Implementation Statement

Manufacturer: **Dominion Voting Systems** *Product*: **Democracy Suite 5.5-A** *Date*: **10/31/18**

This document describes the implementation of the system defined above. Within this document is the following:

- an overview of the system,
- a high level functional diagram,
- the primary components included and their release version numbers,
- the system's limitations, and
- a conformity statement.

System Overview:

The Dominion Democracy Suite 5.5-A Voting System is a modification to the certified Democracy Suite 5.5 Voting System. The primary purpose of this modification is to meet requirements in the State of Pennsylvania. Minor modifications to the ImageCast X (ICX) software were necessary to be compliant. In addition, the ICX DRE configuration was removed from the component list for this system, as was the ICX Classic 15in. unit. For more details regarding the Democracy Suite System, please refer to the document filename "2.02-DemocracySuiteSystemOverview-5.5-A.pdf", which accompanies the application.

The list below includes changes between this Democracy Suite 5.5-A system and a baseline of the Democracy Suite 5.5 Voting System:

General

- Removed the ICX DRE configuration as it was not required by the State of Pennsylvania
- Removed the ICX Classic 15" model for marketing purposes

ICX General

- Modification to ICX straight party behavior to show a modal pop-up window when a voter attempts to undervote a partisan contest after selecting a partisan choice in the straight party contest; the pop-up clarifies that the voter needs to remove their straight-party vote and manually vote all partisan contests if they wish for one or more of those contests affected by the straight party vote to be undervoted
- Updated default ICX localizations to change wording of final voter session wording to reflect that the ballot is being printed rather than cast
- Used MCF v5.5.10.19 (EMS 5.5 default configuration file for the ICX) as changes to MCF v5.5.10.20 from D-Suite 5.5 were related to VVPAT printer component and not relevant to the 5.5-A system configuration

The Dominion Voting Systems Democracy Suite 5.5-A System is a paper-based optical scan voting system. The certified system consists of four major components:

1. Election Management System (EMS)

2. ImageCast X (ICX BMD) ballot making device

3. ImageCast Precinct (ICP) precinct scanner

4. ImageCast Central (ICC) central count scanner

Below is a description of the Democracy Suite 5.5-A components.

1. Election Management System

The Democracy Suite 5.5-A EMS set of applications are responsible for all pre-voting and post-voting groups of activities in the process of defining and managing elections. The Dominion Voting Systems Democracy Suite 5.5-A EMS consists of following components running as either a front-end/client application or as a back-end/server application. Below is a list and brief description of each.

- EMS Election Event Designer client application (EED) – integrates election definition functionality and represents a main pre-voting phase end-user application.
- EMS Results Tally and Reporting client application (RTR) – integrates election results acquisition, validation, tabulation, reporting and publishing capabilities and represents a main post-voting phase end-user application.
- EMS Audio Studio client application (AS) – represents an end-user helper application used to record audio files for a given election project. As such, it is utilized during the pre-voting phase of the election cycle.
- EMS Election Data Translator (EDT) – represents an end-user application to export election data from an election project and import election data into an election project.
- EMS Application Server application – represents a server side application responsible for executing long running processes, such as rendering ballots, generating audio files and election files.
- EMS Database Server application – represents a server side RDBMS repository of the election project database which holds all the election project data, such as districts, precincts, candidates, contests, ballot layouts, tabulators, vote totals, and poll status.
- EMS Network Attached Storage (NAS) server application – represents a server side file repository for election project file based artifacts, such as ballots, audio files, reports, log files, and election files.

- EMS Server Applications and Services
    - EMS Data Center Manager server application – represents a system level configuration application used in EMS back-end data center configuration.
    - EMS File System Service client application – a stand-alone service that runs on client machines, enabling access to low level operating system API for partitioning CF cards, reading raw partition on ICP CF card, etc.
    - EMS Adjudication Services server application – provides ballot information such as contest, candidates and their coordinates from the EMS to the Adjudication client application.
    - EMS Smart Card Helper – service that is installed on an ImageCast Voter Activation workstation to provide the required data format for programming smart cards for the ICX devices.
- EMS Adjudication client application (ADJ) – optional application that reviews voter intent on a ballot by ballot basis from the ImageCast Central device utilized during either the absentee voting or post-voting activity phases.
- EMS ImageCast Voter Activation – application installed on a workstation at the polling place that allows pollworkers to program smart cards, which are used by voters to activate voting sessions on an ImageCast X terminal.

The EMS platform is available in two deployable physical hardware configurations:

- ***EMS Express hardware configuration*** - all EMS software components are installed on a single physical PC with the option to use the EMS client components on one or more physical PCs that are connected to the server through a Local Area Network (LAN).
- ***EMS Standard hardware configuration*** - the EMS server components are installed on a single physical server, in addition to the LAN switch devices, while the EMS client components are installed on one or more physical PCs or laptops. All system components are interconnected in a client-server local LAN environment.

2. ImageCast X (ICX) precinct ballot making device

The ImageCast X consists exclusively of COTS available hardware and operating system, while the applications installed on top customize its behavior as a Ballot Marking Device (BMD). The ImageCast X application is the software that verifies a voter's session eligibility, using the smart card, and then presents the appropriate ballot to the voter. When a voter is satisfied with choices selected, ImageCast X application verifies them and produces an Electronic Mobile Ballot. The ImageCast X is designed to perform the following functions:

- Ballot marking and printing of electronic mobile ballots
- Ballot review and second chance voting
- Accessible voting and ballot marking

3. ImageCast Precinct (ICP) precinct scanner

The ImageCast Precinct Ballot Counter is a precinct-based optical scan ballot tabulator that is used in conjunction with ImageCast compatible ballot storage boxes. The system is designed to scan marked paper ballots printed on standard or secure paper stock, interpret voter marks on the paper ballot, and safely store and tabulate each vote from each paper ballot. The ImageCast Precinct also supports enhanced accessibility voting through optional accessories connected to the ImageCast unit. In combination with ImageCast X ballot marking platform, ImageCast Precinct provides capability to review and verify electronic mobile ballots produced by the ImageCast X ballot marking platform.

4. ImageCast Central (ICC) central count scanner

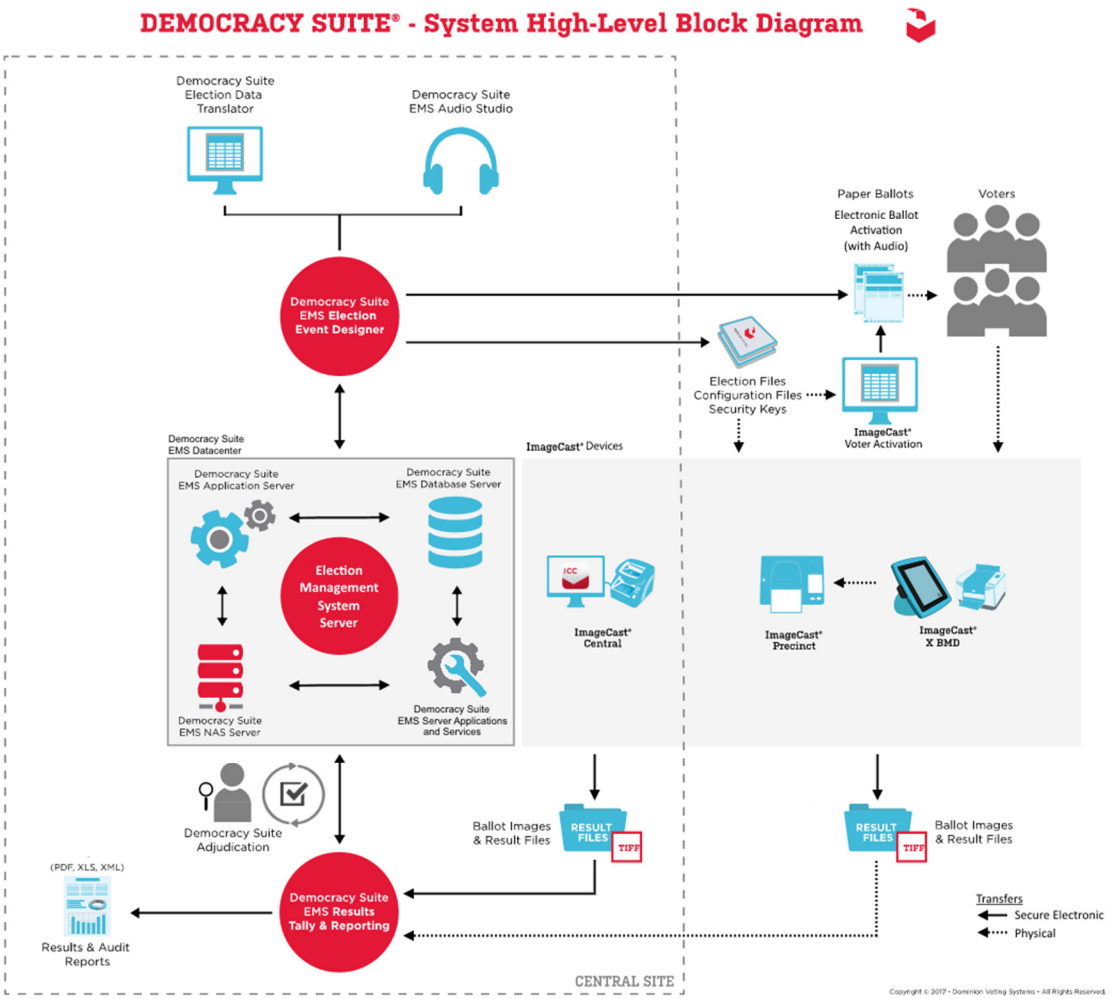
The Dominion Democracy Suite ICC Ballot Counter system is a high-speed, central optical scan ballot tabulator based on Commercial off the Shelf (COTS) hardware, coupled with the custom-made ballot processing application software. It is used for high speed scanning and counting of paper ballots. For the Canon scanners, the central scanning system hardware consists of a combination of two COTS devices used together to provide the required ballot scanning processing functionality; a scanner, which is used to provide ballot scanning and image transfers to the local ImageCast Central Workstation, and a COTS computer used for ballot image and election rules processing and results transfer to the EMS Datacenter. The ImageCast Central Workstation is COTS hardware which executes software for both image processing and election rules application. The COTS scanners supported by D-Suite 5.5-A are:

- Canon DR-G1130 Scanner
- Canon DR-M160 II Scanner

Manufacturer: **Dominion Voting Systems**

Functional Diagram

Below is a functional diagram of the Democracy Suite 5.5-A System.



Components Included

This table provides information describing the primary components and revision level included in this application.

System Component	Software or Firmware Version	Hardware Version	Operating System or COTS
ImageCast Precinct	5.5.3-0002	320A	uClinux
ImageCast Precinct	5.5.3-0002	320C	uClinux
ImageCast X BMD	5.5.10.30	Avalue SID-21V-Z37 Avalue HID-21V-BTX HP M402dn HP M402dne	Android 4.4 Android 5.1

Manufacturer: **Dominion Voting Systems**

System Component	Software or Firmware Version	Hardware Version	Operating System or COTS
ImageCast Voter Activation	5.5.12.1	N/A (application software)	Windows 10
ImageCast Central	5.5.3.0002	Canon DR-G1130 Canon DR-M160 II	Windows 10
Democracy Suite Election Management System	5.5.12.1	N/A (application software)	Windows Server 2012 R2 Windows 10
Democracy Suite EMS Adjudication	5.5.8.1	N/A (application software)	Windows 10
Democracy Suite EMS Adjudication Services	5.5.8.1	N/A (application software)	Windows Server 2012 R2

System Limitations

This table depicts the limits for the system in this application.

Characteristic	Limiting Component	Limit	Comment
Ballot positions	The ballot	462	Standard Configuration
Precincts in an election	EMS	1000	Standard Configuration
Contests in an election	EMS	1000	Standard Configuration
Candidates/Counters in an election	EMS	10000	Standard Configuration
Candidates/Counters in a precinct	Tabulator	462	Standard Configuration
Candidates/Counters in a tabulator	Tabulator	10000	Standard Configuration
Ballot Styles in an election	Tabulator	3000	Standard Configuration
Ballot IDs in a tabulator	ICP	200	Standard Configuration
Contests in a ballot style	ICX	156	Standard Configuration
Candidates in a contest	EMS	231	Standard Configuration
Ballot styles in a precinct	Tabulator	5	Standard Configuration
Number of political parties	Tabulator	30	Standard Configuration
“vote for” in a contest	Tabulator	30	Standard Configuration
Supported languages in an election	Tabulator	5	Standard Configuration
Number of write-ins	The ballot	462	Standard Configuration
Ballot positions	The ballot	462	Express Configuration
Precincts in an election	EMS	250	Express Configuration
Contests in an election	EMS	250	Express Configuration
Candidates/Counters in an election	EMS	2500	Express Configuration
Candidates/Counters in a precinct	Tabulator	462	Express Configuration
Candidates/Counters in a tabulator	EMS	2500	Express Configuration
Ballot Styles in an election	EMS	750	Express Configuration
Ballot IDs in a tabulator	ICP	200	Express Configuration
Contests in a ballot style	ICX	156	Express Configuration
Candidates in a contest	EMS	231	Express Configuration
Ballot styles in a precinct	Tabulator	5	Express Configuration
Number of political parties	Tabulator	30	Express Configuration

Manufacturer: **Dominion Voting Systems**

Characteristic	Limiting Component	Limit	Comment
"vote for" in a contest	Tabulator	30	Express Configuration
Supported languages in an election	Tabulator	5	Express Configuration
Number of write-ins	The ballot	462	Express Configuration

Conformity Statement: 2005 VVSG

Below is a checklist identifying all the requirements for which a claim of conformance is being made.

Requirement	***Requirement Text***	***Conform***
2	Functional Requirements	
2.1	Overall System Capabilities	
2.1.1	Security System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, all systems shall:	
2.1.1.a.	Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability	***YES***
2.1.1.b	Provide system functions that are executable only in the intended manner and order, and only under the intended conditions	***YES***
2.1.1.c	Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met	***YES***
2.1.1.d	Provide safeguards in response to system failure to protect against tampering during system repair or interventions in system operations	***YES***
2.1.1.e	Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation	***YES***
2.1.1.f	Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled	***YES***
2.1.1.g	Provide documentation of mandatory administrative procedures for effective system security	***YES***
2.1.2	Accuracy Memory hardware, such as semiconductor devices and magnetic storage media, must be accurate. The design of equipment in all voting systems shall provide for the highest possible levels of protection against mechanical, thermal, and electromagnetic stresses that impact system accuracy. Section 4 provides additional information on susceptibility requirements. To ensure vote accuracy, all systems shall:	
2.1.2.a	Record the election contests, candidates, and issues exactly as defined by election officials	***YES***
2.1.2.b	Record the appropriate options for casting and recording votes	***YES***
2.1.2.c	Record each vote precisely as indicated by the voter and produce an accurate report of all votes cast;	***YES***
2.1.2.d	Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy	***YES***
2.1.2.e	Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected	***YES***
2.1.2.f	In addition, DRE systems shall: As an additional means of ensuring accuracy in DRE systems, voting devices shall record and retain redundant copies of the original ballot image. A ballot image is an electronic record of all votes cast by the voter, including undervotes.	***YES***
2.1.3	Error Recovery To recover from a non-catastrophic failure of a device, or from any error or malfunction that is within the operator's ability to correct, the system shall provide the following capabilities:	

Requirement	*Requirement Text*	*Conform*
2.1.3.a	Restoration of the device to the operating condition existing immediately prior to the error or failure, without loss or corruption of voting data previously stored in the device.	***YES***
2.1.3.b	Resumption of normal operation following the correction of a failure in a memory component, or in a data processing component, including the central processing unit	***YES***
2.1.3.c	Recovery from any other external condition that causes equipment to become inoperable, provided that catastrophic electrical or mechanical damage due to external phenomena has not occurred	***YES***
2.1.4	Integrity measures ensure the physical stability and function of the vote recording and counting processes. To ensure system integrity, all systems shall:	
2.1.4.a	Protect against a single point of failure that would prevent further voting at the polling place	***YES***
2.1.4.b	Protect against the interruption of electrical power	***YES***
2.1.4.c	Protect against generated or induced electromagnetic radiation	***YES***
2.1.4.d.	Protect against ambient temperature and humidity fluctuations	***YES***
2.1.4.e	Protect against the failure of any data input or storage device	***YES***
2.1.4.f	Protect against any attempt at improper data entry or retrieval	***YES***
2.1.4.g	Record and report the date and time of normal and abnormal events	***YES***
2.1.4.h	Maintain a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g., during the canvassing process)	***YES***
2.1.4.i	Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator	***YES***
2.1.4.j	Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability	***YES***
2.1.4.k	In addition to the common requirements, DRE systems shall: Maintain a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path	***YES***
2.1.4.l	In addition to the common requirements, DRE systems shall: Provide a capability to retrieve ballot images in a form readable by humans	***YES***
2.1.5	System Audit	

Requirement	Requirement Text	Conform
2.1.5	This subsection describes the context and purpose of voting system audits and sets forth specific functional requirements. Election audit trails provide the supporting documentation for verifying the accuracy of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation. These requirements are based on the premise that system-generated creation and maintenance of audit records reduces the chance of error associated with manually generated audit records. Because most audit capability is automatic, the system operator has less information to track and record, and is less likely to make mistakes or omissions. The subsections that follow present operational requirements critical to acceptable performance and reconstruction of an election. Requirements for the content of audit records are described in Section 5. The requirements for all system types, both precinct and central count, are described in generic language. Because the actual implementation of specific characteristics may vary from system to system, it is the responsibility of the vendor to describe each system's characteristics in sufficient detail so that test labs and system users can evaluate the adequacy of the system's audit trail. This description shall be incorporated in the System Operating Manual, which is part of the Technical Data Package. Documentation of items such as paper ballots delivered, paper ballots collected, administrative procedures for system security, and maintenance performed on voting equipment are also part of the election audit trail, but are not covered in these technical standards. Useful guidance is provided by the Innovations in Election Administration #10; Ballot Security and Accountability, available on the EAC's website.	
2.1.5.1	Operational Requirements	
2.1.5.1	Audit records shall be prepared for all phases of election operations performed using devices controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records shall address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. The software shall activate the logging and reporting of audit data as described below.	***YES***
2.1.5.1.a	Time and Sequence of Audit Records The timing and sequence of audit record entries is as important as the data contained in the record. All voting systems shall meet the requirements for time, sequence and preservation of audit records outlined below.	***YES***
2.1.5.1.a.i	Except where noted, systems shall provide the capability to create and maintain a real-time audit record. This capability records and provides the operator or precinct official with continuous updates on machine status. This information allows effective operator identification of an error condition requiring intervention, and contributes to the reconstruction of election-related events necessary for recounts or litigation.	***YES***
2.1.5.1.a.ii	All systems shall include a real-time clock as part of the system's hardware. The system shall maintain an absolute record of the time and date or a record relative to some event whose time and data are known and recorded.	***YES***
2.1.5.1.a.iii.	All audit record entries shall include the time-and-date stamp.	***YES***
2.1.5.1.a.iv.	The audit record shall be active whenever the system is in an operating mode. This record shall be available at all times, though it need not be continually visible.	***YES***
2.1.5.1.a.v	The generation of audit record entries shall not be terminated or altered by program control, or by the intervention of any person. The physical security and integrity of the record shall be maintained at all times.	***YES***
2.1.5.1.a.vi.	Once the system has been activated for any function, the system shall preserve the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed.	***YES***

