechanisms		N/A - Authentication mechanisms cannot be changed.		
D	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 & password Smartcard (for example, voter access card) iButton Biometric authentication (for example, fingerprint) 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.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
11.3.1-C	Multi-factor authentication for administrators	The voting system must authenticate the administrator with a multi-factor authentication mechanism.		election manager authentication requires both the smart card itself and the associated PIN.	VotingWorks functional and automated testing confirms that MFA is required for system administrators to log in on any device.	System Security, Auditing, & Logging > System Security Architecture > Access Control
D	Discussion	This requirement extends [VVSG2005] I.7.2.1.2-e by requiring multi-factor authentication for the voting system administrator group or role.				
11.3.2	User authentication credentials					
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.		Users do not use a username and password authentication method, instead relying on smart cards and PINs.		System Security, Auditing, & Logging > System Security Architecture > Password and Credential Policies
D	Discussion	This requirement extends [VVSG2005] I.7.2.1.2-e by requiring strong passwords, password histories, and password expiration.				
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.		Smart card passwords are six-digit PINs in conformance with the guideline for memorized secrets randomly generated by a CSP described in the referenced document.	VotingWorks functional and automated testing confirms that all PINs are randomly generated six-digit numbers.	System Security, Auditing, & Logging > System Security Architecture > Access Control
D	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 characters. NIST SP 800-63B also recommends that if a password is provided to the user it may be 6 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.				
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.		Smart card PINs are stored on the cards themselves. The software on the card will only confirm the PIN with a certified VotingWorks device. The hardware is tamper-evident to prevent directly extracting the information.	VotingWorks penetration testing confirms that PINs cannot be extracted from a smart card with an uncertified device.	System Security, Auditing, & Logging > System Security Architecture > Access Control
D	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].				
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.		Generated PINs avoid weak PINs such as 000000 or 123456.	VotingWorks automated testing confirms that weak PINs are skipped when randomly generated.	System Security, Auditing, & Logging > System Security Architecture > Access Control
D	Discussion	Examples of common weak passwords include 0000, 1111, 1234.				
11.3.2-E	Usernames within passwords	The voting system must ensure that the username is not used in the password.		The requirement does not apply because there is no username associated with the password.		System Security, Auditing, & Logging > System Security Architecture > Access Control
D	Discussion	This requirement extends by restricting the use of usernames and related information in passwords.				
11.4	The voting system's default access control policies enforce the principles of least privilege and separation of duties					
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.		VxSuite implements the principle of least privilege.		System Security, Auditing, & Logging > System Security Architecture > Defense-in-Depth and Least Privilege
D	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.				
11.4-B	Separation of duties	Voting system documentation must include suggested practices for dispersing critical operations across multiple groups or roles.		The user manual describes how system administrators should assign roles describes their permissions.	VotingWorks staff review all documentation.	User Manual > Smart Cards and User Roles
D	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.				
11.5	Logical access to voting system assets are revoked when no longer required					
11.5-A	Session time limits	The voting system must enable an administrator the ability to do the following:	11.5-B - Reauthentication	The system administrator can control the following through attributes in the system settings file imported into VxAdmin: overallSessionTimeLimitHours inavtiveSessionTimeLimitMinutes	VotingWorks functional testing confirms that the system respects the session limits specified in the system settings.	System Security, Auditing, & Logging > System Security Architecture > Access Control; User Manual > Election Package
11.5-A.1		set the maximum time limit for a user's session				
11.5-A.2		set the maximum time limit for user inactivity				
D	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.				
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.	7.2-O - Inactivity alerts; 11.5-A - Session time limits	All applications automatically log out the user after the inactivity period specified in the system settings, at which point the user must re-insert their card and re-authenticate.	VotingWorks functional and automated testing confirm that the user is logged out after the specified time-limits.	System Security, Auditing, & Logging > System Security Architecture > Access Control
D	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].				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
11.5-C	Account lockout	The voting system must lockout roles or individuals after an administrator-specified number of consecutive failed authentications attempts.		Users are locked out after failing authentication a certain number of times, defined by the numIncorrectPinAttemptsAllowedBeforeCardLockout in the system settings.	VotingWorks functional and automated testing confirm that the user is locked out after the specified number of failed authentication attempts.	System Security, Auditing, & Logging > System Security Architecture > Access Control; User Manual > Election Package
D	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. 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.				
