★ VIRGINIA ★
DEPARTMENT of ELECTIONS

Voting System Certification Standard

January 2026
Version 3.1

Change History

Version	Brief Description of Change	Date	Author
1.0	Adoption by the State Board of Elections Primary changes were to improve clarity, security-related requirements, and document format; moving information that would likely change over time to appendices	09/17/2019	ELECT
2.0	Adoption by the State Board of Elections Primary changes were in alignment with feedback and addition of Appendices I & J	11/18/2019	ELECT
2.1	Adoption by the State Board of Elections Primary changes were the amount to be deposited by vendor for costs of travel, expenses and billable hours by the VSTL for the certification process and specifics regarding the location and timeline of the certification	03/07/2023	ELECT
2.2	Adoption by the State Board of Elections Primary changes were updates to Code references and language pertaining to those updates to account for amendments and additions to the Code. Updates to the submission of the Technical Data Package to change from paper to digital.	03/04/2025	ELECT
3.0	Adoption by State Board of Elections The primary change was the incorporation of EAC VVSG 2.0 standards. Updates included, increase in vendor fee, increase in certification testing criteria and clarification of methodologies used, addition of multi-factor authentication, stronger security functionality, Role Based Access Control,	09/17/2025	ELECT

	enhancements to ADA compliance requirements. Additional requirements to continue cessation of wireless communications and updates to the submission of the Technical Data Package.		
3.1	Adoption by State Board of Elections Fees for cost of travel, expenses, and billable hours of the VSTL for the certification process have been increased based upon current rates.	1/28/2026	ELECT

Chapter 1: Introduction

1.1. Purpose of Standard

This Standard has been developed and issued as part of a continuing effort to improve the administration of elections in the Commonwealth of Virginia. It provides a formal and organized process for vendors to follow when seeking state certification for a new voting system or for improvements or modifications to a previously certified voting system in Virginia. To this end the Standard is designed to:

1. Ensure conformity with Virginia election laws relating to the acquisition and use of voting systems,
2. Evaluate and certify voting systems marketed by vendors for use in Virginia,
3. Evaluate and re-certify additional capabilities and changes in the method of operation for voting systems previously certified for use in Virginia,
4. Standardize decertification and recertification of voting systems,
5. Ensure that all voting systems operate properly and are installed and tested in compliance with State Board of Elections (SBE) procedures, and
6. Ensure accurate reports of all election results from jurisdictions that use each certified system.

1.2. Specific Requirements

1. Compliance with the requirements contained in the EAC Voluntary Voting System Guidelines (VVSG) 2.0. The voting system must comply with the provisions in the Code of Virginia relating to voting equipment (Article 3, Chapter 6 of Title 24.2).
2. The voting system must comply with any applicable regulations or policies issued by the SBE or ELECT.
3. The vendor must ensure that the voting system can accommodate an interactive visual and non-visual presentation of information to voters, and alternative languages when required. (See Help America Vote Act (HAVA) 52 USC §21081(a)(3), (4), §203 of the Voting Rights Act (52 USC §10503) and Virginia Code §24.2-626.1).

1.3. Decertification

ELECT reserves the right to reexamine any previously certified voting system for any reason at any time. Any voting system that does not pass reexamination will be decertified. A voting system that has been decertified by the SBE cannot be used for elections held in the Commonwealth of Virginia and cannot be purchased by localities to conduct elections.

In addition, the SBE reserves the right to decertify the voting systems if the vendor does not comply with the following requirements:

1. Notify ELECT of any incident, anomaly, or security-related breach experienced in an election jurisdiction, within 24 hours of vendor knowledge (See Appendix L).
2. Report to ELECT annually and within 30 calendar days of vendor knowledge, any changes to Corporate Information including:
    a. Business entity and structure,
    b. Parent and subsidiary companies,
    c. Capital or equity structure,
    d. Control; identity of any individual, entity, partnership, or organization owning a controlling interest,
    e. Investment by any individual, entity, partnership, or organization in an amount that exceeds 5% of the vendor's net cash flow from the prior reporting year,
    f. Location of manufacturing facilities; including names of the third-party vendor(s) employed to either fabricate, assemble or both, any component part of the voting, tabulating, or both, systems being submitted for certification, along with the location of all their facilities with manufacturing capability,
    g. Third-party vendors,
    h. Good Standing status, and
    i. Credit rating.
3. Submit any modifications to a previously certified voting system to ELECT for review within 30 calendar days from modification; see Appendix H for appropriate reporting process.
4. If the operating system or any component either has reached or will reach the Last Date of Mainstream Support within 18 months, as defined in Appendix H, send an upgrade plan with target date(s) to ELECT:
    a. ELECT must receive the upgrade plan at least 12 months before the Last Date of Mainstream Support.
    b. The Last Date of Mainstream Support cannot include any type of Extended Support, as defined in Appendix H.
    c. The voting system may still automatically be decertified as defined in Appendix H.
5. Update all software with the latest patching and vulnerability updates in alignment with Appendix E.

NOTE: The SBE reserves the right to require recertification when new VVSG guidelines or changes to either regulations, standards, or both occur.

1.4. Recertification

See Appendix F for ELECT's guidelines on when voting system must go through recertification.

Chapter 2: Basis for Certification

Pursuant to Va. Code §24.2-629 of the Code of Virginia, voting systems must comply with applicable state and federal requirements. The definition of "voting system" is the total combination of mechanical, electromechanical, and electronic equipment, including the software, firmware, and documentation required to program, control, and support the equipment, that is used to define ballots, cast and count votes, report or display election results, recount votes and maintain and produce any audit trail information.[1]

Federal Compliance Testing demonstrates that the voting system adheres to all requirements set forth in the VVSG by the EAC. Evidence of compliance is the certification of the system by the EAC. See HAVA, 52 USC §21081. Commonwealth certification adheres to the federal EAC VVSG 2.0 standards. State certification testing will evaluate that the voting system complies with all applicable requirements of the Code of Virginia and SBE and ELECT regulations and policies.

2.1. Federal Compliance Testing

EAC certification serves as evidence of compliance. All vendors must have their equipment hardware and software proposed for Commonwealth certification certified directly by EAC. This is proven by presenting the EAC certificate of certification with the system and version the vendor is requesting to be certified by the Commonwealth. ELECT will make the final decision on compliance based on all available information. If there is evidence of a material non-compliance, ELECT will work with the vendor to resolve the issue.

The Commonwealth uses a specific request to certify process. This process includes submitting to ELECT a Microsoft Excel submission file (template provided by ELECT) and completed by the vendor. The submission file lists all required documents a vendor must submit with a request to certify. The submission file also provides a naming convention, document formatting requirements, and contents to be contained in each document. If the documents received do not follow the requirements in the submission file, the request will

[1] This standard does not address ballot on demand systems. For more information please see Virginia Ballot on Demand Systems Certification Standards, August 2022.

be sent back to the vendor for correction. The following documents shall be provided to ELECT:

1. A full copy of the Technical Data Package (TDP) submitted for EAC Federal compliance testing.
2. A copy of the Test Plan and Test Report used by the Voting System Test Laboratories (VSTL) in performing EAC certification testing or results of testing conducted by a federally certified VSTL to the applicable VVSG.
3. A release for provision to the VSTL allowing responses to requests for information from the Commonwealth of Virginia.
4. A release for provision to other states that decertified the system or prior versions of the system to respond to requests for information from the Commonwealth of Virginia.
5. Any additional information ELECT believes is necessary to determine compliance with the applicable VVSG or Commonwealth of Virginia Voting System Certification Standards.