Requirement	*Requirement Text*	*Conform*
2.1.5.1.a.vii.	The system shall be capable of printing a copy of the audit record. A separate printer is not required for the audit record, and the record may be produced on the standard system printer if all the following conditions are met: • The generation of audit trail records does not interfere with the production of output reports • The entries can be identified so as to facilitate their recognition, segregation, and retention • The audit record entries are kept physically secure	***YES***
2.1.5.1.b	Error messages All voting systems shall meet the requirements for error messages below.	
2.1.5.1.b.i.	The voting system shall generate, store, and report to the user all error messages as they occur.	***YES***
2.1.5.1.b.ii	All error messages requiring intervention by an operator or precinct official shall be displayed or printed clearly in easily understood language text, or by means of other suitable visual indicators.	***YES***
2.1.5.1.b.iii	When the voting system uses numerical error codes for trained technician maintenance or repair, the text corresponding to the code shall be self-contained, or affixed inside the voting machine. This is intended to reduce inappropriate reactions to error conditions, and to allow for ready and effective problem correction.	***YES***
2.1.5.1.b.iv.	All error messages for which correction impacts vote recording or vote processing shall be written in a manner that is understandable to an election official who possesses training on system use and operation, but does not possess technical training on system servicing and repair.	***YES***
2.1.5.1.b.v.	The message cue for all voting systems shall clearly state the action to be performed in the event that voter or operator response is required.	***YES***
2.1.5.1.b.v.i.	Voting system design shall ensure that erroneous responses will not lead to irreversible error.	***YES***
2.1.5.1.b.v.ii.	Nested error conditions shall be corrected in a controlled sequence such that voting system status shall be restored to the initial state existing before the first error occurred.	***YES***
2.1.5.1.c.	Status Messages	
2.1.5.1.c.	The Guidelines provide latitude in software design so that vendors can consider various user processing and reporting needs. The jurisdiction may require some status and information messages to be displayed and reported in real-time. Messages that do not require operator intervention may be stored in memory to be recovered after ballot processing has been completed. The voting system shall display and report critical status messages using clear indicators or English language text. The voting system need not display non-critical status messages at the time of occurrence. Voting systems may display non-critical status messages (i.e., those that do not require operator intervention) by means of numerical codes for subsequent interpretation and reporting as unambiguous text. Voting systems shall provide a capability for the status messages to become part of the real-time audit record. The voting system shall provide a capability for a jurisdiction to designate critical status messages.	***YES***
2.1.5.2	Use of Shared Computing Platforms (COTS operating system (off-the-shelf))	

Requirement	Requirement Text	Conform
2.1.5.2	Further requirements must be applied to Commercial-off-the-Shelf operating systems to ensure completeness and integrity of audit data for election software. These operating systems are capable of executing multiple application programs simultaneously. These systems include both servers and workstations, including the many varieties of UNIX and Linux, and those offered by Microsoft and Apple. Election software running on these systems is vulnerable to unintended effects from other user sessions, applications, and utilities executing on the same platform at the same time as the election software. "Simultaneous processes" of concern include: unauthorized network connections, unplanned user logins, and unintended execution or termination of operating system processes. An unauthorized network connection or unplanned user login can host unintended processes and user actions, such as the termination of operating system audit, the termination of election software processes, or the deletion of election software audit and logging data. The execution of an operating system process could be a full system scan at a time when that process would adversely affect the election software processes. Operating system processes improperly terminated could be system audit or malicious code detection. To counter these vulnerabilities, three operating system protections are required on all such systems on which election software is hosted. First, authentication shall be configured on the local terminal (display screen and keyboard) and on all external connection devices ("network cards" and "ports"). This ensures that only authorized and identified users affect the system while election software is running. Second, operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object. This ensures the accuracy and completeness of election data stored on the system. It also ensures the existence of an audit record of any person or process altering or deleting system data or election data. Third, the system shall be configured to execute only intended and necessary processes during the execution of election software. The system shall also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software.	***YES***
2.1.6	Election Management System The Election Management System (EMS) is used to prepare ballots and programs for use in casting and counting votes, and to consolidate, report, and display election results. An EMS shall generate and maintain a database, or one or more interactive databases, that enables election officials or their designees to perform the following functions: • Define political subdivision boundaries and multiple election districts as indicated in the system documentation • Identify contests, candidates, and issues • Define ballot formats and appropriate voting options • Generate ballots and election-specific programs for voting equipment • Install ballots and election-specific programs • Test that ballots and programs have been properly prepared and installed •Accumulate vote totals at multiple reporting levels as indicated in the system documentation •Generate the post-voting reports required by Subsection 2.4 •Process and produce audit reports of the data as indicated in Subsection 5.5	***YES***
2.1.7	Vote Tabulating Program Each voting system shall have a vote tabulation program that will meet specific functional requirements.	
2.1.7.1	Functions The vote tabulating program software resident in each voting machine, vote count server, or other devices shall include all software modules required to:	
2.1.7.1.a.	Monitor system status and generate machine-level audit reports	***YES***

Requirement	Requirement Text	Conform
2.1.7.1.b.	Accommodate device control functions performed by polling place officials and maintenance personnel	YES
2.1.7.1.c.	Register and accumulate votes	YES
2.1.7.1.d.	Accommodate variations in ballot counting logic	YES
2.1.7.2	Voting Variation There are significant variations among state election laws with respect to permissible ballot contents, voting options, and the associated ballot counting logic. The Technical Data Package accompanying the system shall specifically identify which of the following items can and cannot be supported by the voting system, as well as how the voting system can implement the items supported:	
2.1.7.2	Closed primaries	YES
2.1.7.2	Open primaries	YES
2.1.7.2	Partisan offices	YES
2.1.7.2	Non-partisan offices	YES
2.1.7.2	Write-in voting	YES
2.1.7.2	Primary presidential delegation nominations	YES
2.1.7.2	Ballot rotation	YES
2.1.7.2	Straight party voting	YES
2.1.7.2	Cross-party endorsement	N/A
2.1.7.2	Split precincts	YES
2.1.7.2	Vote for N of M	YES
2.1.7.2	Recall issues, with options	YES
2.1.7.2	Cumulative voting	N/A
2.1.7.2	Ranked order voting	N/A
2.1.7.2	Provisional or challenged ballots	YES
2.1.8	Ballot Counter For all voting systems, each piece of voting equipment that tabulates ballots shall provide a counter that:	
2.1.8.a.	Can be set to zero before any ballots are submitted for tally	YES
2.1.8.b.	Records the number of ballots cast during a particular test cycle or election	YES
2.1.8.c.	Increases the count only by the input of a ballot	YES
2.1.8.d.	Prevents or disables the resetting of the counter by any person other than authorized persons at authorized points	YES
2.1.8.e.	Is visible to designated election officials	YES
2.1.9	Telecommunications	
2.1.9	For all voting systems that use telecommunications for the transmission of data during pre-voting, voting or post-voting activities, capabilities shall be provided that ensure data are transmitted with no alteration or unauthorized disclosure during transmission. Such transmissions shall not violate the privacy, secrecy, and integrity demands of the Guidelines. Section 6 describes telecommunications standards that apply to, at a minimum, the following types of data transmissions: ♦Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmit votes individually over a public network ♦Ballot Definition: Information that describes to voting equipment the content and appearance of the ballots to be used in an election ♦Vote Transmission to Central Site: For voting systems that transmit votes individually over a public network, the transmission of a single vote to the county (or contractor) for consolidation with other county vote data ♦Vote Count: Information representing the tabulation of votes at any one of several levels: polling place, precinct, or central count ♦List of Voters: A listing of the individual voters who have cast ballots in a specific election	N/A

Requirement	Requirement Text	Conform
2.1.10	Data Retention	
2.1.10	United States Code Title 42, Sections 1974 through 1974e state that election administrators shall preserve for 22 months "all records and paper that came into (their) possession relating to an application, registration, payment of poll tax, or other act requisite to voting." This retention requirement applies to systems that will be used at anytime for voting of candidates for federal offices (e.g., Member of Congress, United States Senator, and/or Presidential Elector). Therefore, all voting systems shall provide for maintaining the integrity of voting and audit data during an election and for a period of at least 22 months thereafter. Because the purpose of this law is to assist the federal government in discharging its law enforcement responsibilities in connection with civil rights and elections crimes, its scope must be interpreted in keeping with that objective. The appropriate state or local authority must preserve all records that may be relevant to the detection and prosecution of federal civil rights or election crimes for the 22-month federal retention period, if the records were generated in connection with an election that was held in whole or in part to select federal candidates. It is important to note that Section 1974 does not require that election officials generate any specific type or classification of election record. However, if a record is generated, Section 1974 comes into force and the appropriate authority must retain the records for 22 months. For 22-month document retention, the general rule is that all printed copy records produced by the election database and ballot processing systems shall be so labeled and archived. Regardless of system type, all audit trail information spelled out in Subsection 5.5 shall be retained in its original format, whether that be real-time logs generated by the system, or manual logs maintained by election personnel. The election audit trail includes not only in-process logs of election-night and subsequent processing of absentee or provisional ballots, but also time logs of baseline ballot definition formats, and system readiness and testing results. In many voting systems, the source of election-specific data (and ballot formats) is a database or file. In precinct count voting systems, this data is used to program each machine, establish ballot layout, and generate tallying files. It is not necessary to retain this information on electronic media if there is an official, authenticated printed copy of all final database information. However, it is recommended that the state or local jurisdiction also retain electronic records of the aggregate data for each voting machine so that reconstruction of an election is possible without data re-entry. The same requirement and recommendation applies to vote results generated by each precinct count voting machine.	***YES***
2.2	Pre-voting Capabilities This subsection defines capabilities required to support functions performed prior to the opening of polls. All voting systems shall provide capabilities to support: • Ballot preparation • Election programming • Ballot and program installation and control • Readiness testing • Verification at the polling place • Verification at the central counting place The standards also include requirements to ensure compatible interfaces with the ballot definition process and the reporting of election results.	
2.2.1	Ballot Preparation Ballot preparation is the process of using election databases to define the specific contests, questions, and related instructions to be contained in ballots and to produce all permissible ballot layouts. Ballot preparation requirements include: • General capabilities • Ballot formatting • Ballot production	
2.2.1.1	General Capabilities All systems shall provide the general capabilities for ballot preparation. All systems shall be capable of:	
2.2.1.1.a	Enabling the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed on the ballot for each political subdivision and election district	***YES***
2.2.1.1.b.i	Collecting and maintaining the following data i. Offices and their associated labels and instructions	***YES***
2.2.1.1.b.ii	Collecting and maintaining the following data ii. Candidate names and their associated labels	***YES***

Requirement	Requirement Text	Conform
2.2.1.1.b.iii.	Collecting and maintaining the following data iii. Issues or measures and their associated text	YES
2.2.1.1.c	Supporting the maximum number of potentially active voting positions as indicated in the system documentation	YES
2.2.1.1.d	For a primary election, generating ballots that segregate the choices in partisan contests by party affiliation	YES
2.2.1.1.e	Generating ballots that contain identifying codes or marks uniquely associated with each format	YES
2.2.1.1.f	Ensuring that vote response fields, selection buttons, or switches properly align with the specific candidate names and/or issues printed on the ballot display, ballot card or sheet, or separate ballot pages	YES
2.2.1.1.g	Paper-based voting systems shall also meet the following requirements applicable to the technology used: Enable voters to make selections by making a mark in areas designated for this purpose upon each ballot sheet	YES
2.2.1.1.h	Paper-based voting systems shall also meet the following requirements applicable to the technology used: For marksense systems, ensure that the timing marks align properly with the vote response fields	YES
2.2.1.2	Ballot Formatting Ballot formatting is the process by which election officials or their designees use election databases and voting system software to define the specific contests and related instructions contained on the ballot and present them in a layout permitted by state law. All voting systems shall provide a capability for:	
2.2.1.2.a	Creation of newly defined elections	YES
2.2.1.2.b	Rapid and error-free definition of elections and their associated ballot layouts	YES
2.2.1.2.c	Uniform allocation of space and fonts used for each office, candidate, and contest such that the voter perceives no active voting position to be preferred to any other	YES
2.2.1.2.d	Simultaneous display of the maximum number of choices for a single contest as indicated by the vendor in the system documentation	YES
2.2.1.2.e	Retention of previously defined formats for an election	YES
2.2.1.2.f	Prevention of unauthorized modification of any ballot formats	YES
2.2.1.2.g	Modification by authorized persons of a previously defined ballot format for use in a subsequent election	YES
2.2.1.3	Ballot Production Ballot production is the process of converting ballot formats to a media ready for use in the physical ballot production or electronic presentation. The voting system shall provide a means of printing or otherwise generating a ballot display that can be installed in all voting equipment for which it is intended. All voting systems shall provide the capabilities below.	
2.2.1.3.a	The electronic display or printed document on which the user views the ballot is capable of rendering an image of the ballot in any of the languages required by the Voting Rights Act of 1965, as amended.	YES
2.2.1.3.b	The electronic display or printed document on which the user views the ballot does not show any advertising or commercial logos of any kind, whether public service, commercial, or political, unless specifically provided for in state law. Electronic displays shall not provide connection to such material through hyperlink.	YES
2.2.1.3.c	The ballot conforms to vendor specifications for type of paper stock, weight, size, shape, size and location of mark field used to record votes, folding, bleed-through, and ink for printing if paper ballot documents or paper displays are part of the system.	YES
2.2.1.3 d	Vendor documentation for marksense systems shall include specifications for ballot materials to ensure that vote selections are read from only a single ballot at a time, without detection of marks from multiple ballots concurrently (e.g., reading of bleed-through from other ballots).	YES

Manufacturer: **Dominion Voting Systems**

Requirement	*Requirement Text*	*Conform*
2.2.2	Election Programming Election programming is the process by which election officials or their designees use election databases and vendor system software to logically define the voter choices associated with the contents of the ballots. All systems shall provide for the:	
2.2.2.a	Logical definition of the ballot, including the definition of the number of allowable choices for each office and contest	***YES***
2.2.2.b	Logical definition of political and administrative subdivisions, where the list of candidates or contests varies between polling places	***YES***
2.2.2.c	Exclusion of any contest on the ballot in which the voter is prohibited from casting a ballot because of place of residence, or other such administrative or geographical criteria	***YES***
2.2.2.d	Ability to select from a range of voting options to conform to the laws of the jurisdiction in which the system will be used	***YES***
2.2.2.e	Generation of all required master and distributed copies of the voting program, in conformance with the definition of the ballots for each voting device and polling place, and for each tabulating device	***YES***
2.2.3	Ballot and Program Installation and Control All systems shall provide a means of installing ballots and programs on each piece of polling place or central count equipment in accordance with the ballot requirements of the election and the requirements of the jurisdiction in which the equipment will be used. All systems shall include the following at the time of ballot and program installation:	
2.2.3.a	A detailed work plan or other documentation providing a schedule and steps for the software and ballot installation, which includes a table outlining the key dates, events and deliverables	***YES***
2.2.3.b	A capability for automatically verifying that the software has been properly selected and installed in the equipment or in programmable memory devices, and for indicating errors	***YES***
2.2.3.c	A capability for automatically validating that software correctly matches the ballot formats that it is intended to process, for detecting errors, and for immediately notifying an election official of detected errors	***YES***
2.2.4	Readiness Testing Election personnel conduct voting equipment and voting system readiness tests prior to the start of an election to ensure that the voting system functions properly, to confirm that voting equipment has been properly integrated, and to obtain equipment status reports. All voting systems shall provide the capabilities to:	
2.2.4.a.	Verify that voting equipment and precinct count equipment is properly prepared for an election, and collect data that verifies equipment readiness	***YES***
2.2.4.b.	Obtain status and data reports from each set of equipment	***YES***
2.2.4.c.	Verify the correct installation and interface of all voting equipment	***YES***
2.2.4.d.	Verify that hardware and software function correctly	***YES***
2.2.4.e.	Generate consolidated data reports at the polling place and higher jurisdictional levels	***YES***
2.2.4.f.	Segregate test data from actual voting data, either procedurally or by hardware/software features	***YES***
	Readiness Testing (cont'd) Resident test software, external devices, and special purpose test software connected to or installed in voting equipment to simulate operator and voter functions may be used for these tests provided that the following standards are met:	
2.2.4.g.	These elements shall be capable of being tested separately, and shall be proven to be reliable verification tools prior to their use	***YES***
2.2.4.h.	These elements shall be incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase	***YES***
2.2.4.i.	Paper-based systems shall: Support conversion testing that uses all potential ballot positions as active positions	***YES***
2.2.4.j.	Paper-based systems shall: Support conversion testing of ballots with active position density for systems without pre-designated ballot positions	***YES***

Requirement	Requirement Text	Conform
2.2.5	Verification at Polling Place Election officials perform verification at the polling place to ensure that all voting systems and voting equipment function properly before and during an election. All voting systems shall provide a formal record of the following, in any media, upon verification of the authenticity of the command source:	
2.2.5.a.	The election's identification data	***YES***
2.2.5.b.	The identification of all equipment units	***YES***
2.2.5.c.	The identification of the polling place	***YES***
2.2.5.d.	The identification of all ballot formats	***YES***
2.2.5.e.	The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros)	***YES***
2.2.5.f.	A list of all ballot fields that can be used to invoke special voting options	***YES***
2.2.5.g.	Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements.	***YES***
	Verification at Polling Place (cont'd) To prepare voting devices to accept voted ballots, all voting systems shall provide the capability to test each device prior to opening to verify that each is operating correctly. At a minimum, the tests shall include:	
2.2.5.h.	Confirmation that there are no hardware or software failures	***YES***
2.2.5.i.	Confirmation that the device is ready to be activated for accepting votes	***YES***
2.2.5.end	If a precinct count system includes equipment for the consolidation of polling place data at one or more central counting locations, it shall have means to verify the correct extraction of voting data from transportable memory devices, or to verify the transmission of secure data over secure communication links.	***YES***
2.2.6	Verification at the Central Location Election officials perform verification at the central location to ensure that vote counting and vote consolidation equipment and software function properly before and after an election. Upon verification of the authenticity of the command source, any system used in a central count environment shall provide a printed record of the following:	
2.2.6.a	The election's identification data	***YES***
2.2.6.b	The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros)	***YES***
2.2.6.c	Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements	***YES***
2.3	Voting Capabilities	
2.3	All voting systems shall support: ♦Opening the polls ♦Casting a ballot. Additionally, all DRE systems shall support: ♦Activating the ballot. ♦Augmenting the election counter ♦Augmenting the life-cycle counter.	
2.3.1	Opening the Polls The capabilities required for opening the polls are specific to individual voting system technologies. At a minimum, the systems shall provide the functional capabilities indicated below.	
2.3.1.1	Precinct Count Systems To allow voting devices to be activated for voting, all precinct count systems shall provide:	
2.3.1.1.a	An internal test or diagnostic capability to verify that all of the polling place tests specified in Subsection 2.2.5 have been successfully completed	***YES***
2.3.1.1.b	Automatic disabling of any device that has not been tested until it has been tested	***YES***
2.3.1.2	Paper-Based System Requirements To facilitate opening the polls, all paper-based systems shall include:	
2.3.1.2.a	A means of verifying that ballot marking devices are properly prepared and ready to use	***YES***
2.3.1.2.b	A voting booth or similar facility, in which the voter may mark the ballot in privacy;	***YES***
2.3.1.2.c	Secure receptacles for holding voted ballots	***YES***