11.5-D	Lockout time duration	The voting system must allow only an administrator to define the lockout duration.		The system administrator can set the initial lockout duration in the system settings with the startingCardLockoutDurationSeconds attribute.	VotingWorks functional testing confirms that the system respects the lockout duration specified in the system settings.	System Security, Auditing, & Logging > System Security Architecture > Access Control; User Manual > Election Package
D	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.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
12	Physical Security - The voting system prevents or detects attempts to tamper with voting system hardware					
12.1	The voting system supports mechanisms to detect unauthorized physical access.					
12.1-A	Unauthorized physical access	Any unauthorized physical access to voting systems must leave physical evidence that an unauthorized event has taken place.				
D	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 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.		VxSuite components include tamper-evident seal points to control access during storage or operation and leave physical evidence that an unauthorized event has taken place.	VotingWorks function testing confirms that components cannot be access when seals are placed through seal points.	System Security, Auditing, & Logging > Physical Security
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.	11.2.1-C - Access control by voting stage	printer cover is open during an activated voting stage, VxMark produces a visual and audible alert.	VotingWorks functional and automated testing confirm an alert is produced when the printer cover is opened while polls are opened and no user is authenticated.	System Overview > VxMark Function; System Security, Auditing & Logging > Physical Security
D	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.				
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.		on precinct devices that can be disconnected is a USB drive on VxScan. A visual and audible alert is fired when a USB drive is disconnected during an activated voting stage.	VotingWorks functional and automated testing confirm that alerts are generated in this case.	User Manual > VxScan Error Messages; System Security, Auditing & Logging > Physical Security
D	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 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*.				
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.	11.2.1-C - Access control by voting stage; 15.1-D - Logging event types	connect-to-pat-input-init, usb-device-change-detected. If the entire machine is powered on or off there will be a machine-boot or machine-shutdown log.	VotingWorks functional and automated testing confirm that the relevant logs are generated and are included in the exported logs.	System Security, Auditing, & Logging > Logging
D	Discussion	Logging of the devices is vital for determining cause and providing incident information if a physical security event occurs.				
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.				
D	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. 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		All VxSuite componetns have tamper-evident seals to provide physical evidence that unauthorized access has taken place.	VotingWorks functional testing confirms when tamper-evident seals are installed, cases cannot be opened without breaking or defacing the seal.	System Security, Auditing, & Logging > Physical Security
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.				
D	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 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.		N/A - VxSuite does not use locks.		
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:				
12.1-G.1		produces an alert				
12.1-G.2		happens automatically when primary power is unavailable				
12.1-G.3		generates an event log entry, if possible				
D	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. 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.		N/A - VxSuite does not use powered physical security countermeasures.		
12.2	The voting system only exposes physical ports and access points that are essential to voting operations.					
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.		voting operations. Non essential exposed ports (RJ45 ports) have port blockers installed.	VotingWorks quality assurance checks during production ensure that all RJ45 ports have port blockers installed.	System Security, Auditing & Logging > Physical Security
D	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.				
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.				
D	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 requirement does not include power cabling with a backup power supply or analog accessibility device ports that are used during the activated voting stage.		N/A - there are no ports that support digital communication between voting system components.		
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.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
D	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.		All USB ports that are used for removable media are located in restricted tamper-evident physical locations.	VotingWorks functional testing confirms that all USB ports are located behind restricted tamper-evident physical locations when all procedural and operational security documentation is followed.	System Security, Auditing & Logging > Physical Security; System Security, Auditing & Logging > Procedural and Operational Security
12.2-D	Disabling ports	Voting systems must allow authorized administrators to logically put physical ports into a disabled state.		ports are by default logically disabled on all devices.	essential ports are disabled at the point of production.	System Security, Auditing & Logging; quality-assurance/production
D	Discussion	Logically disabling ports prevents unused ports from being used as a staging point for an attack on the voting system.				