2.1.1. Voting System Hardware, Firmware, Infrastructure or Component Elements

All equipment used in a voting system shall be examined to determine its suitability for election use according to the appropriate procedures contained in this document. Equipment to be tested shall be identical in form and function with production units. Engineering or development prototypes are not acceptable. See Appendix G for hardware guidelines.

Any modification to existing hardware, firmware, infrastructure, or other components will invalidate the prior certification by the SBE unless ELECT can review and provide an assurance to the SBE that the change does not affect the accuracy, reliability, security, usability, or accessibility of the system. See Appendix J for the De Minimis Change Guideline that is applicable for hardware.

2.1.2. Voting System Software Elements

Voting system software shall be examined and tested to ensure that it adheres to the performance standards specified in the 2.0 version of the VVSG by the EAC (See Section 2.1).

Any modification to existing software will invalidate the prior certification by the SBE, unless ELECT can review and provide an assurance to the SBE that the change does not affect the accuracy, reliability, security, usability, or accessibility of the system. See Appendix J for the De Minimis Change Guideline that is applicable for software.

2.2. State Certification Testing

State certification testing will evaluate the design and performance of a voting system seeking certification to ensure that it complies with all applicable requirements in the Code of Virginia and SBE and ELECT regulations and policies. ELECT will examine the essential system functions, operational procedures, user guides, documents, and reviews from product users. Hash testing will be conducted to confirm that the application software is identical to the certified versions of federal compliance testing.

ELECT will evaluate the user experience with the current and prior versions of the voting system and certification reports from other states. In addition, the security and reliability analysis of the product model will be reviewed to determine the usability of the voting system for Virginia Elections. Although, successful EAC VVSG 2.0 certification must be accomplished before a system will be reviewed for certification by Virginia. ELECT's certification test plan and test assertions will require a vendor to test, demonstrate, or replicate, as part of Virginia's certification process, some test assertions or requirements already completed through the EAC VVSG 2.0 certification.

State Certification Testing will examine all system operations and procedures, including but not limited to:

1. Define ballot formats for primary elections, general elections, and special elections including all voting options defined by the Code of Virginia.
2. Install applications and election-specific programs and data in the ballot counting device.
3. Count ballots.
4. Prepare to perform and conduct the Logic and Accuracy tests.
5. Obtain voting data and audit data reports.
6. Support recount or election audits.
7. Compliance with physical and language accessibility requirements.
8. Display an appropriate message on the review screen if a voter does not follow the ballot instruction; allow the voter to override the warning messages for overvote, undervote, blank ballot, or invalid Write-in to cast voter's ballot.
9. Create a Cast Vote Record (CVR) for each vote for all elections.
10. Integrate CVRs in a readable format.
11. Does not have a built-in function for wireless connections or communications.
12. Compliance with encryption requirement(s) as stated in Appendix D.
13. Compliance with password protection requirements as stated in Appendix D.
14. Hardening the voting system using the vendor's procedures and specifications.
15. Compliance with the requirements for Write-in image and format.

Chapter 3: Review and Approval Process

3.1. Summary of Process

The State certification is limited to final products that have been used in a full production environment and are available for immediate installation. The certification review process goes through six phases. At the end of each phase, ELECT evaluates the results to determine the certification status.

Six Phases of the Certification Review Process:

1. Certification Request from Vendor
2. Preliminary Review
3. Technical Data Package (TDP) to Voting System Test Laboratory (VSTL)
4. Certification Test Report from VSTL
5. On-Site Testing in Mock Election
6. Approval by the SBE.

3.2. Certification Review Process

Phase 1: Certification Request from Vendor

A vendor requests certification for a specific voting system, software, firmware, hardware, or for a modification to an existing certified voting system. This request should include the following information:

1. Voting System Certification Application Form, and certification request Excel submission file, signed by a company officer. (See Appendix I).
   NOTE: This should clearly identify the specific voting system to be evaluated for certification, specifically:
   a. Each voting system or version of a voting system requires a separate request for certification.
   b. Each component of the hardware, firmware, software, and other components must be identified by version number.
2. Copies of documents substantiating completion of federal compliance testing, including whether the proposed voting system has been certified under the latest version of the VVSG currently accepted for certification by the EAC or tested by a federally certified VSTL. (See Section 2.1).
3. Whether the proposed voting system has ever been denied certification or had certification withdrawn in any state or by the EAC.
4. Eight copies of a brief overview description of the voting system.

a. Typical marketing brochures are usually sufficient for the description.

5. A list of all states where the proposed voting system version is currently used.
6. A list of the general pricing for procurement of the proposed voting system.
7. The vendor will provide a check in the amount of $50,000.00 to cover the costs for the travel, expenses, and billable hours of the VSTL for the certification process. Refunds will be provided to the vendor if the VSTL invoices total less than the check amount and the refund amount is over $100.00. Testing takes place at ELECT, Washington Building, 1100 Bank Street, Richmond, VA 23219. The VSTL technician will travel to Richmond. Certification will exceed one week, beginning on Monday of the first week and ending on Wednesday of the following week, i.e. an 8-day testing period. The 8-day cycle is exclusive of the one-day mock election, which generally happens the day after completion of the VSTL certification testing. Voting system equipment for certification will be shipped to ELECT before certification begins and shipped back after it is complete.
   a. Checks in the amount of $50,000.00 must be received by ELECT before the certification can begin.
      i. Checks or money orders should be made payable to “Treasurer of Virginia” and mailed to: Voting Technology / ELECT, 1100 Bank Street, 1st Floor, Richmond, VA 23219.
   b. The complexity of EAC VVSG 2.0 necessitates additional requirements to be reviewed by Virginia. The certification testing time on site must increase to meet the new additional requirements. Under the new Virginia Voting System Certification Standard 3.0, testing times will be on average 7 to 8 days on site.
8. TDP must clearly identify all items as required in the certification request (Excel submission file):
   a. If the TDP is incomplete or the items in the package are not clearly identified, the entire package could be returned to the vendor.
   b. Upon the receipt of a completed and correctly submitted TDP from the vendor, the evaluation of the voting system will be scheduled.
9. Corporate Information must clearly identify all items:
   a. If the Corporate Information is incomplete or the items in the package are not clearly identified, the entire package could be returned to the vendor. The evaluation process will be scheduled after the corrected package is received.

NOTE: The certification request package containing the items above should be sent to the location indicated by ELECT.