Requirement	*Requirement Text*	*Conform*
	Paper-Based System Requirements (cont'd) In addition to the above requirements, all paper-based precinct count equipment shall include a means of:	
2.3.1.2.d.	Activating the ballot counting device	***YES***
2.3.1.2.e.	Verifying that the device has been correctly activated and is functioning properly	***YES***
2.3.1.2.f.	Identifying device failure and corrective action needed	***YES***
2.3.1.3	DRE System Requirements To facilitate opening the polls, all DRE systems shall include:	
2.3.1.3.a	A security seal, a password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the poll-opening function	***YES***
2.3.1.3.b	A means of enforcing the execution of steps in the proper sequence if more than one step is required	***YES***
2.3.1.3.c	A means of verifying the system has been activated correctly	***YES***
2.3.1.3.d	A means of identifying system failure and any corrective action needed	***YES***
2.3.2	Activating the Ballot (DRE Systems) To activate the ballot, all DRE systems shall:	
2.3.2.a	Enable election officials to control the content of the ballot presented to the voter, whether presented in printed form or electronic display, such that each voter is permitted to record votes only in contests in which that voter is authorized to vote	***YES***
2.3.2.b	Allow each eligible voter to cast a ballot	***YES***
2.3.2.c	Prevent a voter from voting on a ballot to which he or she is not entitled	***YES***
2.3.2.d	Prevent a voter from casting more than one ballot in the same election	***YES***
2.3.2.e	Activate the casting of a ballot in a general election	***YES***
2.3.2.f	Enable the selection of the ballot that is appropriate to the party affiliation declared by the voter in a primary election	***YES***
2.3.2.g	Activate all portions of the ballot upon which the voter is entitled to vote	***YES***
2.3.2.h	Disable all portions of the ballot upon which the voter is not entitled to vote	***YES***
2.3.3	Casting a Ballot Some required capabilities for casting a ballot are common to all systems. Others are specific to individual voting technologies or intended use. Systems must provide additional functional capabilities that enable accessibility to disabled voters as defined in Subsection 3.2.	
2.3.3.1	Common Requirements To facilitate casting a ballot, all systems shall:	
2.3.3.1.a	Provide text that is at least 3 millimeters high and provide the capability to adjust or magnify the text to an apparent size of 6.3 millimeters	***YES***
2.3.3.1.b	Protect the secrecy of the vote such that the system cannot reveal any information about how a particular voter voted, except as otherwise required by individual state law	***YES***
2.3.3.1.c	Record the selection and non-selection of individual vote choices for each contest and ballot measure	***YES***
2.3.3.1.d	Record the voter's selection of candidates whose names do not appear on the ballot, if permitted under state law, and record as many write-in votes as the number of candidates the voter is allowed to select	***YES***
2.3.3.1.e	In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power	***YES***
2.3.3.1.f	Provide the capability for voters to continue casting ballots in the event of a failure of a telecommunications connection within the polling place or between the polling place and any other location	***N/A***
2.3.3.2	Paper-Based System Requirements All paper-based systems shall:	
2.3.3.2.a	Allow the voter to easily identify the voting field that is associated with each candidate or ballot measure response	***YES***
2.3.3.2.b	Allow the voter to mark the ballot to register a vote	***YES***

Requirement	*Requirement Text*	*Conform*
2.3.3.2.c	Allow either the voter or the appropriate election official to place the voted ballot into the ballot counting device (for precinct count systems) or into a secure receptacle (for central count systems)	***YES***
2.3.3.2.d	Protect the secrecy of the vote throughout the process	***YES***
	Paper-Based System Requirements (cont'd) In addition to the above requirements, all paper-based precinct count systems shall:	
2.3.3.2.e.	Provide feedback to the voter that identifies specific contests for which he or she has made no selection or fewer than the allowable number of selections (e.g., undervotes)	***YES***
2.3.3.2.f.	Notify the voter if he or she has made more than the allowable number of selections for any contest (e.g., overvotes)	***YES***
2.3.3.2.g.	Notify the voter before the ballot is cast and counted of the effect of making more than the allowable number of selections for a contest	***YES***
2.3.3.2.h.	Provide the voter opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted	***YES***
2.3.3.3	DRE System Requirements In addition to the above common requirements, DRE systems shall:	
2.3.3.3.a.	Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources)	***YES***
2.3.3.3.b.	Enable the voter to easily identify the selection button or switch, or the active area of the ballot display, that is associated with each candidate or ballot measure response	***YES***
2.3.3.3.c.	Allow the voter to select his or her preferences on the ballot in any legal number and combination	***YES***
2.3.3.3.d.	Indicate that a selection has been made or canceled	***YES***
2.3.3.3.e.	Indicate to the voter when no selection, or an insufficient number of selections, has been made for a contest (e.g., undervotes)	***YES***
2.3.3.3.f.	Notify the voter if he or she has made more than the allowable number of selections for any contest (e.g., overvotes)	***YES***
2.3.3.3.g.	Notify the voter before the ballot is cast and counted of the effect of making more than the allowable number of selections for a contest	***YES***
2.3.3.3.h	Provide the voter opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted	***YES***
2.3.3.3.i.	Notify the voter when the selection of candidates and measures is completed	***YES***
2.3.3.3.j.	Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast	***YES***
2.3.3.3.k.	For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot	***YES***
2.3.3.3.l.	Notify the voter after the vote has been stored successfully that the ballot has been cast	***N/A***
2.3.3.3.m.	Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur	***N/A***
2.3.3.3.n.	Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds	***YES***
2.3.3.3.o.	Ensure that the votes stored accurately represent the actual votes cast	***YES***
2.3.3.3.p.	Prevent modification of the voter's vote after the ballot is cast	***YES***
2.3.3.3.q.	Provide a capability to retrieve ballot images in a form readable by humans [in accordance with the requirements of Subsections 2.1.2 (f) and 2.1.4 (k) and (l)]	***YES***
2.3.3.3.r.	Increment the proper ballot position registers or counters	***YES***
2.3.3.3.s.	Protect the secrecy of the vote throughout the voting process	***YES***
2.3.3.3.t.	Prohibit access to voted ballots until after the close of polls	***YES***

Requirement	Requirement Text	Conform
2.3.3.3.u.	Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the voting system	YES
2.3.3.3.v.	Isolate test ballots such that they are accounted for accurately in vote counts and are not reflected in official vote counts for specific candidates or measures	YES
2.4	Post-Voting Capabilities All voting systems shall provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails. In addition, precinct count voting systems must provide a means to close the polls including generating appropriate reports. If the system provides the capability to broadcast results, additional standards apply.	
2.4.1	Closing the Polls These requirements for closing the polls and locking voting systems against future voting are specific to precinct count systems. The voting system shall provide the means for:	
2.4.1.a	Preventing the further casting of ballots once the polls has closed	YES
2.4.1.b	Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal	YES
2.4.1.c	Incorporating a visible indication of system status	YES
2.4.1.d	Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated	YES
2.4.1.e	Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election	YES
2.4.2	Consolidating Vote Data	
2.4.2	All systems shall provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes).	YES
2.4.3	Producing Reports All systems shall be able to create reports summarizing the vote data on multiple levels. All systems shall provide capabilities to:	
2.4.3.a	Support geographic reporting, which requires the reporting of all results for each contest at the precinct level and additional jurisdictional levels	YES
2.4.3.b	Produce a printed report of the number of ballots counted by each tabulator	YES
2.4.3.c	Produce a printed report for each tabulator of the results of each contest that includes the votes cast for each selection, the count of undervotes, and the count of overvotes	YES
2.4.3.d	Produce a consolidated printed report of the results for each contest of all votes cast (including the count of ballots from other sources supported by the system as specified by the vendor) that includes the votes cast for each selection, the count of undervotes, and the count of overvotes	YES
2.4.3.e	Be capable of producing a consolidated printed report of the combination of overvotes for any contest that is selected by an authorized official (e.g., the number of overvotes in a given contest combining candidate A and candidate B, combining candidate A and candidate C, etc.)	YES
2.4.3.f	Produce all system audit information required in Subsection 5.4 in the form of printed reports, or in electronic memory for printing centrally	YES
2.4.3.g	Prevent data from being altered or destroyed by report generation, or by the transmission of results over telecommunications lines	YES
2.4.3	Producing Reports (cont'd) All systems shall be able to create reports summarizing the vote data on multiple levels. In addition, all precinct count voting systems shall:	
2.4.3.h.	Prevent the printing of reports and the unauthorized extraction of data prior to the official close of the polls	YES
2.4.3.i.	Provide a means to extract information from a transportable programmable memory device or data storage medium for vote consolidation	YES
2.4.3.j.	Consolidate the data contained in each unit into a single report for the polling place when more than one voting machine or precinct tabulator is used	YES

Requirement	Requirement Text	Conform
2.4.3.k.	Prevent data in transportable memory from being altered or destroyed by report generation, or by the transmission of official results over telecommunications lines	YES
2.4.4	Broadcasting Results (Optional capability; if supported by the vendor) Some voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available shall	
2.4.4.a	Provide only aggregated results, and not data from individual ballots	N/A
2.4.4.b	Provide no access path from unofficial electronic reports or files to the storage devices for official data	N/A
2.4.4.c	Clearly indicate on each report or file that the results it contains are unofficial	N/A
2.5	Maintenance, Transportation, and Storage All systems shall be designed and manufactured to facilitate preventive and corrective maintenance, conforming to the hardware standards described in Subsection 4.1. All vote casting and tally equipment designated for storage between elections shall:	
2.5.a	Function without degradation in capabilities after transit to and from the place of use, as demonstrated by meeting the performance standards described in Subsection 4.1	YES
2.5.b	Function without degradation in capabilities after storage between elections, as demonstrated by meeting the performance standards described in Subsection 4.1	YES
3.1	Usability and Accessibility Requirements	
3.1.1	Usability Testing	
	The vendor shall conduct summative usability tests on the voting system using individuals representative of the general population. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification. Discussion: Voting system developers are required to conduct realistic usability tests on the final product. For the present, vendors can define their own testing protocols. Future revisions to the Guidelines will include requirements for usability testing that will provide specific performance benchmarks.	YES
3.1.2	Functional Capabilities The voting process shall provide certain functional capabilities to support voter usability.	
3.1.2.a	The voting system shall provide feedback to the voter that identifies specific contests or ballot issues for which he or she has made no selection or fewer than the allowable number of selections (e.g., undervotes)	YES
3.1.2.b	The voting system shall notify the voter if he or she has made more than the allowable number of selections for any contest (e.g., overvotes)	YES
3.1.2.c	The voting system shall notify the voter before the ballot is cast and counted of the effect of making more than the allowable number of selections for a contest	YES
3.1.2.d	The voting system shall provide the voter the opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted	YES
3.1.2.e	The voting system shall allow the voter, at his or her choice, to submit an undervoted or overvoted ballot without correction	YES
3.1.2.f	DRE voting machines shall allow the voter to change a vote within a contest before advancing to the next contest. Discussion: The point here is that voters using a DRE should not have to wait for the final ballot review screen in order to change a vote.	YES
3.1.2.g	DRE voting machines should provide navigation controls that allow the voter to advance to the next contest or go back to the previous contest before completing a vote on the contest currently being presented (whether visually or aurally). Discussion: For example, the voter should not be forced to proceed sequentially through all the contests before going back to check his or her selection for a previous contest.	YES

Requirement	Requirement Text	Conform
3.1.3	The voting equipment shall be capable of presenting the ballot, ballot selections, review screens and instructions in any language required by state or federal law.	YES
3.1.4	Cognitive Issues The voting process shall be designed to minimize cognitive difficulties for the voter.	
3.1.4.a	Consistent with election law, the voting system should support a process that does not introduce any bias for or against any of the selections to be made by the voter. In both visual and aural formats, contest choices shall be presented in an equivalent manner. Discussion: Certain differences in presentation are mandated by state law, such as the order in which candidates are listed and provisions for voting for write-in candidates. But comparable characteristics such as font size or voice volume and speed must be the same for all choices.	YES
3.1.4.b	The voting machine or related materials shall provide clear instructions and assistance to allow voters to successfully execute and cast their ballots independently. Discussion: Voters should not routinely need to ask for human assistance.	YES
3.1.4.b.i	Voting machines or related materials shall provide a means for the voter to get help at any time during the voting session. Discussion: The voter should always be able to get help if needed. DRE voting machines may provide this with a distinctive “help” button. Any type of voting equipment may provide written instructions that are separate from the ballot.	YES
3.1.4.b.ii	The voting machine shall provide instructions for all its valid operations. Discussion: If an operation is available to the voter, it must be documented. Examples include how to change a vote, how to navigate among contests, how to cast a straight party vote, and how to cast a write-in vote.	YES
3.1.4.c	The voting system shall provide the capability to design a ballot for maximum clarity and comprehension.	YES
3.1.4.c.i	The voting equipment should not visually present a single contest spread over two pages or two columns. Discussion: Such a visual separation poses the risk that the voter may perceive one contest as two. If a contest has a large number of candidates, it may be infeasible to observe this guideline.	YES
3.1.4.c.ii	The ballot shall clearly indicate the maximum number of candidates for which one can vote within a single contest.	YES
3.1.4.c.iii	There shall be a consistent relationship between the name of a candidate and the mechanism used to vote for that candidate. Discussion: For example, if the response field where voters indicate their selections is located to the left of a candidate’s name, then each response field shall be located to the left of the associated candidates’ names.	YES
3.1.4.d	Warnings and alerts issued by the voting system should clearly state the nature of the problem and the set of responses available to the voter. The warning should clearly state whether the voter has performed or attempted an invalid operation or whether the voting equipment itself has malfunctioned in some way. Discussion: In case of an equipment failure, the only action available to the voter might be to get assistance from a poll worker.	YES
3.1.4.e	The use of color by the voting system should agree with common conventions: (a) green, blue or white is used for general information or as a normal status indicator; (b) amber or yellow is used to indicate warnings or a marginal status; (c) red is used to indicate error conditions or a problem requiring immediate attention.	YES
3.1.5	Perceptual Issues The voting process shall be designed to minimize perceptual difficulties for the voter.	YES
3.1.5.a	No voting machine display screen shall flicker with a frequency between 2 Hz and 55 Hz. Discussion: Aside from usability concerns, this requirement protects voters with epilepsy.	YES
3.1.5.b	Any aspect of the voting machine that is adjustable by the voter or poll worker, including font size, color, contrast, and audio volume, shall automatically reset to a standard default value upon completion of that voter's session. Discussion: The voting machine must present the same initial appearance to every voter.	YES

Requirement	Requirement Text	Conform
3.1.5.c	If any aspect of a voting machine is adjustable by the voter or poll worker, there shall be a mechanism to reset all such aspects to their default values. Discussion: The purpose is to allow a voter who has adjusted the machine into an undesirable state to reset all the aspects to begin again.	***YES***
3.1.5.d	All electronic voting machines shall provide a minimum font size of 3.0 mm (measured as the height of a capital letter) for all text.	***YES***
3.1.5.e	All voting machines using paper ballots should make provisions for voters with poor reading vision. Discussion: Possible solutions include: (a) providing paper ballots in at least two font sizes, 3.0-4.0mm and 6.3-9.0mm and (b) providing a magnifying device.	***YES***
3.1.5.f	The default color coding shall maximize correct perception by voters with color blindness. Discussion: There are many types of color blindness and no color coding can, by itself, guarantee correct perception for everyone. However, designers should take into account such factors as: red-green color blindness is the most common form; high luminosity contrast will help colorblind voters to recognize visual features; and color-coded graphics can also use shape to improve the ability to distinguish certain features.	***YES***
3.1.5.g	Color coding shall not be used as the sole means of conveying information, indicating an action, prompting a response, or distinguishing a visual element. Discussion: While color can be used for emphasis, some other non-color mode must also be used to convey the information, such as a shape or text style. For example, red can be enclosed in an octagon shape.	***YES***
3.1.5.h	All text intended for the voter should be presented in a sans serif font. Discussion: Experimentation has shown that users prefer such a font and the legibility of serif and sans serif fonts is equivalent.	***YES***
3.1.5.i	The minimum figure-to-ground ambient contrast ratio for all text and informational graphics (including icons) intended for the voter shall be 3:1.	***YES***
3.1.6	Interaction Issues The voting process shall be designed to minimize interaction difficulties for the voter.	***YES***
3.1.6.a	Voting machines with electronic image displays shall not require page scrolling by the voter. Discussion: This is not an intuitive operation for those unfamiliar with the use of computers. Even those experienced with computers often do not notice a scroll bar and miss information at the bottom of the “page.” Voting systems may require voters to move to the next or previous page." "	***YES***
3.1.6.b	The voting machine shall provide unambiguous feedback regarding the voter’s selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance.	***YES***
3.1.6.c	If the voting machine requires a response by a voter within a specific period of time, it shall issue an alert at least 20 seconds before this time period has expired and provide a means by which the voter may receive additional time.	***YES***
3.1.6.d	Input mechanisms shall be designed to minimize accidental activation.	***YES***
3.1.6.d.i	On touch screens, the sensitive touch areas shall have a minimum height of 0.5 inches and minimum width of 0.7 inches. The vertical distance between the centers of adjacent areas shall be at least 0.6 inches, and the horizontal distance at least 0.8 inches.	***YES***
3.1.6.d.ii	No key or control on a voting machine shall have a repetitive effect as a result of being held in its active position. Discussion: This is to preclude accidental activation. For instance, if a voter is typing in the name of a write-in candidate, depressing and holding the “e” key results in only a single “e” added to the name.	***YES***
3.1.7	Privacy	

Requirement	Requirement Text	Conform
3.1.7	The voting process shall preclude anyone else from determining the content of a voter's ballot, without the voter's cooperation. Discussion: Privacy ensures that the voter can make selections based solely on his or her own preferences without intimidation or inhibition. Among other practices, this forbids the issuance of a receipt to the voter that would provide proof of how he or she voted.	***YES***
3.1.7.1	Privacy at the Polls When deployed according to the installation instructions provided by the vendor, the voting station shall prevent others from observing the contents of a voter's ballot.	***YES***
3.1.7.1.a	The ballot and any input controls shall be visible only to the voter during the voting session and ballot submission.	***YES***
3.1.7.1.b	The audio interface shall be audible only to the voter. Discussion: Voters who are hard of hearing but need to use an audio interface may also need to increase the volume of the audio. Such situations require headphones with low sound leakage.	***YES***
3.1.7.1.c	As mandated by HAVA 301 (a)(1)(C), the voting system shall notify the voter of an attempted overvote in a way that preserves the privacy of the voter and the confidentiality of the ballot.	***YES***
3.1.7.2	No Recording of Alternate Format Usage Voter anonymity shall be maintained for alternative format ballot presentation.	***YES***
3.1.7.2.a	No information shall be kept within an electronic cast vote record that identifies any alternative language feature(s) used by a voter.	***YES***
3.1.7.2.b	No information shall be kept within an electronic cast vote record that identifies any accessibility feature(s) used by a voter.	***YES***
3.2	Accessibility Requirements	
3.2.1	General The voting process shall incorporate the following features that are applicable to all types of disabilities:	
3.2.1.a	When the provision of accessibility involves an alternative format for ballot presentation, then all information presented to voters including instructions, warnings, error and other messages, and ballot choices shall be presented in that alternative format.	***YES***
3.2.1.b	The support provided to voters with disabilities shall be intrinsic to the accessible voting station. It shall not be necessary for the accessible voting station to be connected to any personal assistive device of the voter in order for the voter to operate it correctly.	***YES***
	Discussion: This requirement does not preclude the accessible voting station from providing interfaces to assistive technology. [See definition of "personal assistive devices" in the Glossary.] Its purpose is to assure that disabled voters are not required to bring special devices with them in order to vote successfully. The requirement does not assert that the accessible voting station will obviate the need for a voter's ordinary non-interfacing devices, such as eyeglasses or canes. Jurisdictions should ensure that an accessible voting station provides clean and sanitary devices for voters with dexterity disabilities.	
3.2.1.c	When the primary means of voter identification or authentication uses biometric measures that require a voter to possess particular biological characteristics, the voting process shall provide a secondary means that does not depend on those characteristics. Discussion: For example, if fingerprints are used for voter identification, another mechanism shall be provided for voters without usable fingerprints.	***YES***
3.2.2	Vision	
3.2.2	The voting process shall be accessible to voters with visual disabilities. Discussion: Note that all aspects of the voting process are to be accessible, not just the voting machine.	***YES***
3.2.2.1	Partial Vision	