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.	15.1-D - Logging event types	staff through modifying the BIOS configuration of the device. Log entries in syslog document the state of enabled/disabled ports after any BIOS reconfiguration.	VotingWorks staff can logically put physical ports into a disabled state and that syslog documents the state of enabled/disabled ports after BIOS reconfiguration.	System Security, Auditing & Logging; quality-assurance/production
D	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.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
13	Data Protection - The voting system protects data from unauthorized access, modification, or deletion					
13.1	The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.					
13.1.1	Configuration file					
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.	11.2.1-A - Ensuring authorized access	Only system administrators can access the screen to import the initial unsigned election package into VxAdmin. Election packages exported from VxAdmin to configure other machines are digitially signed and cannot be modified. If a signed election package is modified, election package authentication on import will fail, and machines will refuse to import the election package.	VotingWorks functional and automated testing confirms this behavior.	User Manual > Smart Cards and User Roles; User Manual > Configure VxAdmin; System Security, Auditing, & Logging > System Security Architecture > Artifact Authentication
D	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 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. Applies to: Vote-capture and tabulation system				
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.		Only system administrators can access the screen to import the initial unsigned election package into VxAdmin. Election packages exported from VxAdmin to configure other machines are digitially signed and cannot be modified. If a signed election package is modified, election package authentication on import will fail, and machines will refuse to import the election package.	VotingWorks functional and automated testing confirms this behavior.	User Manual > Smart Cards and User Roles; User Manual > Configure VxAdmin; System Security, Auditing, & Logging > System Security Architecture > Artifact Authentication
D	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. Applies to: EMS workstation	11.3.1-C - Multi-factor authentication for administrators; 15.1-E - Configuration file access log			
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.	11.3.1-A - Access control mechanism application	N/A: There are no network appliances so the requirement does not apply.		System Security, Auditing, & Logging > System Security Architecture > Networking
D	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. Applies to: Network appliance				
13.1.2	Election records					
13.1.2-A	Integrity protection for election records	The voting system must integrity prevent modification of CVRs and ballot images when they are stored anywhere within the voting system.	13.2-A - Signing stored election records; 13.2-B - Verification of election records	Cast vote record exports are digitially signed. On VxAdmin import, the records are authenticated. If an export doesn't have a matching signature, VxAdmin will refuse to import it.	VotingWorks functional and automated testing confirms that a cast vote record export without a matching signature cannot be loaded into VxAdmin.	System Security, Auditing, & Logging > System Security Architecture > Artifact Authentication
D	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.				
13.2	The source and integrity of electronic tabulation reports are verifiable					
13.2-A	Signing stored election records	Cast vote records and ballot images must be digitally signed when stored and before being transmitted.		Cast vote record exports are digitially signed. On VxAdmin import, the records are authenticated. If an export doesn't have a matching signature, VxAdmin will refuse to import it.	VotingWorks functional and automated testing confirms that a cast vote record export without a matching signature cannot be loaded into VxAdmin.	System Security, Auditing, & Logging > System Security Architecture > Artifact Authentication
D	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].				
13.2-B	Verification of election records	A voting system must:				
13.2-B.1		cryptographically verify the integrity and authenticity of all election data received		Cast vote record exports are digitially signed. On VxAdmin import, the records are authenticated. If an export doesn't have a matching signature, VxAdmin will refuse to import it.		

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
13.2-B.2		immediately log any verification error of received election results		The log event import-cast-vote-record-complete will be emitted and indicate the verification failed.	VotingWorks functional and automated testing confirms that a cast vote record export without a matching signature cannot be loaded into VxAdmin and results in an on-screen error.	System Security, Auditing, & Logging > System Security Architecture > Artifact Authentication; System Overview > VxAdmin Function
13.2-B.3		immediately present on-screen any verification errors		The import error is presented on screen to the election manager.		
13.2-B.4		not tabulate or aggregate any data that fails verification		Imports that fail verification are not loaded.		
D	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.				
13.3	All cryptographic algorithms are public, well-vetted, and standardized.					
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:		VotingWorks uses only FIPS-compliant cryptographic modules.		System Security, Auditing, & Logging > System Security Architecture > Cryptography > Cryptographic Modules
13.3-A.1		software cryptographic modules		VotingWorks uses the OpenSSL FIPS provider when not using a hardware/TPM provider.	In the basic configuration wizard run on first boot after imaging, we run the mandatory \`openssl fipsinstall\` command to ensure that the FIPS provider is configured correctly and OpenSSL is running in FIPS mode.	System Security, Auditing, & Logging > System Security Architecture > Cryptography > Cryptographic Modules
13.3-A.2		hardware cryptographic modules		VotingWorks uses FIPS-compliant TPM chips and smart cards.	We've identified the CMVP certs for all VotingWorks hardware cryptographic modules.	System Security, Auditing, & Logging > System Security Architecture > Cryptography > Cryptographic Modules
D	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, and quite commonly can use a software module for some functions and a hardware module for other functions.				