Technical Data Package

1. The TDP must be fully digital, Optical Character Recognition (OCR) compliant, and contain the following items:
   a. *Change Log:* The TDP must contain a document that clearly defines the changes from the last voting system certified in Virginia to the system being submitted for certification.
   b. *Hardware Schematic Diagrams*: Schematic diagrams of all hardware.
   c. *Hardware Theory of Operations*: Documentation describing the theory of operation of hardware, not limited to power cords and backup battery.
   d. *Software System Design*: Documentation describing logical design of the software.
      i. The documentation should clearly indicate various modules of the software, such as:
      ii. The list of functions,
      iii. System flowchart,
      iv. The interrelationships among modules, and
      v. The list of data formats that the voting system can import and export.
      vi. Clearly specify the operating system and version with:
         1. The Last Date of Mainstream Support, as defined in Appendix H, and
         2. The latest operating system version, security patches available, SHA256 hash value, and modification
   e. *Software Deviations:* Include any exception(s) to the Security Content Automation Protocol (SCAP) checklist; document the reason why there is an exception and the mitigating controls and tools in place to secure the system.
   f. *Software Source Code:* A source code evaluation conducted in accordance with applicable Software Design and Coding Standards.
   g. *Definition of Marked Oval/Target*: Define the system thresholds used to declare a readable mark in an oval or target to be read by the scanner.
   h. *Independent Third-Party Application Penetration Analysis Report*: An accredited application penetration test conducted within the past 6 months that analyzed the system being presented for certification, for potential vulnerabilities according to current industry standards. Potential vulnerabilities may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. The test must involve active exploitation of security vulnerabilities of the voting system and whether the vulnerabilities can be mitigated through compensating controls. Pursuant to Virginia Code § 24.2-625.1, the Penetration Analysis Report is confidential and excluded from inspection and copying under the Virginia Freedom

of Information Act. If a penetration test has been conducted in another state within 6 months on the same version of the voting system, that may be submitted to fulfill this requirement.

i. *Customer Maintenance, Repair & Troubleshooting Manual*: Documentation normally supplied to the customer for use by the person(s) who will provide maintenance, repair, and troubleshooting of the system.

j. *Operations Manual:* Documentation normally supplied to the customer for use by the person(s) who will operate the system. At a minimum, the manual should include maximum volume and speed of the scanner, maximum capacity of container bin, ballot box, storage units, electronic storage device, and instructions for proper and safe operation of the system to prevent injury or damage to any individual or the hardware, including fire and electrical hazards.

k. *User Guide and Documents:* The vendor should provide the following:
    i. Quick reference guide with detailed instructions for a precinct election officer to set up, use, and shut down the voting system,
    ii. ADA compliant training material that:
        1. May be in written or video form, and
        2. Must be in a format suitable for use at a polling place as a simple “how-to” guide.
    iii. Clear model of voting system architecture with the following documentation:
        1. End-User Documentation,
        2. System-Level and Administrator-Level Documentation, and
        3. Developer Documentation.
    iv. Failsafe voting system data recovery procedures
        1. For example: Recovery procedures for retrieving duplicated (contingency recovery) information from a different location within the device (or another device if recovery is required prior to any ballots being voted on the device and if networked capability is allowed and certified) if access to the primary storage area is not possible for some unforeseen reason,
    v. A list of customers who are using or have previously used the voting system
        1. Include a description of all known incidents or anomalies involving the functioning of the voting system, including how those incidents or anomalies were resolved with customer and date noted, and
    vi. If the operating system or any component (hardware, software, or both) has reached or will reach the Last Date of Mainstream Support within 18 months, as defined in Appendix H, send an upgrade plan with target date(s) to ELECT; the

Last Date of Mainstream Support cannot include any type of Extended Support, as defined in Appendix H.

l. *Recommended Security Practices:* CIS Security Best Practices, not limited to:
   i. System Security Architecture,
   ii. System Event Logging,
   iii. System Security Specification,
   iv. Security Content Automation Protocol (SCAP),
   v. Cryptography,
   vi. Equipment and Data Security,
   vii. Network and Data Transmission Security ,
   viii. Access control,
   ix. Authentication procedure,
   x. Software, and
   xi. Physical Security.

m. *Standard Contract, Product Support, and Service Level Agreement (SLA):* Customer and Technical Support hours and contact information. SLA should specify the escalation timeline and procedures with contact information. Vendor's capacity to provide, not limited to:
   i. On-Site Support and Technical Support within SLA on:
      1. Election Day (defined as the start of the in-person absentee voting period up to and including Election Day), and
      2. Within 60 days before Election Day,
   ii. Resolution of outstanding issues, repair, maintenance, and service requests within 30 days.

n. *Maintenance Services, Pricing, and Financing Options*: A list of maintenance services with price. Terms for replacing a component or voting equipment. Available financing options for purchase or lease,

o. *Warranty:* The vendor will provide a list of warranty specifications to include the following:
   i. The period and extent of the warranty,
   ii. Repair or Replacement,
      1. The circumstances under which equipment is replaced rather than repaired,
      2. The method by which a user requests such replacement,
   iii. Warranty coverage and costs, and
   iv. Technical documentation of all hardware and software that is used to certify that the individual component will perform in the manner and for the specified time.

p. *Software License Agreement:* Vendor must provide a consolidated source with details of the software license agreements of all procured software and programs used in the creation, development and continued support of the associated release and version being certified.
q. *Test Data and Software:* Vendor's internal quality assurance procedure, internal or external test data and reports, ballot decks, and software that can be used to demonstrate the various functions of the voting system. Vendor should also verify that the versions of the applications submitted are identical to the versions that have undergone federal compliance testing, for example hash testing tools
r. *Non-Disclosure Agreement or Oath between the Vendor and VSTL*.
    i. Please review the Excel submission file for more information on the naming conventions, content and formatting to be used in the TDP documents.

NOTE: If the voting system is certified, ELECT will retain the TDP so long as the voting system is marketed or used in Virginia.

Corporate Information

Corporate Information must contain the following items:

1. History and description of the business including year established, products and services offered, areas served, branch offices, subsidiary and parent companies, capital and equity structure, identity of any individual, entity, partnership, or organization owning a controlling interest, and the identity of any investor whose investments have an aggregate value exceeding 5% of the vendor's net cash flow in any reporting year,
2. Management and staff organization, number of full-time and part-time employees by category, and resumes of key employees who will assist Virginia localities in acquiring the system if it is authorized for use,
3. Certified financial statements for current and past three (3) fiscal years
    a. If vendor is not the manufacturer of the voting system, then submit the certified financial statements of the manufacturer for the past three (3) fiscal years,
4. Bank Comfort Letter from vendor's primary financial institution
    a. If the vendor uses more than one financial institution, multiple Comfort Letters must be submitted,
5. Certificate of Good Standing issued within 2 months of request for certification,
6. Credit rating issued within 2 months of request for certification,
7. If publicly traded, indexes rating of business debt,
8. Gross sales in voting products and services for the past three (3) fiscal years and the percent of vendor's total sales,

9. The location of all facilities with manufacturing capability; including names and locations of third-party vendor(s) employed or contracted to fabricate, assemble, or both any component part of the voting system, tabulating system, or both being submitted for certification. The location and servicing capability of each facility that will be used to service the voting system, tabulating system, or both for certification and the service limitation of the facility,
10. Quality assurance process used in manufacturing and servicing the voting system, and
11. Configuration management process used with the voting system.

NOTE: If the voting system is certified, ELECT will retain the Corporate Information for as long as the voting system is marketed or used in Virginia. ELECT will sign a confidentially statement for corporate information only.

Proprietary Information

Prior to or upon submission of its certification request, vendor shall identify any information in its request and accompanying materials that it believes should be treated as confidential and proprietary. Further, vendor must state the reasons such information should be treated as confidential and proprietary.