Requirement	Requirement Text	Conform
3.2.2.1.a	The vendor shall conduct summative usability tests on the voting system using partially sighted individuals. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification. Discussion: Voting system developers are required to conduct realistic usability tests on the final product. For the present, vendors can define their own testing protocols. Future revisions to the Guidelines will include requirements for usability testing that will provide specific performance benchmarks.	***YES***
3.2.2.1.b	The accessible voting station with an electronic image display shall be capable of showing all information in at least two font sizes, (a) 3.0-4.0 mm and (b) 6.3-9.0 mm, under control of the voter. Discussion: All millimeters will be calculated using Hard Metric Conversion. [See Glossary for definition.] While larger font sizes may assist most voters with poor vision, certain disabilities such as tunnel vision are best addressed by smaller font sizes.	***YES***
3.2.2.1.c	An accessible voting station with a monochrome-only electronic image display shall be capable of showing all information in high contrast either by default or under the control of the voter or poll worker. High contrast is a figure-to-ground ambient contrast ratio for text and informational graphics of at least 6:1.	***YES***
3.2.2.1.d	An accessible voting station with a color electronic image display shall allow the voter to adjust the color or the figure-to-ground ambient contrast ratio. Discussion: See Technical Guide for Color, Contrast and Text Size in Appendix D for examples of how a voting station may meet this requirement by offering a limited number of discrete choices. In particular, it is not required that the station offer a continuous range of color or contrast values.	***YES***
3.2.2.1.e	Buttons and controls on accessible voting stations shall be distinguishable by both shape and color. Discussion: The redundant cues have been found to be helpful to those with partial vision.	***YES***
3.2.2.1.f	An accessible voting station using an electronic image display shall provide synchronized audio output to convey the same information as that which is displayed on the screen. Discussion: The redundant cues are helpful to those with low vision. They are also helpful to individuals who may have difficulty reading the text on the screen.	***YES***
3.2.2.2	Blindness	
3.2.2.2.a	The vendor shall conduct summative usability tests on the voting system using individuals who are blind. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification. Discussion: Voting system developers are required to conduct realistic usability tests on the final product. For the present, vendors can define their own testing protocols. Future revisions to the Guidelines will include requirements for usability testing that will provide specific performance benchmarks.	***YES***
3.2.2.2.b	The accessible voting station shall provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface, as specified in Subsection 2.3.3. Discussion: Note the necessity of both audio output and tactilely discernible controls for voter input. Full functionality includes at least:	***YES***

Requirement	Requirement Text	Conform
	• Instructions and feedback on initial activation of the ballot (such as insertion of a smart card) • Instructions and feedback to the voter on how to operate the accessible • voting station, including settings and options (e.g., volume control, • repetition) • Instructions and feedback for navigation of the ballot • Instructions and feedback for contest choices, including write-in • candidates • Instructions and feedback on confirming and changing selections • Instructions and feedback on final submission of ballot	***YES***
3.2.2.2.b.i	The ATI of the accessible voting station shall provide the same capabilities to vote and cast a ballot as are provided by other voting machines or by the visual interface of the standard voting machine. Discussion: For example, if a visual ballot supports voting a straight party ticket and then changing the choice in a single contest, so must the ATI.	***YES***
3.2.2.2.b.ii	The ATI shall allow the voter to have any information provided by the voting system repeated.	***YES***
3.2.2.2.b.iii	The ATI shall allow the voter to pause and resume the audio presentation.	***YES***
3.2.2.2.iv	The ATI shall allow the voter to skip to the next contest or return to previous contests. Discussion: This is analogous to the ability of sighted voters to move on to the next contest once they have made a selection or to abstain from voting on a contest altogether.	***YES***
3.2.2.2.v	The ATI shall allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately. Discussion: This is analogous to the ability of sighted voters to skip over the wording of a referendum on which they have already made a decision prior to the voting session (e.g., “Vote yes on proposition #123”).	***YES***
3.2.2.2.c	All voting stations that provide audio presentation of the ballot shall conform to the following requirements: Discussion: These requirements apply to all voting machine audio output, not just to the ATI of an accessible voting station.	***YES***
3.2.2.2.c.i	The ATI shall provide its audio signal through an industry standard connector for private listening using a 3.5mm stereo headphone jack to allow voters to use their own audio assistive devices.	***YES***
3.2.2.2.c.ii	When a voting machine utilizes a telephone style handset or headphone to provide audio information, it shall provide a wireless T-Coil coupling for assistive hearing devices so as to provide access to that information for voters with partial hearing. That coupling shall achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.	***YES***
3.2.2.2.c.iii	No voting equipment shall cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices. The voting equipment, considered as a wireless device, shall achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19. Discussion: Hearing devices" include hearing aids and cochlear implants. "	***YES***
3.2.2.2.c.iv	A sanitized headphone or handset shall be made available to each voter. Discussion: This requirement can be achieved in various ways, including the use of throwaway" headphones	***YES***
3.2.2.2.c.v	The voting machine shall set the initial volume for each voter between 40 and 50 dB SPL. Discussion: A voter does not "inherit" the volume as set by the previous user of the voting station.	***YES***
3.2.2.2.c.vi	The voting machine shall provide a volume control with an adjustable volume from a minimum of 20dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.	***YES***
3.2.2.2.c.vii	The audio system shall be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.	***YES***

Requirement	Requirement Text	Conform
3.2.2.2.c.viii	The audio presentation of verbal information should be readily comprehensible by voters who have normal hearing and are proficient in the language. This includes such characteristics as proper enunciation, normal intonation, appropriate rate of speech, and low background noise. Candidate names should be pronounced as the candidate intends.	***YES***
3.2.2.2.c.ix	The audio system shall allow voters to control the rate of speech. The range of speeds supported should be at least 75% to 200% of the nominal rate. Discussion: Many blind voters are accustomed to interacting with accelerated speech.	***YES***
3.2.2.2.d	If the normal procedure is to have voters initialize the activation of the ballot, the accessible voting station shall provide features that enable voters who are blind to perform this activation. Discussion: For example, smart cards might provide tactile cues so as to allow correct insertion.	***YES***
3.2.2.2.e	If the normal procedure is for voters to submit their own ballots, then the accessible voting station shall provide features that enable voters who are blind to perform this submission. Discussion: For example, if voters normally feed their own optical scan ballots into a reader, blind voters should also be able to do so.	***YES***
3.2.2.2.f	All mechanically operated controls or keys on an accessible voting station shall be tactilely discernible without activating those controls or keys.	***YES***
3.2.2.2.g	On an accessible voting station, the status of all locking or toggle controls or keys (such as the shift" key) shall be visually discernible	***YES***
3.2.3	Dexterity	
3.2.3.a	The vendor shall conduct summative usability tests on the voting system using individuals lacking fine motor control. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification. Discussion: Voting system developers are required to conduct realistic usability tests on the final product. For the present, vendors can define their own testing protocols. Future revisions to the Guidelines will include requirements for usability testing that will provide specific performance benchmarks.	***YES***
3.2.3.b	All keys and controls on the accessible voting station shall be operable with one hand and shall not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys shall be no greater 5 lbs. (22.2 N). Discussion: Controls are to be operable without excessive force.	***YES***
3.2.3.c	The accessible voting station controls shall not require direct bodily contact or for the body to be part of any electrical circuit. Discussion: This requirement ensures that controls are operable by individuals using prosthetic devices.	***YES***
3.2.3.d	The accessible voting station shall provide a mechanism to enable non-manual input that is functionally equivalent to tactile input. Discussion: This requirement ensures that the accessible voting station is operable by individuals who do not have the use of their hands. All the functionality of the accessible voting station (e.g., straight party voting, write-in candidates) that is available through the other forms of input, such as tactile, must also be available through a non-manual input mechanism if it is provided by the accessible voting station.	***YES***
3.2.3.e	If the normal procedure is for voters to submit their own ballots, then the accessible voting station shall provide features that enable voters who lack fine motor control or the use of their hands to perform this submission.	***YES***
3.2.4	Mobility The voting process shall be accessible to voters who use mobility aids, including wheelchairs.	***YES***
3.2.4.a	The accessible voting station shall provide a clear floor space of 30 inches (760 mm) minimum by 48 inches (1220 mm) minimum for a stationary mobility aid. The clear floor space shall be level with no slope exceeding 1:48 and positioned for a forward approach or a parallel approach.	***YES***

Requirement	*Requirement Text*	*Conform*
3.2.4.b	All controls, keys, audio jacks and any other part of the accessible voting station necessary for the voter to operate the voting machine shall be within reach as specified under the following sub-requirements: Discussion: Note that these requirements have meaningful application mainly to controls in a fixed location. A hand-held tethered control panel is another acceptable way of providing reachable controls.	***YES***
3.2.4.b.i	If the accessible voting station has a forward approach with no forward reach obstruction then the high reach shall be 48 inches maximum and the low reach shall be 15 inches minimum. See Figure 1.	***YES***
3.2.4.b.ii	If the accessible voting station has a forward approach with a forward reach obstruction, the following requirements apply: See Figure 2.	***YES***
3.2.4.b.ii.a	The forward obstruction shall be no greater than 25 inches in depth, its top no higher than 34 inches and its bottom surface no lower than 27 inches.	***YES***
3.2.4.b.ii.b	If the obstruction is no more than 20 inches in depth, then the maximum high reach shall be 48 inches, otherwise it shall be 44 inches.	***YES***
3.2.4.b.iii.	Space under the obstruction between the finish floor or ground and 9 inches (230 mm) above the finish floor or ground shall be considered toe clearance and shall comply with the following provisions: Toe clearance shall extend 25 inches (635 mm) maximum under the obstruction " The minimum toe clearance under the obstruction shall be either 17 inches (430 mm) or the depth required to reach over the obstruction to operate the accessible voting station	***YES***
3.2.4.b.iv.	Space under the obstruction between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground shall be considered knee clearance and shall comply with the following provisions: Knee clearance shall extend 25 inches (635 mm) maximum under the obstruction at 9 inches (230 mm) above the finish floor or ground. " • The minimum knee clearance at 9 inches (230 mm) above the finish floor or ground shall be either 11 inches (280 mm) or 6 inches less than the toe clearance, whichever is greater. • Between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground, the knee clearance shall be permitted to reduce at a rate of 1 inch (25 mm) in depth for each 6 inches (150 mm) in height. Discussion: It follows that the minimum knee clearance at 27 inches above the finish floor or ground shall be 3 inches less than the minimum knee clearance at 9 inches above the floor. • Knee clearance shall be 30 inches (760 mm) wide minimum.	***YES***
3.2.4.b.v	If the accessible voting station has a parallel approach with no side reach obstruction then the maximum high reach shall be 48 inches and the minimum low reach shall be 15 inches. See Figure 3.	***YES***
3.2.4.b.vi	If the accessible voting station has a parallel approach with a side reach obstruction, the following sub-requirements apply. See Figure 4.	***YES***
3.2.4.b.vi.a	The side obstruction shall be no greater than 24 inches in depth and its top no higher than 34 inches.	***YES***
3.2.4.b.vi.b	If the obstruction is no more than 10 inches in depth, then the maximum high reach shall be 48 inches, otherwise it shall be 46 inches. Discussion: Since this is a parallel approach, no clearance under the obstruction is required.	***YES***
3.2.4.c	All labels, displays, controls, keys, audio jacks, and any other part of the accessible voting station necessary for the voter to operate the voting machine shall be easily legible and visible to a voter in a wheelchair with normal eyesight (no worse than 20/40, corrected) who is in an appropriate position and orientation with respect to the accessible voting station Discussion: There are a number of factors that could make relevant parts of the accessible voting station difficult to see such as; small lettering, controls and labels tilted at an awkward angle from the voter's viewpoint, and glare from overhead lighting.	***YES***
3.2.5	Hearing The voting process shall be accessible to voters with hearing disabilities.	***YES***

Requirement	Requirement Text	Conform
3.2.5.a	The accessible voting station shall incorporate the features listed under requirement 3.2.2.2 (c) for voting equipment that provides audio presentation of the ballot to provide accessibility to voters with hearing disabilities. Discussion: Note especially the requirements for volume initialization and control.	***YES***
3.2.5.b	If voting equipment provides sound cues as a method to alert the voter, the tone shall be accompanied by a visual cue, unless the station is in audio-only mode. Discussion: For instance, the voting equipment might beep if the voter attempts to overvote. If so, there would have to be an equivalent visual cue, such as the appearance of an icon, or a blinking element. Some voting equipment may have an audio-only mode, in which case, there would be no visual cue.	***YES***
3.2.6	Speech The voting process shall be accessible to voters with speech disabilities.	***YES***
3.2.6.a	No voting equipment shall require voter speech for its operation. Discussion: This does not preclude voting equipment from offering speech input as an option, but speech must not be the only means of input.	***YES***
3.2.7	English Proficiency	
3.2.7	For voters who lack proficiency in reading English, or whose primary language is unwritten, the voting equipment shall provide spoken instructions and ballots in the preferred language of the voter, consistent with state and federal law. The requirements of 3.2.2.2 (c) shall apply to this mode of interaction.	***YES***
3.2.8	Cognition	
3.2.8	The voting process should be accessible to voters with cognitive disabilities. Discussion: At present there are no design features specifically aimed at helping those with cognitive disabilities. Requirements 3.2.2.1 (f), the synchronization of audio with the screen in a DRE, is helpful for some cognitive disabilities such as dyslexia. Requirements in Subsection 3.1.4 also address cognitive issues relative to voting system usability.	***YES***
4	Hardware Requirements This section contains the requirements for the machines and manufactured devices that are part of a voting system. It specifies minimum values for certain performance characteristics; physical characteristics; and design, construction, and maintenance characteristics for the hardware and selected related components of all voting systems, such as: Ballot printers " Ballot cards and sheets " Ballot displays " Voting devices • Removable electronic data storage media • Servers • Printers This section applies to the combination of software and hardware to accomplish specific performance and system control requirements. Standards that are specific to software alone are provided in Section 5. The requirements of this section apply generally to all hardware used in voting systems, including: • Hardware provided by the voting system vendor and its suppliers • Hardware furnished by an external provider (for example, providers of commercial-off-the-shelf equipment) where the hardware may be used in any way during voting system operation • Hardware provided by the voting jurisdiction	
4.1	Performance Requirements The performance requirements address a broad range of parameters, encompassing: Accuracy requirements	
4.1	Performance requirements for voting systems represent the combined operational capability of both system hardware and software. Accuracy, as measured by data error rate, and operational failure are treated as distinct attributes in performance testing. All systems shall meet the performance requirements under operating conditions and after storage under non-operating conditions.	***YES***

Manufacturer: **Dominion Voting Systems**

Requirement	*Requirement Text*	*Conform*
4.1.1	Accuracy Requirements Voting system accuracy addresses the accuracy of data for each of the individual ballot positions that could be selected by a voter, including the positions that are not selected. For a voting system, accuracy is defined as the ability of the system to capture, record, store, consolidate and report the specific selections and absence of selections, made by the voter for each ballot position without error. Required accuracy is defined in terms of an error rate that for testing purposes represents the maximum number of errors allowed while processing a specified volume of data. This rate is set at a sufficiently stringent level that the likelihood of voting system errors affecting the outcome of an election is exceptionally remote even in the closest of elections. The error rate is defined using a convention that recognizes differences in how vote data is processed by different types of voting systems. Paper-based and DRE systems have different processing steps. Some differences also exist between precinct count and central count systems. Therefore, the acceptable error rate applies separately and distinctly to each of the following functions:	
4.1.1.a	For all paper-based voting systems:	
4.1.1.a.i	Scanning ballot positions on paper ballots to detect selections for individual candidates and contests	***YES***
4.1.1.a.ii	Conversion of selections detected on paper ballots into digital data	***YES***
4.1.1.b	For all DRE voting systems:	
4.1.1.b.i	Recording the voter selections of candidates and contests into voting data storage	***YES***
4.1.1.b.ii	Recording voter selections of candidates and contests into ballot image storage independently from voting data storage	***YES***
4.1.1.c	For precinct-count voting systems (paper-based and DRE):	
4.1.1.c.i	Consolidation of vote selection data from multiple precinct-based voting machines to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data	***YES***
4.1.1.d	For central-count voting systems (paper-based and DRE):	
4.1.1.d.i	Consolidation of vote selection data from multiple counting devices to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data	***YES***
4.1.1.end	For testing purposes, the acceptable error rate is defined using two parameters: the desired error rate to be achieved, and the maximum error rate that should be accepted by the test process. For each processing function indicated above, the voting system shall achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions.	***YES***
4.1.2	Environmental Requirements	
4.1.2	The environmental requirements for voting systems include shelter, space, furnishings and fixtures, supplied energy, environmental control, and external telecommunications services. Environmental conditions applicable to the design and operation of voting systems consist of the following categories: Natural environment • Induced environment, including proper and improper operation and handling of the system and its components during the election processes • Transportation and storage • Electromagnetic signal environment, including exposure to and generation of radio frequency energy All voting systems shall be designed to withstand the environmental conditions contained in the appropriate test procedures of the Guidelines. These procedures will be applied to all devices for casting, scanning and counting ballots, except those that constitute COTS devices that have not been modified in any manner to support their use as part of a voting system and that have a documented record of performance under conditions defined in the Guidelines. The Technical Data Package supplied by the vendor shall include a statement of all requirements and restrictions regarding environmental protection, electrical service, recommended auxiliary power, telecommunications service, and any other facility or resource required for the proper installation and operation of the system.	***YES***
4.1.2.1	Shelter Requirements	