13.3-B	E2E cryptographic voting protocols	Cryptographic functions specific to E2E cryptographic voting protocols must adhere to requirements set by the EAC and are omitted from FIPS 140-2 validation.	9.1.6-A - Verified cryptographic protocol	N/A: VxSuite is not a cryptographic E2E verifiable voting system		
D	Discussion	The cryptographic E2E verifiable voting protocol used by the voting system is subject to the evaluation in requirement 9.1.6-B – Verified Cryptographic Protocol. Common place cryptographic operations used within E2E systems, such as encryption, decryption, and hashing, are subject to the FIPS 140 [NIST01, NIST19a] validation requirement. Applies to: Cryptographic E2E verifiable voting systems				
13.3-C	Cryptographic strength	Devices using cryptography must employ NIST approved algorithms with a security strength of at least 112-bits.		VotingWorks uses ECC 256-bit keys for all cryptographic operations, minus Secure Boot code signing, which uses RSA 4096-bit keys.	All cryptographic code is internally security reviewed to ensure that we continue to meet this requirement.	System Security, Auditing, & Logging > System Security Architecture > Cryptography > Cryptographic Keying Material
D	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.				
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.		N/A: VotingWorks does not use Message Authentication Codes.		
D	Discussion	Message authentication codes of 96-bits are conventional in standardized secure communications protocols, and acceptable to protect voting records and systems.				
13.3-E	Cryptographic key management documentation	The voting system documentation must describe how key management is to be performed.		VotingWorks documents its use of cryptographic keys in great detail in the Security Architecture section of its TDP.		System Security, Auditing, & Logging > System Security Architecture
D	Discussion	This document provides procedural steps that can be taken to ease the burden of key management and safely perform these operations.				
13.4	The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.					
13.4-A	Confidentiality and integrity protection of transmitted data	The voting system must:				
13.4-A.1		mutually authenticate all network connections		N/A: The requirement does not apply because no data is sent over a network.		System Security, Auditing, & Logging > Networking
13.4-A.2		cryptographically protect the confidentiality of all data sent over a network				
13.4-A.3		cryptographically protect the integrity of all election data sent over the network				
D	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. 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].				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
14	System Integrity - The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental					
14.1	The voting system uses multiple layers of controls to provide resiliency against security failures or vulnerabilities.					
14.1-A	Risk assessment documentation	The voting system's documentation must contain a risk assessment		Documentation is included in the technical data package.	VotingWorks staff review documentation.	System Security, Auditing, & Logging > Risk Assessment
D	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 Assessments [NIST12] or ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management [ISO18d].				
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.		Documentation is included in the technical data package.	VotingWorks staff review documentation.	System Security, Auditing, & Logging > Risk Assessment
D	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.				
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:	3.1.3-C - Physical security	Documentation is included in the technical data package.	VotingWorks staff review documentation.	System Security, Auditing, & Logging > Risk Assessment; System Security, Auditing, & Logging > System Security Architecture
14.1-C.1		cryptography				
14.1-C.2		malware protection				
14.1-C.3		firewall access control lists, rules, and configurations				
14.1-C.4		system configurations				
D	Discussion	Risk assessments can be large, complicated documents. This requirement ensures that a single narrative exists to explain to election officials and other system owners how the overall security operates for the voting system.				
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.		Documentation is included in the technical data package.	VotingWorks staff review documentation.	User Manual > Setup Inspection
D	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.				
	The voting system limits its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.					
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.		All components have networking completely disabled with multiple layers of defense.	VotingWorks functional testing confirms that components do not have the hardware necessary to connect to a network and, even with network hardware, components do not have the software to utilize it.	System Security; Auditing, & Logging > System Security Architecture > Networking
D	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.				
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.		This requirement does not apply to VxSuite because there is no networking functionality.		
D	Discussion	This helps to ensure that network functionality is not enabled by accident.				
14.2-C	Wireless communication restrictions	Voting systems must not be capable of establishing wireless connections as provided in this section.	8.1-E - Standard audio connectors; 15.4-C - Documentation for disabled wireless	All components are manufactured without wi-fi or bluetooth cards and wireless connections are further disabled at the software level.	VotingWorks functional testing confirms that components do not have the hardware necessary to connect to a wireless network and, even with wireless hardware, components do not have the software to utilize it.	System Security; Auditing, & Logging > System Security Architecture > Networking
D	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. By disallowing wireless capabilities in the voting system, this 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 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.				
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.		This requirement does not apply to VxSuite because there is no networking functionality.		