"Identify" means the information must be clearly marked with a justification as to why the information should be treated as confidential and proprietary information. A vendor shall not designate as proprietary information (a) the entire certification request or (b) any portion of the certification request that does not contain trade secrets or proprietary information.
Pursuant to §2.2-3705.6(3), proprietary information is exempt from record requests under the Virginia Freedom of Information Act (VFOIA). Records required to be released that contain both proprietary and non-proprietary information will be redacted before disclosure. ELECT cannot guarantee the extent to which any material provided will be exempt from disclosure in litigation or otherwise. ELECT, however, agrees to provide vendor with five (5) days' notice prior to disclosing such material to third parties so that vendor can seek relief from a court prior to disclosure of such materials by ELECT.

Phase 2: Preliminary Review

The Voting Systems Security Manager, or designee, will review the TDP, Corporate Information, and other materials provided, and notify vendor of any deficiencies. Certification

of the voting system will not proceed beyond this phase until the TDP and Corporate Information are complete.

The Voting System Security Manager, or designee, will conduct a preliminary analysis of the Technical Data Package with VSTL. The Voting System Security Manager, or designee, will also review the Corporate Information and other materials to prepare an Evaluation Proposal, which includes:

1. Components of the voting system to be certified,
2. Financial stability and sustainability of the vendor to maintain product support and contractual agreement for the voting system,
3. Preliminary analysis of TDP.

Phase 3: Technical Data Package to Voting System Test Laboratory (VSTL)

In addition, vendor should submit the TDP to the Voting Systems Security Manager, who shall provide the TDP to the VSTL following review.

Phase 4: Certification Test Report from VSTL

VSTL works directly with the vendor and ELECT to complete all test assertions and test cases. The Certification Test Report will be sent to ELECT upon completion.

Phase 5: On-Site Testing in Mock Election

Vendor will coordinate with the local jurisdiction to test the voting system at a minimum of one polling place. With the vendor and a representative from ELECT present, at least one member of the electoral board and the General Registrar from the local jurisdiction will oversee the test of the system in a mock election. ELECT has the discretion to perform a mock election, using the same process, on-site at the ELECT main building in Richmond, Virginia; instead of a polling place; a general registrar and electoral board member must still be present.

Phase 6: Approval by the SBE

Based on the report from the VSTL, results from the mock election testing, and other information in their possession, the SBE makes the final determination of whether the voting system will be certified for use in Virginia. The decision will be sent to the vendor.

3.3 Incomplete Certification Process

If the certification process is terminated, the vendor will forfeit all fees received by ELECT. Any certification process terminated under this provision must be re-initiated from Phase

1. The vendor is responsible for paying all outstanding balances due to ELECT before ELECT accepts subsequent requests from the vendor.

ELECT reserves the right to terminate the certification process when:

1. Vendor does not respond to a request from ELECT within 90 days,
2. ELECT issues any concerns regarding the certification,
3. The Vendor withdraws from the process,
4. The system fails the VSTL certification test,
5. The test lab cannot conduct the certification testing with the equipment on-hand, or
6. Failure of any step in the test assertions process during the certification week.

3.4 Catalog of Requirements

Requirements (objectives) in this standard have been updated to reflect cybersecurity reviews and updates from both Federal and State regulations to mitigate risks to election systems. Requirements are organized to provide standardization and to align to Commonwealth of Virginia Security Standards (SEC 530-01.1 Controls and Objectives, (SEC-530)), EAC VVSG 2.0, and NIST 800-171A Rev. 2.

The requirements are organized into a well-defined structure and placed into categories named “control families”. There are twelve (12) families, each having a Control Family name and corresponding two-letter acronym. Each control family contains security controls or required functionality for the voting system.

Assessment Criteria and Methodology

State certification testing will evaluate the design and performance of a vendor’s voting system to ensure it complies with all applicable requirements in the Code of Virginia and SBE regulations and policies. ELECT will examine the essential system functions, operational procedures, user guides, documents, and reviews from product users. Hash testing will be conducted to confirm the application software is identical to the certified versions of federal compliance testing.

ELECT may evaluate the user experience with the current and prior versions of the voting system and certification reports from other states. In addition, the security and reliability analysis of the product model will be reviewed to determine the usability of the voting system for Virginia elections. ELECT will also evaluate the testing results from the EAC VSTL that will be submitted as part of the Technical Data Package (TDP).

Assessment objectives identify the specific items being assessed and can include specifications, mechanisms, activities, and organization.

1. Specifications are document-based artifacts (e.g. network diagrams, security plans, requirements, administrator user guides, operator guides, and architectural designs) associated with any proposed voting system
2. Mechanisms are specific to hardware, software, and firmware safeguards employed within a system
3. Activities are protection-related actions supporting a system that involves people (e.g. anti-virus updates, anti-malware updates, BIOS configuration, and access control mechanisms for the addition of users by an administrator).

Criteria

Assessment objectives are based on existing criteria in EAC VVSG 2.0, Code of Virginia, Administrative Code of Virginia, and HAVA, 52 USC §21081. The criteria are authoritative and provide the basis for the Virginia Voting System Certification Standard 3.0.

Methodology

To verify and validate a Vendor is meeting the Virginia Voting System Certification Standard 3.0 criteria, evidence must be provided demonstrating a vendor has fulfilled the objectives. Demonstrative evidence may be provided through the following:

Interview

Interviews of vendor staff may provide information to help the ELECT auditor gain insight into security objectives implementation.

Demonstration

Demonstrations, akin to testing, include review, inspection, observation, study, or analysis of objectives. The items used to demonstrate objectives include documents, mechanisms, or activities.

Common types of documents used as evidence may include but are not limited to:

a. Written policies, processes, and procedures,
b. Training materials,
c. Planning documents, and
d. System, network, and data flow diagrams.

This list of documents is not exhaustive or prescriptive.

Testing

Testing is an important part of the assessment process as it demonstrates what functionality and processes have or have not been built, integrated, or completed. Not all security objectives utilize testing to allow an entity to determine whether the requirement has been met.

Applying methodologies to criteria: Assessment

Each requirement in the Catalog of Requirements is determined to have been Met or Not Met through the application of one of the listed methodologies:

Test: all applicable objectives for the requirement must be tested leveraging technical methods to analyze expected outcomes.

Demonstration (DEMO): a demonstration of requirement implementation must be conducted by the VSSM & VSTL Representative in conjunction with the Vendor demonstrating conformity to the respective requirement.

Documentation (DOC): an examination of documentation in lieu of a demonstration or test will be specified in the Catalog of Requirements.

ELECT may require any test assertion that has a methodology marked as “Demo” or “Doc” to instead be completed as a test for verification of compliance.

Assessment Findings

The Assessment Findings for each requirement results in one of two possible findings: MET or NOT MET.

MET: All applicable objectives for the requirement are satisfied based on evidence. All evidence must be in final form. Unacceptable forms of evidence include working papers, draft documentation, and unofficial or unapproved policies. Each test assertion or objective must be explicitly complied with based on the objective IDs and written descriptions. Vendors should pay close attention to the certification objectives and ensure their systems meet the requirements as stated. If the vendor has questions, they should contact ELECT.

NOT MET: One or more objectives of the requirements are not satisfied. For each requirement marked NOT MET, it is best practice to record statements that explain why and document the appropriate evidence showing that the vendor voting system does not conform fully to all the requirements. When any requirement, objective, or test assertion fails and is not met after the objective is tested for compliance, ELECT may stop the certification process at the point of failure. The vendor remains responsible for all payments and fees to the VSTL and ELECT.

Requirements Descriptions

This section provides detailed information and guidance for assessing requirements as described in this Standard.