Requirement	Requirement Text	Conform
4.1.2.1	All precinct count systems shall be designed for storage and operation in any enclosed facility ordinarily used as a warehouse or polling place, with prominent instructions as to any special storage requirements.	***YES***
4.1.2.2	Space Requirements	
4.1.2.2	There is no restriction on space allowed for the installation of voting systems, except that the arrangement of these systems shall not impede performance of their duties by polling place officials, the orderly flow of voters through the polling place or the ability for the voter to vote in private.	***YES***
4.1.2.3	Furnishings and Fixtures	
4.1.2.3	Any furnishings or fixtures provided as a part of voting systems, and any components provided by the vendor that are not a part of the voting system but that are used to support its storage, transportation or operation, shall comply with the safety design of Subsection 4.3.8.	***YES***
4.1.2.4	Electrical Supply Components of voting systems that require an electrical supply shall meet the following standards:	
4.1.2.4.a	Precinct count voting systems shall operate with the electrical supply ordinarily found in polling places (Nominal 120 Vac/60Hz/1 phase)	***YES***
4.1.2.4.b	Central count voting systems shall operate with the electrical supply ordinarily found in central tabulation facilities or computer room facilities (Nominal 120 Vac/60Hz/1, nominal 208 Vac/60Hz/3 or nominal 240 Vac/60Hz/2)	***YES***
4.1.2.4.c	All voting machines shall also be capable of operating for a period of at least 2 hours on backup power, such that no voting data is lost or corrupted nor normal operations interrupted. When backup power is exhausted the voting machine shall retain the contents of all memories intact. The backup power capability is not required to provide lighting of the voting area.	***YES***
4.1.2.5	Electrical Power Disturbance Vote scanning and counting equipment for paper-based voting systems, and all DRE voting equipment, shall be able to withstand, without disruption of normal operation or loss of data:	
4.1.2.5.a	Voltage dip of 30% of nominal @10 ms;	***YES***
4.1.2.5.b	Voltage dip of 60% of nominal @100 ms & 1 sec	***YES***
4.1.2.5.c	Voltage dip of >95% interrupt @5 sec	***YES***
4.1.2.5.d	Surges of +15% line variations of nominal line voltage	***YES***
4.1.2.5.e	Electric power increases of 7.5% and reductions of 12.5% of nominal specified power supply for a period of up to four hours at each power level	***YES***
4.1.2.6	Electrical Fast Transient Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand, without disruption of normal operation or loss of data, electrical fast transients of:	
4.1.2.6.a	+ 2 kV and - 2 kV on External Power lines (both AC and DC)	***YES***
4.1.2.6.b	+ 1 kV and - 1 kV on Input/Output lines(signal, data, and control lines) longer than 3 meters	***YES***
4.1.2.6.c	Repetition Rate for all transient pulses will be 100 kHz	
4.1.2.7	Lightning Surge Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand, without disruption of normal operation or loss of data, surges of:	
4.1.2.7.a	+2 kV AC line to line	***YES***
4.1.2.7.b	+2 kV AC line to earth	***YES***
4.1.2.7.c	+ or – 0.5 kV DC line to line >10m	***YES***
4.1.2.7.d	+ or – 0.5 kV DC line to earth >10m	***YES***
4.1.2.7.e	+1 kV I/O sig/control >30m	***YES***
4.1.2.8	Electrostatic Disruption	

Requirement	Requirement Text	Conform
4.1.2.8	Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand ±15 kV air discharge and ±8 kV contact discharge without damage or loss of data. The equipment may reset or have momentary interruption so long as normal operation is resumed without human intervention or loss of data. Loss of data means votes that have been completed and confirmed to the voter.	***YES***
4.1.2.9	Electromagnetic Emissions	
4.1.2.9	Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall comply with the Rules and Regulations of the Federal Communications Commission, Part 15; Class B requirements for both radiated and conducted emissions.	***YES***
4.1.2.10	Electromagnetic Susceptibility	
4.1.2.10	Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand an electromagnetic field of 10 V/m modulated by a 1 kHz 80% AM modulation over the frequency range of 80 MHz to 1000 MHz, without disruption of normal operation or loss of data.	***YES***
4.1.2.11	Conducted RF Immunity Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand, without disruption of normal operation or loss of data, conducted RF energy of:	
4.1.2.11.a	10V rms over the frequency range 150 KHz to 80 MHz with an 80% amplitude modulation with a 1 KHz sine wave AC & DC power	***YES***
4.1.2.11.b	10V sig/control >3 m over the frequency range 150 KHz to 80 MHz with an 80% amplitude modulation with a 1 KHz sine wave	***YES***
4.1.2.12	Magnetic Fields Immunity	
4.1.2.12	Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand, without disruption of normal operation or loss of data, AC magnetic fields of 30 A/m at 60 Hz.	***YES***
4.1.2.13	Environmental Control – Operating Environment	
4.1.2.13	Equipment used for election management activities or vote counting (including both precinct and central count systems) shall be capable of operation in temperatures ranging from 50 to 95 degrees Fahrenheit.	***YES***
4.1.2.14	Environmental Control – Transit and Storage Equipment used for vote casting or for counting votes in a precinct count system, shall meet these specific minimum performance standards that simulate exposure to physical shock and vibration associated with handling and transportation by surface and air common carriers, and to temperature conditions associated with delivery and storage in an uncontrolled warehouse environment:	
4.1.2.14.a	High and low storage temperatures ranging from -4 to +140 degrees Fahrenheit, equivalent to MIL-STD-810D, Methods 501.2 and 502.2, Procedure I-Storage	***YES***
4.1.2.14.b	Bench handling equivalent to the procedure of MIL-STD-810D, Method 516.3, Procedure VI	***YES***
4.1.2.14.c	Vibration equivalent to the procedure of MIL-STD-810D, Method 514.3, Category 1- Basic Transportation, Common Carrier	***YES***
4.1.2.14.d	Uncontrolled humidity equivalent to the procedure of MIL-STD-810D, Method 507.2, Procedure I-Natural Hot-Humid	***YES***
4.1.2.15	Data Network Requirements	
4.1.2.15	Voting systems may use a local or remote data network. If such a network is used, then all components of the network shall comply with the telecommunications requirements described in Section 6 and the Security requirements described in Section 7.	***YES***
4.1.3	Election Management System (EMS) Requirements The Election Management System (EMS) requirements address electronic hardware and software used to conduct the pre-voting functions defined in Section 2 with regard to ballot preparation, election programming, ballot and program installation, readiness testing, verification at the polling place, and verification at the central location.	

Requirement	Requirement Text	Conform
4.1.3.1	Recording Requirements Voting systems shall accurately record all election management data entered by the user, including election officials or their designees. For recording accuracy, all systems shall:	
4.1.3.1.a	Record every entry made by the user	YES
4.1.3.1.b	Add permissible voter selections correctly to the memory components of the device	YES
4.1.3.1.c	Verify the correctness of detection of the user selections and the addition of the selections correctly to memory	YES
4.1.3.1.d	Add various forms of data entered directly by the election official or designee, such as text, line art, logos, and images	YES
4.1.3.1.e	Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory	YES
4.1.3.1.f	Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals	YES
4.1.3.1.g	Log corrected data errors by the voting system	YES
4.1.3.2	Memory Stability	
4.1.3.2	Memory devices used to retain election management data shall have demonstrated error-free data retention for a period of 22 months.	YES
4.1.4	Vote Recording Requirements The vote recording requirements address the enclosure, equipment, and supplies used by voters to vote.	
4.1.4.1	Common Requirements All voting systems shall provide voting booths or enclosures for poll site use. Such booths or enclosures may be integral to the voting system or supplied as components of the voting system, and shall:	YES
4.1.4.1.a	Be integral to, or make provision for, the installation of the voting machine	YES
4.1.4.1.b	Ensure by its structure stability against movement or overturning during entry, occupancy, and exit by the voter	YES
4.1.4.1.c	Provide privacy for the voter, and be designed in such a way as to prevent observation of the ballot by any person other than the voter	YES
4.1.4.1.d	Be capable of meeting the accessibility requirements of Subsection 3.2	YES
4.1.4.2	Paper-based Recording Requirements The paper-based recording requirements govern: Ballot cards or sheets	
4.1.4.2.a	Paper ballots used by paper-based voting systems shall meet the following standards:	
4.1.4.2.a.i	Marks that identify the unique ballot format shall be outside the area in which votes are recorded, so as to minimize the likelihood that these marks will be mistaken for vote responses and the likelihood that recorded votes will obliterate these marks	YES
4.1.4.2.a.ii	If printed alignment marks are used to locate the vote response fields on the ballot, these marks shall be outside the area in which votes are recorded, so as to minimize the likelihood that these marks will be mistaken for vote responses and the likelihood that recorded votes will obliterate these marks	YES
4.1.4.2.a.iii	The Technical Data Package shall specify the required paper stock, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of mark fields used for vote response fields and to identify unique ballot formats, placement of alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system	YES
4.1.4.2.b	Marking Devices The Technical Data Package shall specify marking devices, which, if used to make the prescribed form of mark, produce readable marked ballots such that the system meets the performance requirements for accuracy in Subsection 4.1.1. Marking devices can be either manual (such as pens or pencils) or electronic. These specifications shall identify:	YES
4.1.4.2.b.i	Specific characteristics of marking devices that affect readability of marked ballots	YES
4.1.4.2.b.ii	Performance capabilities with regard to each characteristic	YES

Requirement	Requirement Text	Conform
4.1.4.2.b.iii	For marking devices manufactured by multiple external sources, a listing of sources and model numbers that are compatible with the system	YES
4.1.4.2.c	Frames or Fixtures for Printed Ballots A frame or fixture for printed ballot cards is optional. However, if such a device is provided, it shall:	N/A
4.1.4.2.c.i	Be of any size and shape consistent with its intended use	N/A
4.1.4.2.c.ii	Position the card properly	N/A
4.1.4.2.c.iii	Hold the ballot card securely in its proper location and orientation for voting	N/A
4.1.4.2.c.iv	Comply with the requirements for design and construction contained in Subsection 4.3	N/A
4.1.4.2.d.	Ballot Boxes and Ballot Transfer Boxes Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, shall:	
4.1.4.2.d.i	Be of any size, shape, and weight commensurate with their intended use	YES
4.1.4.2.d.ii	Incorporate locks or seals, the specifications of which are described in the system documentation	YES
4.1.4.2.d.iii	Provide specific points where ballots are inserted, with all other points on the box constructed in a manner that prevents ballot insertion	YES
4.1.4.2.d.iv	For precinct count systems, contain separate compartments for the segregation of unread ballots, ballots containing write-in votes or any irregularities that may require special handling or processing. In lieu of compartments, the conversion processing may mark such ballots with an identifying spot or stripe to facilitate manual segregation	YES
4.1.4.3	DRE System Recording Requirements The DRE system recording requirements address the detection and recording of votes, including the logic and data processing functions required to determine the validity of voter selections, to accept and record valid selections, and to reject invalid selections. The requirements also address the physical environment in which ballots are cast.	
4.1.4.3.a	Activity Indicator DRE systems shall include an audible or visible activity indicator providing the status of each voting device. This indicator shall:	YES
4.1.4.3.a.i	Indicate whether the device has been activated for voting	YES
4.1.4.3.a.ii	Indicate whether the device is in use	YES
4.1.4.3.b	Vote Recording Accuracy and Integrity To ensure vote recording accuracy and integrity while protecting the anonymity of the voter, all DRE systems shall:	YES
4.1.4.3.b.i	Contain all mechanical, electromechanical, and electronic components; software; and controls required to detect and record the activation of selections made by the voter in the process of voting and casting a ballot	YES
4.1.4.3.b.ii	Incorporate redundant memories to detect and allow correction of errors caused by the failure of any of the individual memories	YES
4.1.4.3.b.iii	Provide at least two processes that record the voter's selections that: To the extent possible	YES
4.1.4.3.b.iv	Use a different process to store ballot images, for which the method of recording may include any appropriate encoding or data compression procedure consistent with the regeneration of an unequivocal record of the ballot as cast by the voter	YES
4.1.4.3.b.v	Provide a capability to retrieve ballot images in a form readable by humans	YES
4.1.4.3.b.vi	Ensure that all processing and storage protects the anonymity of the voter	YES
4.1.4.3.c	Recording Accuracy DRE systems shall meet the following requirements for recording accurately each vote and ballot cast:	
4.1.4.3.c.i	Detect every selection made by the voter	YES
4.1.4.3.c.ii	Correctly add permissible selections to the memory components of the device	YES
4.1.4.3.c.iii	Verify the correctness of the detection of the voter selections and the addition of the selections to memory	YES
4.1.4.3.c.iv	Achieve an error rate not to exceed the requirement indicated in Subsection 4.1.1	YES

Requirement	Requirement Text	Conform
4.1.4.3.c.v	Preserve the integrity of voting data and ballot images (for DRE machines) stored in memory for the official vote count and audit trail purposes against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals	***YES***
4.1.4.3.c.vi	Maintain a log of corrected data	***YES***
4.1.4.3.end	Recording reliability refers to the ability of the DRE system to record votes accurately at its maximum rated processing volume for a specified period of time. The DRE system shall record votes reliably in accordance with the requirements of Subsection 4.3.3.	***YES***
4.1.5	Paper-based Conversion Requirements The paper-based conversion requirements address the ability of the system to read the ballot card and to translate its pattern of marks into electronic signals for later processing. These capabilities may be built into the voting system in an integrated fashion, or may be provided by one or more components that are not unique to the system, such as a general purpose data processing card reader or read head suitably interfaced to the system. These requirements address two major functions: ballot handling and ballot reading.	
4.1.5	Ballot Handling Ballot handling consists of a ballot card's acceptance, movement through the read station, and transfer into a collection station or receptacle.	
4.1.5.1.a	The capacity to convert the marks on individual ballots into signals is uniquely important to central count systems. The capacity for a central count system shall be documented by the vendor. This documentation shall include the capacity for individual components that impact the overall capacity	***YES***
4.1.5.1.b	Unreadable Ballots (Central Count Paper-based) When ballots are unreadable or some condition is detected requiring that the cards be segregated from normally processed ballots for human review (e.g. write-ins), all central count paper-based systems shall do one of the following:	
4.1.5.1.b.i	Outstack the ballot	***YES***
4.1.5.1.b.ii	Stop the ballot reader and display a message prompting the election official or designee to remove the ballot	***YES***
4.1.5.1.b.iii	Mark the ballot with an identifying mark to facilitate its later identification	***N/A***
4.1.5.1.c	Additionally, the system shall provide a capability that can be activated by an authorized election official to identify ballots containing overvotes, blank ballots, and ballots containing undervotes in a designated contest. If enabled, these capabilities shall perform one of the above actions in response to the indicated condition.	***YES***
4.1.5.1.d	Unreadable Ballots (Precinct Count) When ballots are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review (e.g. write-in votes) all precinct count systems shall:	
4.1.5.1.d.i	In response to an unreadable or blank ballot, return the ballot and provide a message prompting the voter to examine the ballot	***YES***
4.1.5.1.d.ii	In response to a ballot with a write-in vote, segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification	***YES***
4.1.5.1.d.iii	In response to a ballot with an overvote the system shall: Provide a capability to identify an overvoted ballot " Return the ballot " Provide an indication prompting the voter to examine the ballot " Allow the voter to correct the ballot " Provide a means for an authorized election official to deactivate this capability entirely and by contest "	***YES***
4.1.5.1.d.iv	In response to a ballot with an undervote, the system shall: Provide a capability to identify an undervoted ballot " Return the ballot " Provide an indication prompting the voter to examine the ballot " Allow the voter to correct the ballot " Allow the voter to submit the ballot with the undervote " Provide a means for an authorized election official to deactivate this capability "	***YES***
4.1.5.1.e	Ballot readers shall prevent multiple feed or detect and provide an alarm indicating multiple feed. Multiple feed occurs when a ballot reader attempts to read more than one ballot at a time.	***YES***

Requirement	Requirement Text	Conform
4.1.5.1.e.i	If multiple feed is detected, the card reader shall halt in a manner that permits the operator to remove the unread cards causing the error, and reinsert them in the card input hopper	YES
4.1.5.1.e.ii	The frequency of multiple feeds with ballots intended for use with the system shall not exceed l in 10,000	YES
4.1.5.2	Ballot Reading Accuracy This paper-based system requirement governs the conversion of the physical ballot into electronic data. Reading accuracy for ballot conversion refers to the ability to:	
4.1.5.2.a	Recognize vote punches or marks, or the absence thereof, for each possible selection on the ballot	YES
4.1.5.2.b	Discriminate between valid punches or marks and extraneous perforations, smudges, and folds	YES
4.1.5.2.c	Convert the vote punches or marks, or the absence thereof, for each possible selection on the ballot into digital signals	YES
4.1.5.2.d	To ensure accuracy, paper-based systems shall: Detect punches or marks that conform to vendor specifications with an error rate not exceeding the requirement indicated in Subsection 4.1.1	YES
4.1.5.2.e	To ensure accuracy, paper-based systems shall: Ignore, and not record, extraneous perforations, smudges, and folds	YES
4.1.5.2.f	To ensure accuracy, paper-based systems shall: Reject ballots that meet all vendor specifications at a rate not to exceed 2 percent	YES
4.1.6	Tabulation Processing Requirements Tabulation processing requirements apply to the hardware and software required to accumulate voting data for all candidates and measures within voting machines and polling places, and to consolidate the voting data at a central level or multiple levels. These requirements also address the generation and maintenance of audit records, the detection and disabling of improper use or operation of the system, and the monitoring of overall system status. Separate and distinct requirements for paper-based and DRE voting systems are presented below.	
4.1.6.1	Paper Based Processing Requirements The paper-based processing requirements address all mechanical devices, electromechanical devices, electronic devices, and software required to perform the logical and numerical functions of interpreting the electronic image of the voted ballot, and assigning votes to the proper memory registers.	YES
4.1.6.1.a	Processing Accuracy Processing accuracy refers to the ability of the system to receive electronic signals produced by punches for punchcard systems and vote marks and timing information for marksense systems; perform logical and numerical operations upon these data; and reproduce the contents of memory when required, without error. Specific requirements are detailed below:	YES
4.1.6.1.a.i	Processing accuracy shall be measured by vote selection error rate, the ratio of uncorrected vote selection errors to the total number of ballot positions that could be recorded across all ballots when the system is operated at its nominal or design rate of processing	YES
4.1.6.1.a.ii	The vote selection error rate shall include data that denotes ballot style or precinct as well as data denoting a vote in a specific contest or ballot proposition	YES
4.1.6.1.a.iii	The vote selection error rate shall include all errors from any source	YES
4.1.6.1.a.iv	The vote selection error rate shall not exceed the requirement indicated in Subsection 4.1.1	YES
	Paper-based Devices	
4.1.6.1.b	Paper-based system memory devices, used to retain control programs and data, shall have demonstrated error-free data retention for a period of 22 months, under the environmental conditions for operation and non-operation (i.e., storage).	YES
4.1.6.2	DRE Voting Systems The DRE voting systems processing requirements address all mechanical devices, electromechanical devices, electronic devices, and software required to process voting data after the polls are closed.	