D	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.	15.4-B - Secure configuration documentation			
14.2-E	External network restrictions	A voting system must not be configured to:		All components have networking completely disabled with multiple layers of defense.	VotingWorks functional testing confirms that components do not have the hardware necessary to connect to a network and, even with network hardware, components do not have the software to utilize it.	System Security, Auditing, & Logging > System Security Architecture > Networking
14.2-E.1		establish a connection to an external network, or				
14.2-E.2		connect to any device external to the voting system				

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
D	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 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.				
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.	15.4-B - Secure network configuration documentation	Together, scripts across https://github.com/votingworks/vxsuite-build-system and https://github.com/votingworks/vxsuite-complete-system ensure that the OS is configured correctly over the course of the build and imaging process.	Final quality control ensures that settings are correct. Settings must also inherently be correct to boot our final signed images, e.g., our signed images won't boot if Secure Boot is not enabled.	Software Installation; System Security, Auditing, & Logging > System Security Architecture > Networking
D	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.				
14.2-G	Unused code	The voting system software must not contain unused, or dead code.		VxSuite does not contain dead code. VotingWorks engineering removes code whenever it becomes unused due to new code being introduced.	Full test coverage requirements force tests to run all code paths, which means no code is dead code. In libraries with limited test coverage, required manual code review ensures dead code is removed.	Quality Assurance Manual > Quality Assurance Protocols – Software
D	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. 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.				
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.		DEP and ASLR are built into the Linux OS that the VotingWorks application is built on.	We've run commands to verify that these mechanisms are active. See the linked TDP section for details.	System Security, Auditing, & Logging > System Security Architecture > Defense-in-Depth and Least Privilege > DEP and ASLR
	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.				
14.2-I	Importing software libraries	The voting system software must import only library components that are necessary.		Our Trusted Build process delineates all required dependencies and guarantees that only those dependencies are installed.		Software Installation > Trusted Build
D	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 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.				
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:		Documentation is included in the technical data package.	VotingWorks staff review documentation.	System Security, Auditing, & Logging > Vulnerability Management
14.2-J.1		how the voting system design process identifies and addresses well-known vulnerabilities				
14.2-J.2		disclosure of all known vulnerabilities within the system				
14.2-J.3		a patch management plan				
14.2-J.4		the method to receive and send reports of vulnerabilities				
D	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 (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].				
14.2-K	Known vulnerabilities	The underlying voting system platform must be free of well-known vulnerabilities as identified in the vulnerability management plan.		Documentation is included in the technical data package.	VotingWorks staff review documentation.	System Security, Auditing, & Logging > Vulnerability Management
D	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.				
14.3	The voting system maintains and verifies the integrity of software, firmware, and other critical components					
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:				
14.3-A.1		a reference to the template or standard used, if any, to develop the supply chain risk management strategy		This requirement does not apply because no template or standard was used.		

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
14.3-A.2		the assurance requirements to mitigate supply chain risks		Documentation is included in the technical data package.	VotingWorks staff review documentation.	System Security, Auditing, & Logging > Hardware Criticality and Supplier Analysis
14.3-A.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				
14.3-A.4		the plan for reviewing and auditing suppliers and partners				
14.3-A.5		the response and recovery plan for a supply chain risk incident				
D	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 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.				
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		Documentation is included in the technical data package.	VotingWorks staff review documentation.	System Security, Auditing, & Logging > Hardware Criticality and Supplier Analysis
D	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].				
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:		Documentation is included in the technical data package.	VotingWorks staff review documentation.	System Security, Auditing, & Logging > Hardware Criticality and Supplier Analysis
14.3-C.1		component name				
14.3-C.2		manufacturer				
14.3-C.3		model or version				
14.3-C.4		applicable platform for software (e.g., Windows or Linux)				
D	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].				