Each security or functional control is identified by i) a Control Family name, ii) Control ID/Family ID number (1 -12), iii) Control Acronym, and iv) an Objective ID beginning with a two-letter identifier.

For example, AA-1.1-C.2.24 is a control in the ADA and Accessibility (AA) Control family. Each Objective ID is followed by an Objective and Evaluation Assertion (function or process the system must be able to do or the test assertion), the authority for the requirement (Code of Virginia, Virginia Administrative Code, VVSG 2.0), and the Methodology used to verify the Objective and Evaluation Assertion (test, demo, doc). The table below provides a snapshot of this structure.

Control Acronym	Control ID	Objective ID	Objective and Evaluation Assertion	Virginia Functional Need/ VVSG 2.0 Requirement	Virginia Requirement Description	Methodology: Test Demo Doc
AA	1	AA-1.1-C.24	Must be able to alter instructions on the voting system's electronically displayed ballots and audio ballots for ADA/BMD machines.	§ 24.2-629 (B)(1). State Board approval process of electronic voting systems.	It shall provide clear instructions for voters on how to mark or select their choice and cast that vote.	Test

Technical Standard Terms used in the Objective

There are several technical standard terms defined in Appendix A: Glossary. This appendix includes other definitions that may be useful for understanding the standard.

Appendices

Appendix A – Glossary

The following terms are defined in the United States Election Assistance Commission (EAC), the Code of Virginia, and Virginia General Registrars and Electoral Boards (GREB) Handbook.

ADA – Americans with Disability Act (ADA) of 1990 broadly protects the rights of individuals with disabilities in employment, access to state and local government services, places of public accommodation, transportation, and other important areas of American life. The ADA also requires newly designed and constructed or altered state and local government facilities, public accommodations, and commercial facilities to be readily accessible to and usable by individuals with disabilities.

Anomaly – Any event related to the security or functioning of the voting system that is out of the ordinary regardless of whether it is exceptional or not; a deviation from the norm.

Cast Vote Record (CVR) – Permanent record of all votes produced by a single voter.

Center for Internet Security (CIS) – A group of benchmarks for best practices created by industry that are globally recognized and continually updated to improve cyber defense.

De Minimis or Engineering Change Order (ECO) Change – A minimum change to a certified voting system's hardware, software, TDP, or data. The nature of changes will not materially alter the system's reliability, functionality, capability, or operation. Under no circumstance shall a change be considered a De Minimis Change if it has reasonable and identifiable potential to impact the system's performance and compliance with the applicable Voting Standard. Reference: EAC Testing & Certification Program Manual version 2.0 and Notices of Clarification.

Department of Elections (ELECT) – ELECT conducts the SBE's administrative and programmatic operations and discharges the board's duties consistent with delegated authority.

Election Assistance Commission (EAC) – The Help America Vote Act (HAVA) directs the U.S. Election Assistance Commission (EAC) to provide for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories. HAVA also introduces different terminology for these functions. Under the EAC process, test labs are "accredited" and voting systems are "certified." The term "standards" has been replaced with

the term "*Guidelines*." As prescribed by HAVA, the EAC process was initially based on the 2002 Voting Systems Standards and will transition to the latest standards issued.

Help America Vote Act of 2002 (HAVA) – The Help America Vote Act (HAVA) of 2002 made reforms to America's voting process by establishing minimum standards for states regarding election administration. Title III of HAVA contains standards regarding voting systems, provisional voting and voting information, computerized statewide voter registration list, and requirements for first-time voters who register by mail. HAVA standards are critical to the operation of an election.

Incident – Any event related to the security or functioning of the voting system that caused or may have caused an interruption to the Check-in or Reporting process.

Logic and Accuracy Testing – Logic and accuracy testing is an integral part of preparing for an election. Each machine (not a sampling of machines) that will be used in an election must be tested prior to that election to ensure it is programmed correctly and is functioning properly. The logic and accuracy test will also uncover any ballot printing or coding issues that may affect accurate and complete tabulation. Each machine should be tested with a sufficient number of ballots or votes to substantiate that each machine recorded the correct number of votes for each candidate. An electoral board member, a general registrar, or a designated representative must be present during this process and must certify the results from each machine. Form ELECT-633 must be submitted electronically to the Department of Elections after logic and accuracy testing is complete.

State Board of Elections (SBE) –For purposes of these standards, the State Board of Elections is imbued with the powers and duties provided in Title 24.2 of the Code of Virginia. Specifically regarding voting equipment and systems, the board is authorized to approve electronic voting systems that meet the requirements of Chapter 6, Article 3 of the Code of Virginia.

Voting System – The total combination of mechanical, electromechanical, and electronic equipment, including the software, firmware, and documentation required to program, control, and support the equipment, that is used to define ballots, cast and count votes, report or display election results, recount votes and maintain and produce any audit trail information.

Voting System Security Manager (VSSM) – The ELECT designated evaluation agent, responsible for oversight of voting systems and electronic pollbooks certification and security.

Voting System Test Laboratory (VSTL) – Test labs that are accredited to perform conformance testing of voting systems. VSTLs use the SBE approved voting system certification standard to guide the development of test plans, the testing of systems, and the preparation of test reports and recommendations for granting state certification.

Appendix B – Contacts

The certification request package should be sent to:

Virginia Department of Elections
ATTN: Voting System Certification
1100 Bank Street, 1st Floor
Richmond, Virginia 23219-3497

All other inquiries should be sent to: info@elections.virginia.gov.

Appendix C – Local Validation of Certification on Purchase

It is the responsibility of both the vendor and the local jurisdiction to ensure that a voting system supplied or purchased for use in Virginia has been certified by the SBE. The vendor is required to submit any modifications to a previously certified voting system to ELECT for review.
If any question arises involving the certification of a voting system in use in Virginia, ELECT shall verify the voting system in use is identical to the voting system that was submitted for certification. Any unauthorized modifications to a certified system may result in decertification by the SBE or bar the vendor from receiving future certification of voting systems in Virginia.

Acceptance Test

To ensure the voting system purchased for a local election office operates as required and meets all needed functionality, the local jurisdiction, assisted by state officials or consultants, will conduct an Acceptance Test.

The local jurisdiction verifies the purchased or leased system delivered is identical to the certified system and the installed equipment and software are fully functional and compliant with the administrative and statutory requirements of the jurisdiction. The local jurisdiction may perform a hash testing of application software and will send a letter to ELECT as required by the procurement process confirming the versions of software and model(s) of equipment received are identical to the certified system.

As part of the acceptance test the vendor will replicate its designed functionality as presented and tested during certification, including:

1. Process simulated ballots for each precinct or polling place in the jurisdiction,
2. Display an appropriate message on the review screen if a voter does not follow the ballot instruction
    a. Able to override the warning messages for overvote, undervote, or blank ballot to cast the ballot,
3. Handle Write-in votes,
4. Create a Cast Vote Record (CVR) per each vote,
5. Produce an input to or generate a final report of the election, and interim reports as required,
6. Generate system status and error messages,
7. Comply with and enable voter and operator compliance with all applicable, procedural, regulatory, and statutory requirements,
8. Produce an audit log.