Manufacturer: **Dominion Voting Systems**

Requirement	Requirement Text	Conform
4.1.6.2.a.	Processing Speed DRE voting systems shall meet the following requirements for processing speed:	
4.1.6.2.a.i	Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds)	***YES***
4.1.6.2.a.ii	If the consolidation of polling place data is done locally, perform this consolidation in a time not to exceed five minutes for each device in the polling place	***N/A***
4.1.6.2.b	Processing Accuracy Processing accuracy is defined as the ability of the system to process voting data stored in DRE voting devices or in removable memory modules installed in such devices. Processing includes all operations to consolidate voting data after the polls have been closed. DRE voting systems shall:	
4.1.6.2.b.i	Produce reports that are completely consistent, with no discrepancy among reports of voting device data produced at any level	***YES***
4.1.6.2.b.ii	Produce consolidated reports containing absentee, provisional or other voting data that are similarly error-free. Any discrepancy, regardless of source, is resolvable to a procedural error, to the failure of a non-memory device or to an external cause	***YES***
4.1.6.2.c	Memory Stability	
4.1.6.2.c	DRE system memory devices used to retain control programs and data shall have demonstrated error-free data retention for a period of 22 months. Error-free retention may be achieved by the use of redundant memory elements, provided that the capability for conflict resolution or correction among elements is included.	***YES***
4.1.7	Reporting Requirements The reporting requirements govern all mechanical, electromechanical, and electronic devices required for voting systems to print audit record entries and results of the tabulation. These requirements also address data storage media for transportation of data to other sites.	
4.1.7.1	Removable Storage Media	
4.1.7.1	In voting systems that use storage media that can be removed from the system and transported to another location for readout and report generation, these media shall use devices with demonstrated error-free retention for a period of 22 months under the environmental conditions for operation and non-operation contained in Subsection 4.1.2. Examples of removable storage media include: programmable read-only memory (PROM), random access memory (RAM) with battery backup, magnetic media or optical media.	***YES***
4.1.7.2	Printers All printers used to produce reports of the vote count shall be capable of producing:	
4.1.7.2.a	Alphanumeric headers	***YES***
4.1.7.2.b	Election, office and issue labels	***YES***
4.1.7.2.c	Alphanumeric entries generated as part of the audit record	***YES***
4.1.8	Vote Data Management Requirements The vote data management requirements for all systems address capabilities that manage, process, and report voting data after the data has been consolidated at the polling place or other jurisdictional levels. These capabilities allow the system to: Consolidate voting data from polling place data memory or transfer devices " Report polling place summaries " Process absentee ballots	
4.1.8.1	Data File Management All voting systems shall provide the capability to:	
4.1.8.1.a	Integrate voting data files with ballot definition files	***YES***
4.1.8.1.b	Verify file compatibility	***YES***
4.1.8.1.c	Edit and update files as required	***YES***
4.1.8.2	Data Report Generation	
4.1.8.2	All voting systems shall include report generators for producing output reports at the device, polling place, and summary level, with provisions for administrative and judicial subdivisions as required by the using jurisdiction.	***YES***

Manufacturer: **Dominion Voting Systems**

Requirement	*Requirement Text*	*Conform*
4.2	Physical Characteristics This subsection covers physical characteristics of all voting systems and components that affect their general utility and suitability for election operations.	
4.2.1	Size	
4.2.1	There is no numerical limitation on the size of any voting equipment, but the size of each voting machine should be compatible with its intended use and the location at which the equipment is to be used.	***YES***
4.2.2	Weight	
4.2.2	There is no numerical limitation on the weight of any voting equipment, but the weight of each voting machine should be compatible with its intended use and the location at which the equipment is to be used.	***YES***
4.2.3	Transport and Storage of Precinct Systems: All precinct voting systems shall:	
4.2.3.a	Provide a means to safely and easily handle, transport, and install voting equipment, such as wheels or a handle or handles	***YES***
4.2.3.b.i	Be capable of using, or be provided with, a protective enclosure rendering the equipment capable of withstanding: Impact, shock and vibration loads associated with surface and air transportation	***YES***
4.2.3.b.ii	Be capable of using, or be provided with, a protective enclosure rendering the equipment capable of withstanding: Stacking loads associated with storage	***YES***
4.3	Design, Construction, and Maintenance Characteristics This subsection covers voting system materials, construction workmanship, and specific design characteristics important to the successful operation and efficient maintenance of the voting system.	
4.3.1	Materials, Processes, and Parts The approach to system design is unrestricted, and may incorporate any form or variant of technology capable of meeting the voting systems requirements and standards.	
4.3.1	Precinct count systems shall be designed in accordance with best commercial practice for microcomputers, process controllers, and their peripheral components. Central count voting systems and equipment used in a central tabulating environment shall be designed in accordance with best commercial and industrial practice.	***YES***
4.3.1	All voting systems shall:	
4.3.1.a	Be designed and constructed so that the frequency of equipment malfunctions and maintenance requirements are reduced to the lowest level consistent with cost constraints	***YES***
4.3.1.b	Include, as part of the accompanying Technical Data Package, an approved parts list	***YES***
4.3.1.c	Exclude parts or components not included in the approved parts list	***YES***
4.3.2	Durability	
4.3.2	All voting systems shall be designed to withstand normal use without deterioration and without excessive maintenance cost for a period of ten years.	***YES***
4.3.3	Reliability	
4.3.3	The reliability of voting system devices shall be measured as Mean Time Between Failure (MTBF) for the system submitted for testing. MBTF is defined as the value of the ratio of operating time to the number of failures which have occurred in the specified time interval. A typical system operations scenario consists of approximately 45 hours of equipment operation, consisting of 30 hours of equipment set-up and readiness testing and 15 hours of elections operations. For the purpose of demonstrating compliance with this requirement, a failure is defined as any event which results in either the: Loss of one or more functions " • Degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds	
4.3.3	The MTBF demonstrated during certification testing shall be at least 163 hours.	***YES***

Requirement	Requirement Text	Conform
4.3.4	Maintainability	
4.3.4	Maintainability represents the ease with which maintenance actions can be performed based on the design characteristics of equipment and software and the processes the vendor and election officials have in place for preventing failures and for reacting to failures. Maintainability includes the ability of equipment and software to self-diagnose problems and make non-technical election workers aware of a problem. Maintainability addresses all scheduled and unscheduled events, which are performed to: Determine the operational status of the system or a component; adjust, align, tune or service components; repair or replace a component having a specified operating life or replacement interval; repair or replace a component that exhibits an undesirable predetermined physical condition or performance degradation; repair or replace a component that has failed; verify the restoration of a component or the system to operational status	***YES***
4.3.4	Maintainability shall be determined based on the presence of specific physical attributes that aid system maintenance activities, and the ease with which system maintenance tasks can be performed by the test lab. Although a more quantitative basis for assessing maintainability, such as the Mean Time to Repair the system is desirable, the certification of a system is conducted before it is approved for sale and thus before a broader base of maintenance experience can be obtained.	
4.3.4.1	Physical Attributes The following physical attributes will be examined to assess reliability:	
4.3.4.1.a	Presence of labels and the identification of test points	***YES***
4.3.4.1.b	Provision of built-in test and diagnostic circuitry or physical indicators of condition	***YES***
4.3.4.1.c	Presence of labels and alarms related to failures	***YES***
4.3.4.1.d	Presence of features that allow non-technicians to perform routine maintenance tasks (such as update of the system database)	***YES***
4.3.4.2	Additional Attributes The following additional attributes will be considered to assess system maintainability:	
4.3.4.2.a	Ease of detecting that equipment has failed by a non-technician	***YES***
4.3.4.2.b	Ease of diagnosing problems by a trained technician	***YES***
4.3.4.2.c	Low false alarm rates (i.e., indications of problems that do not exist)	***YES***
4.3.4.2.d	Ease of access to components for replacement	***YES***
4.3.4.2.e	Ease with which adjustment and alignment can be performed	***YES***
4.3.4.2.f	Ease with which database updates can be performed by a non-technician	***YES***
4.3.4.2.g	Adjust, align, tune or service components	***YES***
4.3.5	Availability The availability of a voting system is defined as the probability that the equipment (and supporting software) needed to perform designated voting functions will respond to operational commands and accomplish the function. The voting system shall meet the availability standard for each of the following voting functions:	
4.3.5.a.	For all paper-based systems:	
4.3.5.a.i	Recording voter selections (such as by ballot marking or punch)	***YES***
4.3.5.a.ii	Scanning the punches or marks on paper ballots and converting them into digital data	***YES***
4.3.5.b	For all DRE systems, recording and storing voter ballot selections	***YES***
4.3.5.c	For precinct count systems (paper-based and DRE), consolidation of vote selection data from multiple precinct based systems to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data	***YES***
4.3.5.d	For central-count systems (paper-based and DRE), consolidation of vote selection data from multiple counting devices to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data	***YES***

Requirement	*Requirement Text*	*Conform*
4.3.5	System availability is measured as the ratio of the time during which the system is operational (up time) to the total time period of operation (up time plus down time). Inherent availability (Ai) is the fraction of time a system is functional, based upon Mean Time Between Failure (MTBF) and Mean Time To Repair (MTTR), that is: Ai = (MTBF)/(MTBF + MTTR) MTTR is the average time required to perform a corrective maintenance task during periods of system operation. Corrective maintenance task time is active repair time, plus the time attributable to other factors that could lead to logistic or administrative delays, such as travel notification of qualified maintenance personnel and travel time for such personnel to arrive at the appropriate site. Corrective maintenance may consist of substitution of the complete device or one of its components, as in the case of precinct count and some central count systems, or it may consist of on-site repair. The voting system shall achieve at least 99 percent availability during normal operation for the functions indicated above. This standard encompasses for each function the combination of all devices and components that support the function, including their MTTR and MTBF attributes.	
4.3.5	Vendors shall specify the typical system configuration that is to be used to assess availability, and any assumptions made with regard to any parameters that impact the MTTR. These factors shall include at a minimum:	***YES***
4.3.5.e	Recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation	***YES***
4.3.5.f	Recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation	***YES***
4.3.5.g	Organizational affiliation (i.e., jurisdiction, vendor) of qualified maintenance personnel	***YES***
4.3.6	Product Marking All voting systems shall:	
4.3.6.a	Identify all devices by means of a permanently affixed nameplate or label containing the name of the manufacturer or vendor, the name of the device, its part or model number, its revision letter, its serial number, and if applicable, its power requirements	***YES***
4.3.6.b	Display on each device a separate data plate containing a schedule for and list of operations required to service or to perform preventive maintenance	***YES***
4.3.6.c	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	***YES***
4.3.7	Workmanship To help ensure proper workmanship, all manufacturers of voting systems shall:	
4.3.7.a	Adopt and adhere to practices and procedures to ensure that their products are free from damage or defect that could make them unsatisfactory for their intended purpose	***YES***
4.3.7.b	Ensure that components provided by external suppliers are free from damage or defect that could make them unsatisfactory for their intended purpose	***YES***
4.3.8	Safety All voting systems shall meet the following requirements for safety:	
4.3.8.a	All voting systems and their components shall be designed to eliminate hazards to personnel or to the equipment itself	***YES***
4.3.8.b	Defects in design and construction that can result in personal injury or equipment damage must be detected and corrected before voting systems and components are placed into service	***YES***
4.3.8.c	Equipment design for personnel safety shall be equal to or better than the appropriate requirements of the Occupational Safety and Health Act, Code of Federal Regulations, Title 29, Part 1910	***YES***
5	Software Requirements The requirements of this section are intended to ensure that voting system software is reliable, robust, testable, and maintainable. The requirements in this section also support system accuracy, logical correctness, privacy, security and integrity. The general requirements of this section apply to software used to support the entire range of voting system activities described in Section 2.	
5.3	Data and Document Retention All systems shall:	

Requirement	Requirement Text	Conform
5.3.a	Maintain the integrity of voting and audit data during an election, and for at least 22 months thereafter, a time sufficient to resolve most contested elections and support other activities related to the reconstruction and investigation of a contested election	YES
5.3.b	Protect against the failure of any data input or storage device at a location controlled by the jurisdiction or its contractors, and against any attempt at improper data entry or retrieval	YES
5.4	Audit Record Data	
5.4	Audit trails are essential to ensure the integrity of a voting system. Operational requirements for audit trails are described in Subsection 2.5.1.1. Audit record data are generated by these procedures. The audit record data in the following subsections are essential to the complete recording of election operations and reporting of the vote tally. This list of audit records may not reflect the design constructs of some systems. Therefore, vendors shall supplement it with information relevant to the operation of their specific systems.	
5.4.1	Pre-election Audit Records	
5.4.1	During election definition and ballot preparation, the system shall audit the preparation of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates. The log shall include:	YES
5.4.1.a	The allowable number of selections a contest	YES
5.4.1.b	The combinations of voting patterns permitted or required by the jurisdiction	YES
5.4.1.c	The inclusion or exclusion of contests as the result of multiple districting within the polling place	YES
5.4.1.d	Any other characteristics that may be peculiar to the jurisdiction, the election or the polling place location	YES
5.4.1.e	Manual data maintained by election personnel	YES
5.4.1.f	Samples of all final ballot formats	YES
5.4.1.g	Ballot preparation edit listings	YES
5.4.2	System Readiness Audit Records The following minimum requirements apply to system readiness audit records:	
5.4.2.a	Prior to the start of ballot counting, a system process shall verify hardware and software status and generate a readiness audit record. This record shall include the identification of the software release, the identification of the election to be processed, and the results of software and hardware diagnostic tests	YES
5.4.2.b	In the case of systems used at the polling place, the record shall include polling place identification	YES
5.4.2.c	The ballot interpretation logic shall test and record the correct installation of ballot formats on voting devices	YES
5.4.2.d	The software shall check and record the status of all data paths and memory locations to be used in vote recording to protect against contamination of voting data	YES
5.4.2.e	Upon the conclusion of the tests, the software shall provide evidence in the audit record that the test data have been expunged	YES
5.4.2.f	If required and provided, the ballot reader and arithmetic-logic unit shall be evaluated for accuracy, and the system shall record the results. It shall allow the processing or simulated processing of sufficient test ballots to provide a statistical estimate of processing accuracy	YES
5.4.2.g	For systems that use a public network, provide a report of test ballots that includes:	YES
5.4.2.g.i	Number of ballots sent	YES
5.4.2.g.ii	When each ballot was sent	YES
5.4.2.g.iii	Machine from which each ballot was sent	YES
5.4.2.g.iv	Specific votes or selections contained in the ballot	YES
5.4.3	In-Process Audit Records In-process audit records document system operations during diagnostic routines and the casting and tallying of ballots. At a minimum, the in-process audit records shall contain:	

Requirement	Requirement Text	Conform
5.4.3.a	Machine generated error and exception messages to demonstrate successful recovery. Examples include, but are not necessarily limited to:	YES
5.4.3.a.i	The source and disposition of system interrupts resulting in entry into exception handling routines	YES
5.4.3.a.ii	All messages generated by exception handlers	YES
5.4.3.a.iii	The identification code and number of occurrences for each hardware and software error or failure	YES
5.4.3.a.iv	Notification of system login or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing	YES
5.4.3.a.v	Other exception events such as power failures, failure of critical hardware components, data transmission errors or other types of operating anomalies	YES
5.4.3.b	Critical system status messages other than informational messages displayed by the system during the course of normal operations. These items include, but are not limited to:	
5.4.3.b.i	Diagnostic and status messages upon startup	YES
5.4.3.b.ii	The “zero totals” check conducted before opening the polling place or counting a precinct centrally	YES
5.4.3.b.iii	For paper-based systems, the initiation or termination of card reader and communications equipment operation	YES
5.4.3.b.iv	For DRE machines at controlled voting locations, the event (and time, if available) of activating and casting each ballot (i.e., each voter's transaction as an event). This data can be compared with the public counter for reconciliation purposes	YES
5.4.3.c	Non-critical status messages that are generated by the machine's data quality monitor or by software and hardware condition monitors	YES
5.4.3.d	System generated log of all normal process activity and system events that require operator intervention, so that each operator access can be monitored and access sequence can be constructed	YES
5.4.4	Vote Tally Data In addition to the audit requirements described above, other election-related data is essential for reporting results to interested parties, the press, and the voting public, and is vital to verifying an accurate count.	
5.4.4	Voting systems shall meet these reporting requirements by providing software capable of obtaining data concerning various aspects of vote counting and producing printed reports. At a minimum, vote tally data shall include:	
5.4.4.a	Number of ballots cast, using each ballot configuration, by tabulator, by precinct, and by political subdivision	YES
5.4.4.b	Candidate and measure vote totals for each contest, by tabulator	YES
5.4.4.c	The number of ballots read within each precinct and for additional jurisdictional levels, by configuration, including separate totals for each party in primary elections	YES
5.4.4.d	Separate accumulation of overvotes and undervotes for each contest, by tabulator, precinct and for additional jurisdictional levels (no overvotes would be indicated for DRE voting devices)	YES
5.4.4.e	For paper-based systems only, the total number of ballots both able to be processed and unable to be processed; and if there are multiple card ballots, the total number of cards read	YES
5.4.4.end	For systems that produce an electronic file containing vote tally data, the contents of the file shall include the same minimum data cited above for printed vote tally reports.	YES
5.5	Voter Secrecy (DRE Systems) All DRE systems shall ensure vote secrecy by:	
5.5.a	Immediately after the voter chooses to cast his or her ballot, record the voter’s selections in the memory to be used for vote counting and audit data (including ballot images), and erase the selections from the display, memory, and all other storage, including all forms of temporary storage	YES

Requirement	Requirement Text	Conform
5.5.b	Immediately after the voter chooses to cancel his or her ballot, erase the selections from the display and all other storage, including buffers and other temporary storage	YES
6	Telecommunications Requirements	
6.1.2	Telecommunications Operations and Providers This section applies to voting-related transmissions over public networks, such as those provided by local distribution and long distance carriers. This section also applies to private networks regardless of whether the network is owned and operated by the election jurisdiction. For systems that transmit official data over public networks, this section applies to telecommunications components installed and operated at locations supervised by election officials, such as polling places or central offices. This includes: Components acquired by the jurisdiction for the purpose of voting	
6.1.3	Data Transmissions	
6.1.3	These requirements apply to the use of telecommunications to transmit data for the preparation of the system for an election, the execution of an election, and the preservation of the system data and audit trails during and following an election. While this section does not assume a specific model of voting system operations and does not assume a specific model for the use of telecommunications to support such operations, it does address the following types of data, where applicable: Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmits votes individually over a public network Ballot Definition: Information that describes to a voting machine the content and appearance of the ballots to be used in an election Vote Transmission: For systems that transmit votes individually over a public network, the transmission of a single vote within a network at a polling place and to the county (or contractor) for consolidation with other county vote data Vote Count: Information representing the tabulation of votes at any level within the control of the jurisdiction, such as the polling place, precinct or central count List of Voters: A listing of the individual voters who have cast ballots in a specific election Additional data transmissions used to operate a voting system in the conduct of an election, but not explicitly listed above, are also subject to the requirements of this section. For systems that transmit data using public networks, this section applies to telecommunications hardware and software for transmissions within and among all combinations of senders and receivers located at polling places, precinct count facilities and central count facilities (whether operated by the jurisdiction or a contractor).	YES
6.2	Design, Construction, and Maintenance Requirements Design, construction, and maintenance requirements for telecommunications represent the operational capability of both system hardware and software. These capabilities shall be considered basic to all data transmissions.	
6.2.1	Accuracy	
6.2.1	The telecommunications components of all voting systems shall meet the accuracy requirements of Subsection 4.1.1.	YES
6.2.2	Durability	
6.2.2	The telecommunications components of all voting systems shall meet the durability requirements of Subsection 4.3.2.	YES
6.2.3	Reliability	
6.2.3	The telecommunications components of all voting systems shall meet the reliability requirements of Subsection 4.3.3.	YES
6.2.4	Maintainability	
6.2.4	The telecommunications components of all voting systems shall meet the maintainability requirements of Subsection 4.3.4.	YES
6.2.5	Availability	
6.2.5	The telecommunications components of all voting systems shall meet the availability requirements of Subsection 4.3.5.	YES