14.3.1	Boot Integrity					
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.		VxSuite components use dm-verity to verify that software has not been tampered with.	VotingWorks functional testing confirms that only signed and unmodified software can be booted successfully on a locked down machine.	System Security, Auditing, & Logging > System Security Architecture > System Integrity
D	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				
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.		If the secure boot dm-verity check fails, the voting system will not boot and the error is presented on screen.	VotingWorks functional testing confirms that boot fails and a notification occurs when secure boot detects modified code. This can only be tested special development software releases that allow editing code.	System Security, Auditing, & Logging > System Security Architecture > System Integrity
D	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				
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.		If the secure boot dm-verity check fails, the voting system will not boot and the error is presented on screen.	VotingWorks functional testing confirms that a notification occurs when secure boot detects modified code. This can only be tested special development software releases that allow editing code.	System Security, Auditing, & Logging > System Security Architecture > System Integrity
D	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, EMS				
14.3.2	Software Integrity					
14.3.2-A	Installing software	The voting system must only allow digitally signed software and firmware to be installed.		VxSuite prevents unsigned software and firmware from being installed by using secure boot to only allow booting signed VotingWorks images.	VotingWorks functional testing confirms that attempts to install unsigned software fail due to failed secure boto checks.	System Security, Auditing, & Logging > System Security Architecture > System Integrity; Software Installation
D	Discussion	Signed software and firmware ensures that it is not modified before installation, and that it is being distributed by the proper entity.				
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.				
D	Discussion	The security properties of integrity and authenticity are not achieved unless the digital signature for the signed software and firmware is cryptographically verified.				
14.3.2-C	Application allowlisting	The voting system must only run applications that have been verified against an allowlist.		Allowlists are not relevant to VxSuite's security architecture. The voting system components can only run the installed application and new applications cannot be added.		System Security, Auditing, & Logging > System Security Architecture > System Integrity
D	Discussion	This requirement helps ensure only authorized applications run on the voting system. Applies to: Vote-capture device				
14.3.2-D	Integrity protection for software allowlists	The voting system must protect the integrity and authenticity of the allowlist configuration files.				
D	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.				
14.4	Voting system software updates are authorized by an administrator prior to installation.					

VVSG 2.0 Section	Title	Requirement/Discussion Text	Related Requirements	How VxSuite Meets	How VotingWorks Test	TDP Reference
14.4-A	Authenticated operating system updates	The voting system must authenticate administrators before an operating system update is performed.	11.3.1-B - Multi-factor authentication for critical operations; 11.3.1-C - Multi-factor authentication for administrators	MFA for system updates is not application to VxSuite's security architecture. Operating system update, software updates, and firmware updates cannot be performed in the context of the voting system. The only way to perform those updates is to fully re-install the a digitally signed software release onto the hardware, which necessarily happens outside of the context of the voting system.		System Security, Auditing, & Logging > System Security Architecture > System Integrity; Software Installation
D	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.				
14.4-B	Authenticated application updates	The voting system must authenticate administrators before a software update to the voting system application and related software.	11.3.1-B - Multi-factor authentication for critical operations; 11.3.1-C - Multi-factor authentication for administrators			
D	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.				
14.4-C	Authenticated firmware updates	The voting system must authenticate administrators before a firmware or driver update.	11.3.1-B - Multi-factor authentication for critical operations; 11.3.1-C - Multi-factor authentication for administrators			
D	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.				

VVSG 2.0 Section	Title	Requirement/Discussion Text	How VxSuite Meets	How VotingWorks Test	TDP Reference
15	Detection and Monitoring - The voting system provides mechanisms to detect anomalous or malicious behavior.				
15.1	Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.				
15.1-A	Event logging	The voting system must be capable of logging events that occur in a voting system.	The voting system logs events that occur in the system. More information can be found in the logging documentation.	VotingWorks functional testing confirms that logs are created and available in the exported logs.	System Security, Auditing, & Logging > Logging
D	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.			
15.1-B	Exporting logs	The voting system must be capable of exporting logs.	A system administrator can, at any time, export logs in full, export error-only logs, or export the logs in CDF format. More information can be found in the logging documentation.	VotingWorks functional and automated testing confirms that system administrators can always export logs.	System Security, Auditing, & Logging > Logging
D	Discussion	Exporting logs offers the opportunity for external review, clearing storage, and a method to compare with future logs.			
15.1-C	Logging voter information	The voting system must not log any information:	All logs produced by VxSuite applications do not contain any information that could identify a voter or tie a voter to a ballot.	VotingWorks staff manually audit all code changes to ensure that logs containing voter identifiable information are not introduced to the system. A final code review audit was performed of all points in the code where a log is emitted to ensure that no voter identifying information could be recorded. Logs are exported from VotingWorks applications in functional testing and checked for unexpected identifying information.	System Security, Auditing, & Logging > Logging
15.1-C.1		identifying a specific voter			
15.1-C.2		connecting a voter to a specific ballot			
D	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.			
15.1-D	Logging event types	At minimum, the voting system must log the events included in Table 15-1.			
15.1-D.1		General System Functions			
15.1-D.1.a		Device generated error and exception messages - 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. 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.			