Appendix D – Test Assertions

State Certification Audits must include examination of all system operations and procedures, including but not limited to the following Controls:

Control ID	Control Family Name	Control Acronym
1.	ADA and Accessibility	AA
2.	Audit	AU
3.	Ballot Interaction	BI
4.	COTS Analysis	CA
5.	Logic and Accuracy	LA
6.	Operations Manual	OM
7.	Ranked Choice Voting (RCV)	RA
8.	Recount	RC
9.	Reporting	RE
10.	RLA (Risk Limiting Audit)	RL
11.	System Integrity	SI
12.	Voter Privacy	VP

The following test assertions will be executed by the ELECT designated VSTL.

Control Acronym	Control ID	Objective ID	Objective and Evaluation Assertion	Virginia Code/ VVSG 2.0 Requirement (Functional Need)	Virginia Requirement Description	Methodology: Test, Demo, Doc
AA	1	AA-1.1-A.1	The voting system must provide the option for synchronized audio output to convey the same information that is displayed visually to the voter.	5.2-D (VVSG 2.0)		Test
AA	1	AA-1.1-A.2	Sound and visual cues must be coordinated so that:	5.2-E (VVSG 2.0)		Demo
AA	1	AA-1.1-A.3	sound cues are accompanied by visual cues unless the system is set to audio-only; and	5.2-E.1 (VVSG 2.0)		Demo

AA	1	AA-1.1-A.4	visual cues are accompanied by sound cues unless the system is set to visual-only.	5.2-E.2 (VVSG 2.0)		Demo
AA	1	AA-1.1-A.5	During the voting session, the voting system must make it possible for the voter to independently enable or disable either the audio or the visual output and be notified of the change, resulting in a visual-only or audio-only presentation.	6.1-C (VVSG 2.0)		Test
AA	1	AA-1.1-A.6	Reset to default settings: If the adjustable settings of the voter interface have been changed by the voter or election worker during the voting session, the system must automatically reset to the default setting when the voter finishes voting, verifying, and casting.	7.1-A (VVSG 2.0)		Test
AA	1	AA-1.1-A.7	Display and interaction options: The voting system must provide at least the following display format and interaction mode options to enable voters to mark their ballot to vote, and verify and cast their ballot, supporting the full functionality in each mode:	7.2-A (VVSG 2.0)		Test
AA	1	AA-1.1-A.8	Visual format;	7.2-A.1 (VVSG 2.0)		Test
AA	1	AA-1.1-A.9	Enhanced visual format;	7.2-A.2 (VVSG 2.0)		Test
AA	1	AA-1.1-B.10	Audio format;	7.2-A.3 (VVSG 2.0)		Test
AA	1	AA-1.1-B.11	Touch mode; and	7.2-A.4 (VVSG 2.0)		Test

AA	1	AA-1.1-B.12	Limited dexterity mode.	7.2-A.5 (VVSG 2.0)		Test
AA	1	AA-1.1-B.13	Voter display screen has a fixed header or footer that does not disappear, so voters always have access to navigation elements, the name of the current contest, and the voting rules for the contest;	7.2-D.2.a (VVSG 2.0)		Test
AA	1	AA-1.1-B.14	The voting system must be supplied with a means to sanitize headphones or handsets and instructions for election workers on the procedure to ensure that a sanitized headphone or handset is available to each voter.	8.1-H (VVSG 2.0)		Test
AA	1	AA-1.1-B.15	voters with low vision, [can] use the enhanced visual features with and without audio; and	8.3-A.1.c (VVSG 2.0)		Demo
AA	1	AA-1.1-B.16	voters with limited dexterity, [can] use the visual interface with low and no dexterity controls.	8.3-A.1.d (VVSG 2.0)		Demo
AA	1	AA-1.1-B.17	The voting system must provide written and audio instruction for electronically displayed ballots on ADA/BMD machines.	Voting equipment must display an appropriate message if a voter does not follow the ballot instruction. Allow the voter to override the warning message to cast his/her ballot.		Test

AA	1	AA-1.1-B.18	The voting system must allow the voter to return to a contest or question to make corrections for electronically displayed ballots. The voting system must allow an audio voter to return to a contest or question to make corrections.	Voting equipment must display an appropriate message if a voter does not follow the ballot instruction. Allow the voter to override the warning message to cast his/her ballot.		Test
AA	1	AA-1.1-B.19	The voting system must provide feedback to the voter for incomplete/ incorrect votes. i.e. overvotes, undervotes, blank ballot.	Voting equipment must display an appropriate message if a voter does not follow the ballot instruction. Allow the voter to override the warning message to cast his/her ballot.		Test
AA	1	AA-1.1-C.20	The voting system must allow the voter to override warning messages for incomplete/ incorrect votes. i.e. overvotes, undervotes, blank ballot.	Voting equipment must display an appropriate message if a voter does not follow the ballot instruction. Allow the voter to override the warning message to cast his/her ballot.		Test
AA	1	AA-1.1-C.21	The voting system must support audio ballots.	§ 24.2-626.1. Acquisition and use of accessible voting devices.	1. Provide for at least one voting system equipped for individuals with disabilities at each polling place, including non-visual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters. 2. Provide alternative	Test

					language accessibility when required by § 203 of the Voting Rights Act of 1965 (52 U.S.C. § 10503).	
AA	1	AA-1.1-C.22	Using the voting system, an individual voting by audio ballot does not require assistance by marking the ballot.	§ 24.2-626.1. Acquisition and use of accessible voting devices.	1. Provide for at least one voting system equipped for individuals with disabilities at each polling place, including non visual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters. 2. Provide alternative language accessibility when required by § 203 of the Voting Rights Act of 1965 (52 U.S.C. § 10503).	Test
AA	1	AA-1.1-C.23	The voting system must support multiple languages; including, English, Spanish, Vietnamese and allow future additions and support of other languages.	§ 24.2-626.1. Acquisition and use of accessible voting devices. Provide alternative language accessibility when required by § 203 of the Voting Rights Act of 1965 (52 U.S.C. § 10503).	1. Provide for at least one voting system equipped for individuals with disabilities at each polling place, including non visual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters. 2. Provide alternative language accessibility when required by § 203	Test

					of the Voting Rights Act of 1965 (52 U.S.C. § 10503).	
AA	1	AA-1.1-C.24	Must be able to alter instructions on the voting system's electronically displayed ballots and audio ballots for ADA/BMD machines.	§ 24.2-629 (B)(1). State Board approval process of electronic voting systems.	It shall provide clear instructions for voters on how to mark or select their choice and cast that vote.	Test
AU	2	AU-2.2-A.1	The voting system must be capable of logging events that occur in a voting system.	15.1-A (VVSG 2.0)		Test
AU	2	AU-2.2-A.2	The voting system must be capable of exporting logs.	15.1-B (VVSG 2.0)		Test
AU	2	AU-2.2-A.3	At minimum, the voting system must log the events included in Table 15-1.	15.1-D (VVSG 2.0)		Demo
AU	2	AU-2.2-A.4	Includes but is not limited to: • The source and disposition of system interrupts resulting in entry into exception handling routines. • Messages generated by exception handlers. • The identification code and number of occurrences for each hardware and software error or failure. • Notification of physical violations of security. • Other exception events such as power failures, failure of critical hardware components, data transmission errors, or other types of operating anomalies. • All faults and the recovery actions taken. Device generated error and exception messages such as ordinary timer system	15.1-D.1.a (VVSG 2.0)		Demo