Requirement	Requirement Text	Conform
6.2.6	Integrity For WANs using public telecommunications, boundary definition and implementation shall meet the requirements below.	***N/A***
6.2.6.a	Outside service providers and subscribers of such providers shall not be given direct access or control of any resource inside the boundary.	***N/A***
6.2.6.b	Voting system administrators shall not require any type of control of resources outside this boundary. Typically, an end point of a telecommunications circuit will be a subscriber termination on a Digital Service Unit/Customer Service Unit although the specific technology configuration may vary. Regardless of the technology used, the boundary point must ensure that everything on the voting system side is locally configured and controlled by the election jurisdiction while everything on the public network side is controlled by an outside service provider.	***N/A***
6.2.6.c	The system shall be designed and configured such that it is not vulnerable to a single point of failure in the connection to the public network which could cause total loss of voting capabilities at any polling place.	***N/A***
6.2.7	Confirmation	
6.2.7	Confirmation occurs when the system notifies the user of the successful or unsuccessful completion of the data transmission, where successful completion is defined as accurate receipt of the transmitted data. To provide confirmation, the telecommunications components of a voting system shall notify the user of the successful or unsuccessful completion of the data transmission. In the event of unsuccessful transmission the user shall be notified of the action to be taken.	***N/A***
7	Security Requirements	
7.2	Access Control	
7.2.1	General Access Control Policy The vendor shall specify the general features and capabilities of the access control policy recommended to provide effective voting system security. Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for:	
7.2.1.a	Software access controls	***YES***
7.2.1.b	Hardware access controls	***YES***
7.2.1.c	Communications	***YES***
7.2.1.d	Effective password management	***YES***
7.2.1.e	Protection abilities of a particular operating system	***YES***
7.2.1.f	General characteristics of supervisory access privileges	***YES***
7.2.1.g	Segregation of duties	***YES***
7.2.1.h	Any additional relevant characteristics	***YES***
7.2.1.1	Individual Access Privileges Voting system vendors shall:	***YES***
7.2.1.1.a	Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access	***YES***
7.2.1.1.b	Specify whether an individual's authorization is limited to a specific time, time interval or phase of the voting or counting operations	***YES***
7.2.1.1.c	Permit the voter to cast a ballot expeditiously, but preclude voter access to all aspects of the vote counting processes	***YES***
7.2.1.2	Access Control Measures Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include:	
7.2.1.2.a	Use of data and user authorization	***YES***
7.2.1.2.b	Program unit ownership and other regional boundaries	***YES***
7.2.1.2.c	One-end or two-end port protection devices	***YES***
7.2.1.2.d	Security kernels	***YES***

Requirement	Requirement Text	Conform
7.2.1.2.e	Computer-generated password keys	YES
7.2.1.2.f	Special protocols	YES
7.2.1.2.g	Message encryption	YES
7.2.1.2.h	Controlled access security	YES
7.2.1.2.end	Vendors also shall define and provide a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself.	YES
7.3	Physical Security Measures A voting system's sensitivity to disruption or corruption of data depends, in part, on the physical location of equipment and data media, and on the establishment of secure telecommunications among various locations. Most often, the disruption of voting and vote counting results from a physical violation of one or more areas of the system thought to be protected. Therefore, security procedures shall address physical threats and the corresponding means to defeat them.	
7.3.1	Polling Place Security	
7.3.1	For polling place operations, vendors shall develop and provide detailed documentation of measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences.	YES
7.3.1	The measures shall allow the immediate detection of tampering with vote casting devices and precinct ballot counters. They also shall control physical access to a telecommunications link if such a link is used	YES
7.3.2	Central Count Location Security	
7.3.2	Vendors shall develop and document in detail the measures to be taken in a central counting environment. These measures shall include physical and procedural controls related to the handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.	YES
7.4	Software Security Voting systems shall meet specific security requirements for the installation of software and for protection against malicious software.	YES
7.4.1	Software and Firmware Installation The system shall meet the following requirements for installation of software, including hardware with embedded firmware.	
7.4.1.a	If software is resident in the system as firmware, the vendor shall require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations.	YES
7.4.1.b	To prevent alteration of executable code, no software shall be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.	YES
7.4.1.c	The voting system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote counting program, and its associated exception handlers.	YES
7.4.1.d	The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.	YES
7.4.1.e	After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.	YES
7.4.2	Protection Against Malicious Software	
7.4.2	Voting systems shall deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs. Vendors shall develop and document the procedures to be followed to ensure that such protection is maintained in a current status.	YES

Requirement	Requirement Text	Conform
7.5	Telecommunications and Data Transmission There are four areas that must be addressed by telecommunications and data transmission security capabilities: access control, data integrity, detection and prevention of data interception, and protection against external threats.	
7.5.1	Maintaining Data Integrity Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function.	
7.5.1.a	Voting systems that use electrical or optical transmission of data shall ensure the receipt of valid vote records is verified at the receiving station. This should include standard transmission error detection and correction methods such as checksums or message digest hashes. Verification of correct transmission shall occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.	***N/A***
7.5.1.b	Voting systems that use telecommunications to communicate between system components and locations before the polling place is officially closed shall:	***N/A***
7.5.1.b.i	Implement an encryption standard currently documented and validated for use by an agency of the U.S. government	***N/A***
7.5.1.b.ii	Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System	***N/A***
7.5.2	Protection Against External Threats	
7.5.2.a	Voting systems that use public telecommunications networks shall implement protections against external threats to which commercial products used in the system may be susceptible.	***N/A***
7.5.2.b 7.5.2.b.i	Voting systems that use public telecommunications networks shall provide system documentation that clearly identifies all COTS hardware and software products and communications services used in the development and/or operation of the voting system, including operating systems, communications routers, modem drivers and dial-up networking software. i. Such documentation shall identify the name, vendor, and version used for each such component.	***N/A***
7.5.2.c.	Voting systems that use public telecommunications networks shall use protective software at the receiving-end of all communications paths to:	***N/A***
7.5.2.c.i	Detect the presence of a threat in a transmission	***N/A***
7.5.2.c.ii	Remove the threat from infected files/data	***N/A***
7.5.2.c.iii	Prevent against storage of the threat anywhere on the receiving device	***N/A***
7.5.2.c.iv	Provide the capability to confirm that no threats are stored in system memory and in connected storage media	***N/A***
7.5.2.c.v	Provide data to the system audit log indicating the detection of a threat and the processing performed	***N/A***
7.5.2.d	Vendors shall use multiple forms of protective software as needed to provide capabilities for the full range of products used by the voting system.	***YES***
7.5.3	Monitoring and Responding to External Threats Voting systems that use public telecommunications networks may become vulnerable, by virtue of their system components, to external threats to the accuracy and integrity of vote recording, vote counting, and vote consolidation and reporting processes. Therefore, vendors of such systems shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to:	***N/A***
7.5.4	Shared Operating Environment Ballot recording and vote counting can be performed in either a dedicated or non-dedicated environment. If ballot recording and vote counting operations are performed in an environment that is shared with other data processing functions, both hardware and software features shall be present to protect the integrity of vote counting and of vote data. Systems that use a shared operating environment shall:	***N/A***

Requirement	*Requirement Text*	*Conform*
7.5.4.a.	Use security procedures and logging records to control access to system functions	***N/A***
7.5.4.b	Partition or compartmentalize voting system functions from other concurrent functions at least logically, and preferably physically as well	***N/A***
7.5.4.c	Control system access by means of passwords, and restrict account access to necessary functions only	***N/A***
7.5.4.d	Have capabilities in place to control the flow of information, precluding data leakage through shared system resources	***N/A***
7.5.5	Incomplete Election Returns If the voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, the system shall:	***N/A***
7.5.5.a.	Be designed to provide external access to incomplete election returns (for equipment that operates in a central counting environment), only if that access for these purposes is authorized by the statutes and regulations of the using agency. This requirement applies as well to polling place equipment that contains a removable memory module or that may be removed in its entirety to a central place for the consolidation of polling place returns	***N/A***
7.5.5.b	Design voting system software and its security environment such that data accessible to interactive queries resides in an external file or database created and maintained by the elections software under the restrictions applying to any other output report:	***N/A***
7.5.5.b.i	The output file or database has no provision for write access back to the system	***N/A***
7.5.5.b.ii	Persons whose only authorized access is to the file or database are denied write access, both to the file or database, and to the system	***N/A***
7.6	Use of Public Communications Networks Voting systems that transmit data over public telecommunications networks face security risks that are not present in other voting systems. This section describes standards applicable to voting systems that use public telecommunications networks.	***N/A***
7.6.1	Data Transmission All systems that transmit data over public telecommunications networks shall:	***N/A***
7.6.1.a	Preserve the secrecy of voter ballot selections and prevent anyone from violating ballot privacy	***N/A***
7.6.1.b	Employ digital signatures for all communications between the vote server and other devices that communicate with the server over the network	***N/A***
7.6.1.c	Require that at least two authorized election officials activate any critical operation regarding the processing of ballots transmitted over a public communications network, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of votes	***N/A***
7.6.2	Casting Individual Ballots Systems designed for transmission of telecommunications over public networks shall meet security standards that address the security risks attendant with the casting of ballots from polling places controlled by election officials using voting devices configured and installed by election officials and/or their vendor or contractor, and using in-person authentication of individual voters.	***N/A***
7.6.2.1	Documentation of Mandatory Security Activities Vendors of voting systems that cast individual ballots over a public telecommunications network shall provide detailed descriptions of:	***N/A***
7.6.2.1.a	All activities mandatory to ensuring effective voting system security to be performed in setting up the system for operation, including testing of security before an election	***N/A***
7.6.2.1.b	All activities that should be prohibited during voting equipment setup and during the timeframe for voting operations, including both the hours when polls are open and when polls are closed	***N/A***
7.6.2.2	Ability to Operate During Interruption of Service These systems shall provide the following capabilities to provide resistance to interruptions of telecommunications service that prevent voting devices at the polling place from communicating with external components via telecommunications:	***N/A***

Requirement	Requirement Text	Conform
7.6.2.2.a	Detect the occurrence of a telecommunications interruption at the polling place and switch to an alternative mode of operation that is not dependent on the connection between polling place voting devices and external system components	***N/A***
7.6.2.2.b	Provide an alternate mode of operation that includes the functionality of a conventional electronic voting system without losing any single vote	***N/A***
7.6.2.2.c	Create and preserve an audit trail of every vote cast during the period of interrupted communication and system operation in conventional electronic voting system mode	***N/A***
7.6.2.2.d	Upon reestablishment of communications, transmit and process votes accumulated while operating in conventional electronic voting system mode with all security safeguards in effect	***N/A***
7.6.2.2.e	Ensure that all safeguards related to voter identification and authentication are not affected by the procedures employed by the system to counteract potential interruptions of telecommunications capabilities	***N/A***
7.7	Wireless Communications This section provides requirements for implementing and using wireless communications within a voting system. These requirements reduce, but do not eliminate, the risk of using wireless communications for voting systems. (See VVSG Vol. 1 Section 7 for further information pertaining to Wireless)	***N/A***
7.7.2	Identifying Usage Since there are a wide variety of wireless technologies (both standard and proprietary) and differing physical properties of wireless signals, it is important to identify some of the characteristics of the wireless technologies used in the voting system.	***N/A***
7.7.2.a	If a voting system provides wireless communications capabilities, then there shall be a method for determining the existence of the wireless communications capabilities.	***N/A***
7.7.2.b	If a voting system provides wireless communications capabilities, then there shall be an indication that allows one to determine when the wireless communications (such as radio frequencies) capability is active.	***N/A***
7.7.2.c	The indication shall be visual.	***N/A***
7.7.2.d	If a voting system provides wireless communications capabilities, then the type of wireless communications used (such as radio frequencies) shall be identified either via a label or via the voting system documentation.	***N/A***
7.7.3	Protecting Transmitted Data The transmitted data, especially via wireless communications, needs to be protected to ensure confidentiality and integrity. Examples of election information that needs to be protected include: ballot definitions, voting device counts, precinct counts, opening of poll signal, and closing of poll signal. Examples of other information that needs to be protected include: protocol messages, address or device identification information, and passwords. Since radio frequency wireless signals radiate in all directions and pass through most construction material, anyone may easily receive the wireless signals. In contrast, infrared signals are line of sight and do not pass through most construction material. However, infrared signals can still be received by other devices that are in the line of sight. Similarly, wireless signals can be transmitted by others to create unwanted signals. Thus, encryption is required to protect the privacy and confidentiality of the voting information.	***N/A***
7.7.3.a	All information transmitted via wireless communications shall be encrypted and authenticated--with the exception of wireless T-coil coupling--to protect against eavesdropping and data manipulation including modification, insertion, and deletion.	***N/A***
7.7.3.a.i	The encryption shall be as defined in Federal Information Processing Standards (FIPS) 197, “Advanced Encryption Standard (AES).”	***N/A***
7.7.3.a.ii	The cryptographic modules used shall comply with FIPS 140-2, Security Requirements for Cryptographic Modules.	***N/A***
7.7.3.b	The capability to transmit non-encrypted and non-authenticated information via wireless communications shall not exist.	***N/A***

Requirement	Requirement Text	Conform
7.7.3.c	If audible wireless communication is used, and the receiver of the wireless transmission is the human ear, then the information shall not be encrypted. Discussion: This specifically covers wireless T-Coil coupling for assistive devices used by people who are hard of hearing.	***N/A***
7.7.4	Protecting the Wireless Path If wireless communications are used, then the following capabilities shall exist in order to mitigate the effects of a denial of service (DoS) attack:	***N/A***
7.7.4.a	The voting system shall be able to function properly throughout a DoS attack, since the DoS attack may continue throughout the voting period.	***N/A***
7.7.4.b	The voting system shall function properly as if the wireless capability were never available for use.	***N/A***
7.7.4.c	Alternative procedures or capabilities shall exist to accomplish the same functions that the wireless communications capability would have done.	***N/A***
7.7.4.d	If infrared is being used, the shielding shall be strong enough to prevent escape of the voting system signal, as well as strong enough to prevent infrared saturation jamming. Discussion: Since infrared has the line-of-sight property, securing the wireless path can be accomplished by shielding the path between the communicating devices with an opaque enclosure. However, this is only practical for short distances. This shielding would also help prevent accidental eye damage from the infrared signal.	***N/A***
7.7.5	Protecting the Voting System Physical security measures to prevent access to a voting system are not possible when using a wireless communications interface because there is no discrete physical communications path that can be secured.	***N/A***
7.7.5.a	The security requirements in Subsection 2.1.1 shall be applicable to systems with wireless communications.	***N/A***
7.7.5.b	The accuracy requirements in Subsection 2.1.2 shall be applicable to systems with wireless communications.	***N/A***
7.7.5.c	The use of wireless communications that may cause impact to the system accuracy through electromagnetic stresses is prohibited.	***N/A***
7.7.5.d	The error recovery requirements in Subsection 2.1.3 shall be applicable to systems with wireless communications.	***N/A***
7.7.5.e	All wireless communications actions shall be logged.	***N/A***
7.7.5.e.i	The log shall contain at least the following entries: times when the wireless is activated and deactivated, services accessed, identification of device to which data was transmitted to or received from, identification of authorized user, and successful and unsuccessful attempts to access wireless communications or service. Discussion: Other information such as the number of frames or packets transmitted or received at various logical layers may be useful, but is dependent on the wireless technology used.	***N/A***
7.7.5.f	Device authentication shall occur before any access to, or services from, the voting system are granted through wireless communications. Discussion: Authentication is an important element to protect the security of wireless communications. Authentication verifies the identity and legitimacy of users, devices, and services.	***N/A***
7.7.5.f.i	User authentication shall be at least level 2 as per NIST Special Publication 800-63 Version 1.0.1, Electronic Authentication Guideline.	***N/A***
7.8	Independent Verification Systems	
7.8.1	Overview Independent verification (IV) systems are electronic voting systems that produce multiple independent cast vote records of voter ballot selections, which can be audited to a high level of precision. For this to happen, the cast vote records must be handled according to the following protocol: At least two cast vote records of the voter's selections are produced and one of the records is then stored in a manner that it cannot be modified by the voting system. For example	

Requirement	*Requirement Text*	*Conform*
7.8.2	Basic Characteristics of IV Systems This section describes a preliminary set of basic characteristics that apply to all types of IV systems. This information is provided for the purpose of introducing these concepts for consideration in voting system design. It is anticipated that future voting systems will be required to provide some type of independent verification feature to enable voters to have confidence that their ballot selections are correctly recorded and counted.	
7.9	Voter Verifiable Paper Audit Trail Requirements This section contains requirements for DREs with a Voter Verifiable Paper Audit Trail (VVPAT) component. VVPAT capability is not required for national certification. However, these requirements will be applied for certification testing of DRE systems that are intended for use in states that require DREs to provide this capability. The vendor's certification testing application to the EAC must indicate whether the system being presented for testing includes this capability, as provided under Subsection 1.6.2.5 extensions.	
7.9.1	Display and Print a Paper Record	
7.9.1.a	The voting system shall print and display a paper record of the voter ballot selections prior to the voter making his or her selections final by casting the ballot. Discussion: This is the basic requirement for VVPAT capability. It requires the paper record to be created as a distinct representation of the voter ballot selections. It requires the paper record to contain the same information as the electronic record and be suitable for use in verifications of the voting machine's electronic records.	***N/A***
7.9.1.b	The paper record shall constitute a complete record of ballot selections that can be used to assess the accuracy of the voting machine's electronic record, to verify the election results, and, if required by state law, in full recounts. Discussion: This requirement exists to make clear that it is possible to use the paper record for checks of the voting machine's accuracy in recording voter ballot selections, as well as usable for election audits (such as mandatory 1% recounts). The paper record shall also be suitable for use in full recounts of the election if required by state law.	***N/A***
7.9.1.c	The paper record shall contain all voter selection information stored in the electronic (ballot image) record. Discussion: The electronic ballot image record cannot hide any information related to ballot selections; all information relating to voter selections must be equally present in both records. The electronic record may contain other items that don't necessarily need to be on the paper record, such as digital signature information.	***N/A***
7.9.2	Approve or Void the Paper Record	
7.9.2.a	The voting equipment shall allow the voter to approve or void the paper record. Discussion: There are three possible scenarios regarding the voter's disposition of the paper record. The voter can verify that the ballot selections displayed on the DRE summary screen and those printed on the paper record are the same. If they are	***N/A***
7.9.2.b	The voting equipment shall, in the presence of the voter, mark the paper record as being approved by the voter if the ballot selections are accepted; or voided or if the voter decides to change one or more selections.	***N/A***
7.9.2.c	If the records do not match, the voting equipment shall mark and preserve the paper record and shall provide a means to preserve the corresponding electronic record so the source of error or malfunction can be analyzed. Discussion: The voting machine shall be withdrawn from service immediately and its use discontinued in accordance with jurisdiction procedures.	***N/A***
7.9.2.d	The voting machine shall not record the electronic record until the paper record has been approved by the voter.	***N/A***
7.9.2.e	Vendor documentation shall include procedures to enable the election official to return a voting machine to correct operation after a voter has used it incompletely or incorrectly. This procedure shall not cause discrepancies between the tallies of the electronic and paper records.	***N/A***
7.9.3	Electronic and Paper Record Structure	