15.1-D.1.b		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			
15.1-D.1.c		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			
15.1-D.1.d		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			
15.1-D.1.e		Device shutdown and restarts - Both normal and abnormal device shutdowns and restarts			
15.1-D.1.f		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			
15.1-D.1.g		Integrity checks for executables, configuration files, data, and logs - Integrity checks that can indicate possible tampering with files and data			
15.1-D.1.h		The addition and deletion of files - Files that are added or deleted from the voting device			
15.1-D.1.i		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 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			
15.1-D.1.j		Removable media events - Removable media that is inserted into or removed from the voting device			
15.1-D.1.k		Backup and restore - Successful and failed attempts to perform backups and restores.			
15.1-D.2		Authentication and Access Control			
15.1-D.2.a		Authentication related events - Includes but is not limited to: Login/logoff events (both successful and failed attempts); Account lockout events; Password changes			
15.1-D.2.b		Access control related events - Includes but is not limited to: Use of privileges (such as a user running a process as an administrator); Attempts to exceed privileges; All access attempts to application and underlying system resources; Changes to the access control configuration of the voting device			
15.1-D.2.c		User account and role (or groups) management activity - Includes but is not limited to: Addition and deletion of user accounts and roles; User account and role suspension and reactivation; Changes to account or role security attributes such as password length, access levels, login restrictions, and permissions; Administrator account and role password resets			
15.1-D.3		Networking			
15.1-D.3.a		Enabling or disabling networking functionality - Includes but is not limited to: Wired networking; Wireless networking			
15.1-D.4		Software			
15.1-D.4.a		Installing, upgrading, patching, or modifying software or firmware - Logging for installation, upgrading, patching, or modifying software or firmware include logging what was installed, upgraded, or modified as well as a cryptographic hash or other secure identifier of the old and new versions of the data.			

VVSG 2.0 Section	Title	Requirement/Discussion Text	How VxSuite Meets	How VotingWorks Test	TDP Reference
15.1-D.4.b		Changes to configuration settings - Includes but is not limited to: Changes to critical function settings. At a minimum, critical function settings include location of election definition file, contents of the election definition file, vote reporting, location of logs, and voting device configuration settings; Changes to device settings including, but not limited to, enabling and disabling services; Starting and stopping processes	Each logging requirement is mapped to its VotingWorks log event in the 15.1-D table in System Security, Auditing, & Logging > Logging	VotingWorks staff review that all required VVSG 2.0 log events are covered by VotingWorks log events. VotingWorks functional and automated testing confirms that when these events occur the appropropriate logs are actually emitted and readable in the exported logs.	System Security, Auditing, & Logging > Logging
15.1-D.4.c		Abnormal process exits - All abnormal process exits.			
15.1-D.4.d		Successful and failed database connection attempts (if a database is uses) - All database connection attempts.			
15.1-D.4.e		Changes to cryptographic keys - At a minimum, critical cryptographic settings include key addition, key removal, and re-keying.			
15.1-D.5		Voting Functions			
15.1-D.5.a		Ballot definition and modification - During election definition and ballot preparation, the device can provide logging information for preparing the baseline ballot formats and modifications to them, including a description of the modification and corresponding dates. Includes but is not limited to: The account name that made the modifications. A description of what was modified including the file name, location, and the content changed. The date and time of the modification			
15.1-D.5.b		Voting events - Includes: Opening and closing polls; Casting a vote; Canceling a vote during verification; Success or failure of log and election results exportation; Note: for paper-based devices, these requirements might need to be met procedurally.			
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.	System administrators cannot access configuration files at the operating system level. Whenever a system administrator imports or exports configuration for an election, that event is logged. See event codes save-election-package-init, save-election-package-complete, and election-package-load-from-usb-complete.	VotingWorks function penetration confirms that system configuration files are inaccessible and election configuration actions generate log events.	System Security, Auditing, & Logging > System Security Architecture; System Security, Auditing, & Logging > Logging
D	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.			
15.2	The voting system generates, stores, and reports all error messages as they occur.				
15.2-A	Presentation of voting application errors	The voting system must provide immediate notification to the user when a voting application error occurs.	All errors result in the immediate presentation of the error to the user.	VotingWorks testing staff confirm that all encountered errors are accompanied by user notifications.	User Manual; User Manual > [Component] Error Messages
D	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.			