			interrupts and normal I/O system interrupts do not need to be logged.			
AU	2	AU-2.2-A.5	Includes but is not limited to: • Login/logoff events (both successful and failed attempts) • Account lockout events • Password changes	15.1-D.2.a (VVSG 2.0)		Demo
AU	2	AU-2.2-A.6	At a minimum, critical cryptographic settings include key addition, key removal, and re-keying.	15.1-D.4.e (VVSG 2.0)		Doc
AU	2	AU-2.2-A.7	The software installation procedures must specify the creation of a software installation record that includes at a minimum:	3.1.4-I (VVSG 2.0)		Test
AU	2	AU-2.2-A.8	a unique identifier (such as a serial number) for the record;	3.1.4-I.1 (VVSG 2.0)		Demo
AU	2	AU-2.2-A.9	a list of unique identifiers of storage media associated with the record;	3.1.4-I.2 (VVSG 2.0)		Demo
AU	2	AU-2.2-B.10	the time, date, and location of the software installation;	3.1.4-I.3 (VVSG 2.0)		Demo
AU	2	AU-2.2-B.11	names, affiliations, and signatures of all people present;	3.1.4-I.4 (VVSG 2.0)		Demo
AU	2	AU-2.2-B.12	copies of the procedures used to install the software on the programmed devices of the voting system;	3.1.4-I.5 (VVSG 2.0)		Demo
AU	2	AU-2.2-B.13	the certification number of the voting system;	3.1.4-I.6 (VVSG 2.0)		Test
AU	2	AU-2.2-B.14	list of the software installed as well as associated digital signatures and mechanisms for installation and verification on programmed devices of the voting system; and	3.1.4-I.7 (VVSG 2.0)		Demo

AU	2	AU-2.2-B.15	a unique identifier (such as a serial number) of the vote-capture device or election management system (EMS) by which the software is installed.	3.1.4-I.8 (VVSG 2.0)		Demo
AU	2	AU-2.2-B.16	The voting system's audit, casting, tabulation, and vote-capture functions dealing with CVRs must have the capability of importing or exporting CVRs according to CDF specification(s).	4.1-C (VVSG 2.0)		Demo
AU	2	AU-2.2-B.17	All voting systems must provide a voter verifiable audit trail, a permanent paper record of each vote.	§ 24.2-629 (B)(3). State Board approval process of electronic voting systems.	It shall be capable of processing ballots for all parties holding a primary election on the same day, but programmable in such a way that an individual ballot cast by a voter is limited to the party primary election in which the voter chooses to participate.	Test
BI	3	BI-3.3-A.1	The voting system records how many ballots are cast as overvotes, undervotes, Write-ins, and blank ballots for each contest and question.	§ 24.2-657. Determination of vote on voting systems. See Ballot Interaction, Objective ID BI-3.3-A.2	See Ballot Interaction, Objective ID BI-3.3-A.2	Test
BI	3	BI-3.3-A.2	Public and private ballot counters increment for each accepted ballot. The ballot counters do not increment for ballots rejected by the system.	§ 24.2-657. Determination of vote on voting systems. In the presence of all persons who may be present lawfully at the time, giving full view of the voting systems or	If, on any ballot scanner, the number of persons voting in the election, or the number of votes cast for any office or on any question, totals more than the number of names on the poll books of	Test

				printed return sheets, the officers of election shall determine and announce the results as shown by the counters or printed return sheets, including the votes recorded for each office on the Write-in ballots, and shall also announce the vote on every question. The vote as registered shall be entered on the statement of results. When completed, the statement shall be compared with the number on the counters on the equipment or on the printed return sheets.	persons voting on the machines, then the figures recorded by the machines shall be accepted as correct. A statement to that effect shall be entered by the officers of election in the space provided on the statement of results	
BI	3	BI-3.3-A.3	The voting system must alert the voter when the ballot submitted has an overvote or undervote, or the ballot is blank.	§ 24.2-629 (B)(14). State Board approval process of electronic voting systems.	Ballot scanner machines shall report, if possible, the number of ballots on which a voter under voted or over voted.	Test
BI	3	BI-3.3-A.4	The voting system must allow the voter to submit a ballot with an overvote or undervote, or a blank ballot.	§ 24.2-629 (B)(14). State Board approval process of electronic voting systems.	Ballot scanner machines shall report, if possible, the number of ballots on which a voter under voted or over voted.	Test
BI	3	BI-3.3-A.5	The voting system must count ballots cast with an undervote, overvote, or blank ballot. The system	§ 24.2-629 (B)(14). State Board approval process	Ballot scanner machines shall report, if possible, the number of ballots	Test

			must be capable of producing a human-readable report on the number of ballots on which a voter under voted, and the number of ballots on which a voter over voted.	of electronic voting systems.	on which a voter under voted or over voted.	
BI	3	BI-3.3-A.6	All Write-ins are properly handled including segregation of Write-ins physically with a diverter or logically with electronic Write-in Report.	§ 24.2-629 (B)(14). State Board approval process of electronic voting systems.	Ballot scanner machines shall report, if possible, the number of ballots on which a voter under voted or over voted.	Test
BI	3	BI-3.3-A.7	The voting system must make a copy of the voter's Write-in vote; the copy must be as legible as the original.	The voting system must comply with the requirements for Write-in image and format.		Test
BI	3	BI-3.3-A.8	For a Virginia Primary Election, the voting system must define the primary ballot as follows:	Define ballot formats for a primary election, a general election, and special election including all voting options defined by the Code of Virginia.		Test
BI	3	BI-3.3-A.9	a. Open Primary	See Ballot Interaction, Objective ID BI-3.3-A.8		Test
BI	3	BI-3.3-B.10	b. Two Parties	See Ballot Interaction, Objective ID BI-3.3-A.8		Test
BI	3	BI-3.3-B.11	c. No Write-in candidates	See Ballot Interaction, Objective ID BI-3.3-A.8		Test
BI	3	BI-3.3-B.12	d. Support split precincts	See Ballot Interaction, Objective ID BI-3.3-A.8		Test

BI	3	BI-3.3-B.13	e. Voting for N of M contests	See Ballot Interaction, Objective ID BI-3.3-A.8		Test
BI	3	BI-3.3-B.14	f. Support of all contests	See Ballot Interaction, Objective ID BI-3.3-A.8		Test
BI	3	BI-3.3-B.15	g. Support for all candidates	See Ballot Interaction, Objective ID BI-3.3-A.8		Test
BI	3	BI-3.3-B.16	h. Multi-language support (English, Spanish, Vietnamese)	See Ballot Interaction, Objective ID BI-3.3-A.8		Test
BI	3	BI-3.3-B.17	i. Referendum/Question contests	See Ballot Interaction, Objective ID BI-3.3-A.8		Test
BI	3	BI-3.3-B.18	For a Virginia General Election, the voting system must define the general ballot as follows:	Define ballot formats for a primary election, a general election, and special election including all voting options defined by the Code of Virginia.		Test
BI	3	BI-3.3-B.19	1. Partisan contests	See Ballot Interaction, Objective ID BI-3.3-B.18		Test
BI	3	BI-3.3-C.20	2. Non-partisan contests	See Ballot Interaction, Objective ID BI-3.3-B.18		Test
BI	3	BI-3.3-C.21	3. Write-in candidates	See Ballot Interaction, Objective ID BI-3.3-B.18		Test
BI	3	BI-3.3-C.22	4. Support for split precincts	See Ballot Interaction, Objective ID BI-3.3-B.18		Test