Requirement	Requirement Text	Conform
7.9.3.a	All cryptographic software in the voting system shall be approved by the U.S. Government's Cryptographic Module Validation Program, as applicable. Discussion: Cryptographic software may be used for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program (CMVP). There may be cryptographic voting schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP approved software should be used where feasible but is not required. The CMVP website is http://csrc.nist.gov/cryptval.	***YES***
7.9.3.b	The electronic ballot image and paper records shall include information about the election.	***N/A***
7.9.3.b.i	The voting equipment shall be able to include an identification of the particular election, the voting site and precinct, and the voting machine. Discussion: If the voting site and precinct are different, both should be included.	***N/A***
7.9.3.b.ii	The records shall include information identifying whether the balloting is provisional, early, or on election day, and information that identifies the ballot style in use.	***N/A***
7.9.3.b.iii	The records shall include a voting session identifier that is generated when the voting equipment is placed in voting mode, and that can be used to identify the records as being created during that voting session. Discussion: If there are several voting sessions on the same voting machine on the same day, the voting session identifiers must be different. They should be generated from a random number generator.	***N/A***
7.9.3.c	The electronic ballot image and paper records shall be linked by including a unique identifier within each record that can be used to identify each record uniquely and each record's corresponding record. Discussion: The identifier serves the purpose of uniquely identifying and linking the records for cross-checking.	***N/A***
7.9.3.d	The voting machine should generate and store a digital signature for each electronic record.	***N/A***
7.9.3.e	The electronic ballot image records shall be able to be exported for auditing or analysis on standards-based and /or COTS information technology computing platforms.	***N/A***
7.9.3.e.i	The exported electronic ballot image records shall be in a publicly available, non-proprietary format. Discussion: It is advantageous when all electronic records, regardless of manufacturer, use the same format or can easily be converted to a publicly available, non-proprietary format; for example, the OASIS Election Markup Language (EML) Standard.	***N/A***
7.9.3.e.ii	The records should be exported with a digital signature, which shall be calculated on the entire set of electronic records and their associated digital signatures. Discussion: This is necessary to determine if records are missing or substituted.	***N/A***
7.9.3.e.iii	The voting system vendor shall provide documentation as to the structure of the exported ballot image records and how they shall be read and processed by software.	***N/A***
7.9.3.e.iv	The voting system vendor shall provide a software program that will display the exported ballot image records and that may include other capabilities such as providing vote tallies and indications of undervotes.	***N/A***
7.9.3.vi	The voting system vendor shall provide full documentation of procedures for exporting electronic ballot image records and reconciling those records with the paper audit records.	***N/A***
7.9.3.f	The paper record should be created in a format that may be made available across different manufacturers of electronic voting systems. Discussion: There may be a future requirement for some commonality in the format of paper records.	***N/A***
7.9.3.g	The paper record shall be created such that its contents are machine readable. Discussion: This can be done by using specific OCR fonts or barcodes.	***N/A***

Requirement	Requirement Text	Conform
7.9.3.g.i	The paper record shall contain error correcting codes for the purpose of detecting read errors and for preventing other markings on the paper record from being misinterpreted when machine reading the paper record. Discussion: This requirement is not mandatory if a state prohibits the paper record from containing any information that cannot be read and understood by the voter. This requirement serves the purpose of detecting scanning errors and preventing stray or deliberate markings on the paper from being interpreted as valid data.	***N/A***
7.9.3.h	If barcode is used, the voting equipment shall be able to print a barcode with each paper record that contains the human-readable contents of the paper record. Discussion: This requirement is not mandatory if a state prohibits the paper record from containing any information that cannot be read and understood by the voter.	***N/A***
7.9.3.h.i	The barcode shall use an industry standard format and shall be able to be read using readily available commercial technology. Discussion: Examples of such codes are Maxi Code or PDF417.	***N/A***
7.9.3.h.ii	If the corresponding electronic record contains a digital signature, the digital signature shall be included in the barcode on the paper record.	***N/A***
7.9.3.h.iii	The barcode shall not contain any information other than the paper record's human-readable content, error correcting codes, and digital signature information.	***N/A***
7.9.4	Equipment Security and Reliability	
7.9.4.a	The voting machine shall provide a standard, publicly documented printer port (or the equivalent) using a standard communication protocol. Discussion: Using a standard, publicly documented printer protocol assists in security evaluations of system software.	***N/A***
7.9.4.b	Tamper-evident seals or physical security measures shall protect the connection between the printer and the voting machine.	***N/A***
7.9.4.c	If the connection between the voting machine and the printer has been broken, the voting machine shall detect this event and record it in the DRE internal audit log.	***N/A***
7.9.4.d	The paper path between the printing, viewing and storage of the paper record shall be protected and sealed from access except by authorized election officials.	***N/A***
7.9.4.e	The printer shall not be permitted to communicate with any system or machine other than the voting machine to which it is connected.	***N/A***
7.9.4.f	The printer shall only be able to function as a printer; it shall not contain any other services (e.g., provide copier or fax functions) or network capability.	***N/A***
7.9.4.g	The voting machine shall detect errors and malfunctions such as paper jams or low supplies of consumables such as paper and ink that may prevent paper records from being correctly displayed, printed or stored. Discussion: This could be accomplished in a variety of different ways; for example, a printer that is out of paper or jammed could issue audible alarms, with the alarm different for each condition.	***N/A***
7.9.4.h	If an error or malfunction occurs, the voting machine shall suspend voting operations and should present a clear indication to the voter and election officials of the malfunction.	***N/A***
7.9.4.i	The voting machine shall not record votes if an error or malfunction occurs.	***N/A***
7.9.4.j	Printing devices should contain sufficient supplies of paper and ink to avoid reloading or opening equipment covers or enclosures and thus potential circumvention of security features; or be able to reload paper and ink with minimal disruption to voting and without circumvention of security features such as seals.	***N/A***
7.9.4.k	Vendor documentation shall include procedures for investigating and resolving printer malfunctions including, but not limited to; printer operations, misreporting of votes, unreadable paper records, and power failures.	***N/A***
7.9.4.l	Vendor documentation shall include printer reliability specifications including Mean Time Between Failure estimates, and shall include recommendations for appropriate quantities of backup printers and supplies.	***N/A***

Requirement	Requirement Text	Conform
7.9.4.m	Protective coverings intended to be transparent on voting equipment shall be maintainable via a predefined cleaning process. If the coverings become damaged such that they obscure the paper record, they shall be replaceable.	***N/A***
7.9.4.n	The paper record shall be sturdy, clean, and of sufficient durability to be used for verifications, reconciliations, and recounts conducted manually or by automated processing.	***N/A***
7.9.5	Preserving Voter Privacy VVPAT records can be printed and stored by two different methods: Printed and stored on a continuous spool-to-spool paper roll where the voter views the paper record in a window " Printed on separate pieces of paper	
7.9.5.a	Voter privacy shall be preserved during the process of recording, verifying and auditing his or her ballot selections. Discussion: The privacy requirements from Section 3 also apply to voting equipment with VVPAT.	***N/A***
7.9.5.b	When a VVPAT with a spool-to-spool continuous paper record is used, a means shall be provided to preserve the secrecy of the paper record of voter selections.	***N/A***
7.9.5.c	When a VVPAT with a spool-to-spool continuous paper record is used, no record shall be maintained of which voters used which voting machine or the order in which they voted.	***N/A***
7.9.5.d	The electronic and paper records shall be created and stored in ways that preserve the privacy of the voter. Discussion: For VVPAT systems that use separate pieces of paper for the record, this can be accomplished in various ways including shuffling the order of the records or other methods to separate the order of stored records.	***N/A***
7.9.5.e	The privacy of voters whose paper records contain an alternative language shall be maintained.	***N/A***
7.9.5.f	Unique identifiers shall not be displayed in a way that is easily memorable by the voter. Discussion: Unique identifiers on the paper record are displayed or formatted in such a way that they are not memorable to voters, such as by obscuring them in other characters.	***N/A***
7.9.5.g	Both paper rolls and paper record secure receptacles shall be controlled, protected, and preserved with the same security as a ballot box.	***N/A***
7.9.6	VVPAT Usability	
7.9.6.a	All usability requirements from Subsection 3.1 shall apply to voting machines with VVPAT. Discussion: The requirements in this section are in addition to those in Subsection 3.1.	***N/A***
7.9.6.b	The voting equipment shall be capable of showing the information on the paper in a font size of at least 3.0 mm and should be capable of showing the information in at least two font ranges; 3.0-4.0 mm, and 6.3-9.0 mm, under control of the voter or poll worker. Discussion: In keeping with requirements in Subsection 3.1, the paper record should use the same font sizes as displayed by the voting machine, but at least be capable of 3.0 mm. While larger font sizes may assist voters with poor vision, certain disabilities such as tunnel vision are best addressed by smaller font sizes.	***N/A***
7.9.6.c	The voting equipment shall display, print and store the paper record in any of the written alternative languages chosen for the ballot.	***N/A***
7.9.6.c.i	To assist with manual auditing, candidate names on the paper record shall be presented in the same language as used on the DRE summary screen.	***N/A***
7.9.6.c.ii	Information on the paper record not needed by the voter to perform verification shall be in English. Discussion: In addition to the voter ballot selections, the marking of the paper record as accepted or void, and the indication of the ballot page number need to be printed in the alternative language. Other information, such as precinct and election identifiers, shall be in English to facilitate use of the paper record for auditing.	***N/A***
7.9.6.d	The paper and electronic records shall be presented to allow the voter to read and compare the records without the voter having to shift his or her position.	***N/A***

Requirement	*Requirement Text*	*Conform*
7.9.6.e	If the paper record cannot be displayed in its entirety on a single page, a means shall be provided to allow the voter to view the entire record. Discussion: Possible solutions include scrolling the paper or printing a new sheet of paper. The voter should be notified if it is not possible to scroll in reverse, so they will know to complete verification in one pass.	***N/A***
7.9.6.f	If the paper record cannot be displayed in its entirety on a single page, each page of the record shall be numbered and shall include the total count of pages for the record. Discussion: Possible numbering schemes include "Page X of Y."	***N/A***
7.9.6.g	The instructions for performing the verification process shall be made available to the voter in a location on the voting machine. Discussion: All instructions must meet the usability requirements contained in Subsection 3.1.	***N/A***
7.9.7	VVPAT Accessibility	
7.9.7.a	All accessibility requirements from Subsection 3.2 shall apply to voting machines with VVPAT.	***N/A***
7.9.7.b	If the normal voting procedure includes VVPAT, the accessible voting equipment should provide features that enable voters who are visually impaired and voters with an unwritten language to perform this verification. If state statute designates the paper record produced by the VVPAT to be the official ballot or the determinative record on a recount, the accessible voting equipment shall provide features that enable visually impaired voters and voters with an unwritten language to review the paper record. Discussion: For example, the accessible voting equipment might provide an automated reader that converts the paper record contents into audio output.	***N/A***
8	Quality Assurance Requirements	
8.2	General Requirements The voting system vendor is responsible for designing and implementing a quality assurance program to ensure that the design, workmanship, and performance requirements are achieved in all delivered systems and components. At a minimum, this program shall:	
8.2.a	Include procedures for specifying, procuring, inspecting, accepting, and controlling parts and raw materials of the requisite quality	***YES***
8.2.b	Require the documentation of the hardware and software development process	***YES***
8.2.c.i	Identify and enforce all requirements for: In-process inspection and testing that the manufacturer deems necessary to ensure proper fabrication and assembly of hardware	***YES***
8.2.c.ii	Identify and enforce all requirements for: Installation and operation of software and firmware	***YES***
8.2.d	Include plans and procedures for post-production environmental screening and acceptance testing	***YES***
8.2.e	Include a procedure for maintaining all data and records required to document and verify the quality inspections and tests	***YES***
8.3	Components from Third Parties	
8.3	A vendor who does not manufacture all the components of its voting system, but instead procures components as standard commercial items for assembly and integration into a voting system, shall verify that the supplier vendors follow documented quality assurance procedures that are at least as stringent as those used internally by the voting system vendor.	***YES***
8.4	Responsibility for Tests	
8.4	The manufacturer or vendor shall be responsible for performing all quality assurance tests, acquiring and documenting test data, and providing test reports for examination by the test lab as part of the national certification process. These reports shall also be provided to the purchaser upon request.	***YES***
8.5	Parts & Materials Special Tests and Examinations In order to ensure that voting system parts and materials function properly, vendors shall:	
8.5.a	Select parts and materials to be used in voting systems and components according to their suitability for the intended application. Suitability may be determined by similarity of this application to existing standard practice or by means of special tests	***YES***

Requirement	Requirement Text	Conform
8.5.b	Design special tests, if needed, to evaluate the part or material under conditions accurately simulating the actual voting system operating environment	YES
8.5.c	Maintain the resulting test data as part of the quality assurance program documentation	YES
8.6	Quality Conformance Inspections The vendor performs conformance inspections to ensure the overall quality of the voting system and components delivered to the test lab for national certification testing and to the jurisdiction for implementation. To meet the conformance inspection requirements the vendor or manufacturer shall:	
8.6.a	Inspect and test each voting system or component to verify that it meets all inspection and test requirements for the system	YES
8.6.b	Deliver a record of tests or a certificate of satisfactory completion with each system or component	YES
8.7	Documentation Vendors are required to produce documentation to support the independent testing required for their products to be granted national certification. Volume II, Section 2, Description of the Technical Data Package, identifies the documentation required for the national certification testing process. This documentation shall be sufficient to serve the needs of the test lab, election officials, and maintenance technicians. It shall be prepared and published in accordance with standard commercial practice for information technology and electronic and mechanical equipment. It shall include, at a minimum, the following: • System overview • System functionality description • System hardware specification • Software design and specifications • System security specification • System test and verification specification • System operations procedures • System maintenance procedures • Personnel deployment and training requirements • Configuration management plan • Quality assurance program • System change notes	YES
9	Configuration Management This section contains specific requirements for configuration management of voting systems. For the purpose of the Guidelines, configuration management is defined as a set of activities and associated practices that ensures full knowledge and control of the components of a system, starting with its initial development and progressing through its ongoing maintenance and enhancement. This section describes activities in terms of their purposes and outcomes. It does not describe specific procedures or steps to be employed to accomplish them. Specific steps and procedures are left to the vendor to select.	
9.1.1	Configuration Management Requirements	
9.1.1	Configuration management addresses a broad set of record keeping, auditing, and reporting activities that contribute to full knowledge and control of a system and its components. These activities include: Identifying discrete system components " Creating records of a formal baseline and later versions of components " Controlling changes made to the system and its components " Releasing new versions of the system " Auditing the system	
9.1.2	Organization of Configuration Management Requirements	

Requirement	Requirement Text	Conform
9.1.2	The requirements for configuration management include: • Application of configuration management requirements • Configuration management policy • Configuration identification • Baseline, promotion, and demotion procedures • Configuration control procedures • Release process • Configuration audits • Configuration management resources	
9.1.3	Application of Configuration Management Requirements	
9.1.3	Requirements for configuration management apply to all components of voting systems regardless of the specific technologies employed. These components include: Software " Hardware " Communications " Documentation " Identification and naming conventions (including changes to these conventions) for software programs and data files " Development and testing artifacts such as test data and scripts " File archiving and data repositories "	
9.2	Configuration Management Policy	
9.2	The vendor shall describe its policies for configuration management in the Technical Data Package. This description shall address the following elements: Scope and nature of configuration management program activities " Breadth of application of the vendor's policies and practices to the voting system	***YES***
9.3	Configuration Identification Configuration identification is the process of identifying, naming, and acquiring configuration items. Configuration identification encompasses all system components.	
9.3.1	Classification and Naming Configuration Items	
9.3.1	The vendor shall describe the procedures and conventions used to classify configuration items into categories and subcategories, uniquely number or otherwise identify configuration items and name configuration items.	***YES***
9.3.2	Versioning Conventions When a system component is part of a higher level system element such as a subsystem, the vendor shall describe the conventions used to:	
9.3.2.a	Identify the specific versions of individual configuration items and sets of items that are incorporated in higher level system elements such as subsystems	***YES***
9.3.2.b	Uniquely number or otherwise identify versions	***YES***
9.3.2.c	Name versions	***YES***
9.4	Baseline and Promotion Procedures The vendor shall establish formal procedures and conventions for establishing and providing a complete description of the procedures and related conventions used to:	
9.4.a	Establish a particular instance of a component as the starting baseline	***YES***
9.4.b	Promote subsequent instances of a component to baseline status as development progresses through to completion of the initial completed version released to the accredited test lab for testing	***YES***
9.4.c	Promote subsequent instances of a component to baseline status as the component is maintained throughout its life cycle until system retirement (i.e., the system is no longer sold or maintained by the vendor)	***YES***
9.5	Configuration Control Procedures Configuration control is the process of approving and implementing changes to a configuration item to prevent unauthorized additions, changes or deletions. The vendor shall establish such procedures and related conventions, providing a complete description of those procedures used to:	
9.5.a	Develop and maintain internally developed items	***YES***
9.5.b	Acquire and maintain third-party items	***YES***
9.5.c	Resolve internally identified defects for items regardless of their origin	***YES***

Requirement	Requirement Text	Conform
9.5.d	Resolve externally identified and reported defects (i.e., by customers and accredited test labs)	YES
9.6	Release Process The release process is the means by which the vendor installs, transfers or migrates the system to the accredited test lab and, eventually, to its customers. The vendor shall establish such procedures and related conventions, providing a complete description of those used to:	
9.6.a	Perform a first release of the system to an accredited test lab	YES
9.6.b	Perform a subsequent maintenance or upgrade release of the system or particular components, to an accredited test lab	YES
9.6.c	Perform the initial delivery and installation of the system to a customer, including confirmation that the installed version of the system matches exactly the certified system version	YES
9.6.d	Perform a subsequent maintenance or upgrade release of the system or a particular component to a customer, including confirmation that the installed version of the system matches exactly the certified system version	YES
9.7	Configuration Audits	
9.7.1	Physical Configuration Audit The Physical Configuration Audit is conducted by the accredited test lab to compare the voting system components submitted for certification to the vendor's technical documentation. For the PCA, a vendor shall provide:	
9.7.1.a	Identification of all items that are to be a part of the software release	YES
9.7.1.b	Specification of compiler (or choice of compilers) to be used to generate executable programs	YES
9.7.1.c	Identification of all hardware that interfaces with the software	YES
9.7.1.d	Configuration baseline data for all hardware that is unique to the system	YES
9.7.1.e	Copies of all software documentation intended for distribution to users, including program listings, specifications, operations manual, voter manual, and maintenance manual	YES
9.7.1.f	User acceptance test procedures and acceptance criteria	YES
9.7.1.g	Identification of any changes between the physical configuration of the system submitted for the PCA and that submitted for the FCA, with a certification that any differences do not degrade the functional characteristics	YES
9.7.1.h.i	Complete descriptions of its procedures and related conventions used to support this audit by: Establishing a configuration baseline of the software and hardware to be tested	YES
9.7.1.h.ii	Complete descriptions of its procedures and related conventions used to support this audit by: Confirming whether the system documentation matches the corresponding system components	YES
9.7.2	Functional Configuration Audit The Functional Configuration Audit is conducted by the accredited test lab to verify that the system performs all the functions described in the system documentation. The vendor shall:	
9.7.2.a	Completely describe its procedures and related conventions used to support this audit for all system components	YES
9.7.2.b.i	Provide the following information to support this audit: Copies of all procedures used for module or unit testing, integration testing, and system testing	YES
9.7.2.b.ii	Provide the following information to support this audit: Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests	YES
9.7.2.b.iii	Provide the following information to support this audit: Records of all tests performed by the procedures listed above, including error corrections and retests	YES

Requirement	*Requirement Text*	*Conform*
9.8	Configuration Management Resources Often, configuration management activities are performed with the aid of automated tools. Assuring that such tools are available throughout the system life cycle, including if the vendor is acquired by or merged with another organization, is critical to effective configuration management. Vendors may choose the specific tools they use to perform the record keeping, audit, and reporting activities of the configuration management standards. The resources documentation standard provided below focus on assuring that procedures are in place to record information about the tools to help ensure that they, and the data they contain, can be transferred effectively and promptly to a third party should the need arise. Within this context, a vendor is required to develop and provide a complete description of the procedures and related practices for maintaining information about:	
9.8.a	Specific tools used, current version, and operating environment;	***YES***
9.8.b	Physical location of the tools, including designation of computer directories and files;	***YES***
9.8.c	Procedures and training materials for using the tools.	***YES***