15.2-B	Voting application error handling documentation	The voting system documentation must include procedures for handling voting application errors.	Documentation is included in the user manual.	VotingWorks staff review documentation.	User Manual; User Manual > [Component] Error Messages
D	Discussion	Documentation will assist election officials with steps to properly address errors.			
15.2-C	Logging system errors	The voting system must log system errors.	All errors result in an entry in the audit log record with the disposition of failure.	VotingWorks functional and automated testing confirms that system errors are logged.	System Security, Auditing, & Logging > Logging
D	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.			
15.2-D	Creating error reports	The voting system must be capable of creating error reports.	A system administrator or election manager can export error-only logs on all VxSuite devices.	VotingWorks functional and automated testing confirms that error-only logs can be exported and contain the appropriate logs.	User Manual > Retaining and Removing Files; System Security, Auditing, & Logging > Logging
D	Discussion	Error reports allow system administrators to easily analyze the errors that occurred within a system.			
15.3	The voting system is designed to protect against malware.				
15.3-A	Malware protection mechanisms	COTS workstations providing EMS functionality must deploy mechanisms to protect against malware.	VxSuite software is architected to prevent any new code from being added or executed after installation.	VotingWorks functional testing confirms that attempts to edit or add executables are blocked and, when allowed for testing purposes, result in the device failing secure boot.	System Security, Auditing, & Logging > System Security Architecture > System Integrity
D	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).			
15.3-B	Updatable malware protection mechanisms	The malware protection mechanisms for COTS devices providing EMS functionality must be updatable.	N/A - This requirement does not apply to VxSuite. Because VxSuite protects against malware by preventing any new executables from being added to the system, there is no purpose in maintaining or updating a catalog of malware signatures.		
D	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. Applies to: EMS Workstations, vote-capture and tabulation devices.			
15.3-C	Documenting malware protection mechanisms	The voting system documentation must include the process and procedures for updating malware protection mechanisms.	N/A - This requirement does not apply to VxSuite. Because VxSuite protects against malware by preventing any new executables from being added to the system, there is no purpose in maintaining or updating a catalog of malware signatures.		
	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.			

VVSG 2.0 Section	Title	Requirement/Discussion Text	How VxSuite Meets	How VotingWorks Test	TDP Reference
15.3-D	Notification of malware detection	COTS workstations and servers providing EMS functionality must immediately notify an election official when malware is detected.	If malware were detected on boot, the boot fails and presents the election official with a notification.	VotingWorks functional testing confirms that a notification occurs when secure boot detects modified code. This can only be tested special development software releases that allow editing code.	System Security, Auditing, & Logging > System Security Architecture > System Integrity
D	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).			
15.3-E	Logging malware detection	The voting system must log instances of detecting malware.	If malware were detected on boot, the failed dm-verity check would result in a log entry.	VotingWorks functional testing confirms that appropriate logs are produced when secure boot detects modified code. This can only be tested special development software releases that allow editing code.	System Security, Auditing, & Logging > Logging
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.	N/A - This requirement does not apply to VxSuite because VxSuite protects against malware by preventing any new executables from being added to the system, so there is no removal or remediation process. If malware were detected, the device would be unusable and returned to VotingWorks for inspection.		
D	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)			
15.3-G	Logging malware remediation	The voting system must log malware remediation activities.	N/A - This requirement does not apply to VxSuite because VxSuite protects against malware by preventing any new executables from being added to the system, so there is no removal or remediation process. If malware were detected, the device would be unusable and returned to VotingWorks for inspection.		
D	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.			
15.4	A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practices.				
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.	N/A - This requirement does not apply because VxSuite devices are not networked and cannot be networked.		
D	Discussion	Documentation of the internal network architecture can assist with data flow analysis, proper network configuration, and architecture to properly support the voting system. Applies to: Voting systems with networking capabilities			
15.4-B	Secure network configuration documentation	The voting system documentation must list security configurations and be accompanied by network security best practices.	N/A - This requirement does not apply because VxSuite devices are not networked and cannot be networked.		
D	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. 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].			
15.4-C	Documentation for disabled wireless	The voting system documentation must include information about how wireless is disabled within the voting system.	Documentation is included in the technical data package.	VotingWorks staff reviews documentation.	System Security; Auditing, & Logging > System Security Architecture > Networking
D	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 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. Applies to: Voting systems with networking capabilities			
15.4-D	Rule and policy updates	The voting system must be capable of updating rules and policies for network appliances.	apply to VxSuite because there are no network appliances.		
D	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.			