BI	3	BI-3.3-C.23	5. Voting for N of M contests	See Ballot Interaction, Objective ID BI-3.3-B.18		Test
BI	3	BI-3.3-C.24	6. Support of all contests	See Ballot Interaction, Objective ID BI-3.3-B.18		Test
BI	3	BI-3.3-C.25	7. Support for all candidates	See Ballot Interaction, Objective ID BI-3.3-B.18		Test
BI	3	BI-3.3-C.26	8. Multi-language support (English, Spanish, Vietnamese)	See Ballot Interaction, Objective ID BI-3.3-B.18		Test
BI	3	BI-3.3-C.27	9. Referendum/Question contests	See Ballot Interaction, Objective ID BI-3.3-B.18		Test
BI	3	BI-3.3-C.28	Voting systems must be able to read and store printed paper ballots.	§24.2-629(B)(13). State Board approval process of electronic voting systems.	It shall retain each printed ballot cast.	Test
BI	3	BI-3.3-C.29	All Write-ins can be segregated physically with a diverter or logically separated with an electronic Write-in Report.	§ 24.2-629 (B)(12). State Board approval process of electronic voting systems.	It shall be programmable to allow ballots to be separated when necessary.	Test
BI	3	BI-3.3-D.30	Voting systems that centrally process ballots must physically separate Write-ins from other ballots or logically separate ballots with Write-in votes electronically.	§ 24.2-629 (B)(12). State Board approval process of electronic voting systems.	It shall be programmable to allow ballots to be separated when necessary.	Test

BI	3	BI-3.3-D.31	The voting system must support multiple ballot styles on a single tabulator in a primary election.	§ 24.2-629 (B)(3). State Board approval process of electronic voting systems.	It shall be capable of processing ballots for all parties holding a primary election on the same day, but programmable in such a way that an individual ballot cast by a voter is limited to the party primary election in which the voter chooses to participate.	Test
BI	3	BI-3.3-D.32	The voting system can present an accurate ballot based on a voter's geopolitical subdivision based on the districts, regions, cities or other boundaries defined by the Commonwealth of Virginia.	§ 24.2-629 (B)(5). State Board approval process of electronic voting systems.	It shall enable the voter to cast votes for as many persons for an office as lawfully permitted, but no more.	Test
BI	3	BI-3.3-D.33	Each tabulator has a lifetime counter/ "protective counter" that cannot be reset without reloading the firmware.	§ 24.2-629 (B)(9). State Board approval process of electronic voting systems.	It shall be provided with a "protective counter," whereby any operation of the machine before or after the election will be detected.	Test
BI	3	BI-3.3-D.34	The "protective counter" increments correctly for each ballot accepted by the tabulator.	§ 24.2-629 (B)(9). State Board approval process of electronic voting systems.	It shall be provided with a "protective counter," whereby any operation of the machine before or after the election will be detected.	Test
BI	3	BI-3.3-D.35	The "protective counter" does not increment for ballots not accepted by the tabulator.	§ 24.2-629 (B)(9). State Board approval process of electronic voting systems.	It shall be provided with a "protective counter," whereby any operation of the machine before or after the election will be detected.	Test

BI	3	BI-3.3-D.36	Each tabulator has a "public counter" which tracks the number of ballots processed and accepted for an election.	§ 24.2-629 (B)(10). State Board approval process of electronic voting systems.	It shall be provided with a counter that at all times during an election shall show how many persons have voted.	Test
BI	3	BI-3.3-D.37	The "public counter" increments correctly for each ballot accepted by the tabulator.	§ 24.2-629 (B)(10). State Board approval process of electronic voting systems.	It shall be provided with a counter that at all times during an election shall show how many persons have voted.	Test
BI	3	BI-3.3-D.38	The "public counter" does not increment for ballots not accepted by the tabulator.	§ 24.2-629 (B)(10). State Board approval process of electronic voting systems.	It shall be provided with a counter that at all times during an election shall show how many persons have voted.	Test
CA	4	CA-4.4-A.1	The malware protection mechanisms for COTS devices providing EMS functionality must be updatable.	15.3-B (VVSG 2.0)		Demo
CA	4	CA-4.4-A.2	The voting system documentation must include the process and procedures for updating malware protection mechanisms.	15.3-C (VVSG 2.0)		Demo
CA	4	CA-4.4-A.3	COTS workstations and servers providing EMS functionality must immediately notify an election official when malware is detected.	15.3-D (VVSG 2.0)		Demo
CA	4	CA-4.4-A.4	The voting system must log instances of detecting malware.	15.3-E (VVSG 2.0)		Demo
CA	4	CA-4.4-A.5	COTS workstations and servers providing EMS functionality must provide a notification upon the removal or remediation of malware.	15.3-F (VVSG 2.0)		Demo

CA	4	CA-4.4-A.6	The voting system must log malware remediation activities.	15.3-G (VVSG 2.0)		Demo
LA	5	LA-5.5-A.1	The voting system can be programmed for a primary, general, or special election.	The voting system must be able to perform the Logic and Accuracy Tests.		Test
LA	5	LA-5.5-A.2	The voting system can process a known test deck containing valid marks, non-valid marks, undervotes, overvotes, and Write-in votes.	The voting system must be able to perform the Logic and Accuracy Tests.		Test
LA	5	LA-5.5-A.3	The voting system can report accurate results from the known test deck.	The voting system must be able to perform the Logic and Accuracy Tests.		Test
LA	5	LA-5.5-A.4	The voting system provides a verifiable means that all test data are removed after the completion of the Logic and Accuracy Test from the voting system.	The voting system must be able to perform the Logic and Accuracy Tests.		Test
LA	5	LA-5.5-A.5	Test ballots can be produced by a Ballot Marking Device (BMD) and can be used in the known test deck.	The voting system must be able to perform the Logic and Accuracy Tests.		Test
OM	6	OM-6.6-A.1	The voting system's documentation must include the hardware and software information for the critical components defined in the 14.3-B and at minimum list the following information for each component:	14.3-C (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-A.2	component name;	14.3-C.1 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-A.3	manufacturer;	14.3-C.2 (VVSG 2.0)		Doc/Demo

OM	6	OM-6.6-A.4	model or version; and	14.3-C.3 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-A.5	applicable platform for software (e.g., Windows or Linux).	14.3-C.4 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-A.6	The voting system documentation must include the network architecture of any internal network used by any portion of the voting system.	15.4-A (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-A.7	The voting system documentation must list security configurations and be accompanied by network security best practices.	15.4-B (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-A.8	The voting system documentation must include information about how wireless is disabled within the voting system.	15.4-C (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-A.9	System overview documentation must include high-level functional diagrams of the voting system that include all its components. The diagrams must portray how the various components relate and interact.	3.1.1-B (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-B.10	System overview documentation must include written descriptions and diagrams that present the following, as applicable:	3.1.1-C (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-B.11	a description of the functional components (or subsystems) as defined by the manufacturer (for example, environment, election management and control, vote recording, vote conversion, reporting, and their logical relationships);	3.1.1-C.1 (VVSG 2.0)		Doc/Demo

OM	6	OM-6.6-B.12	a description of the operational environment of the system that provides an overview of the hardware, firmware, software, and communications structure;	3.1.1-C.2 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-B.13	a concept of operations that explains each system function and how the function is achieved in the design;	3.1.1-C.3 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-B.14	descriptions of the functional and physical interfaces between components;	3.1.1-C.4 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-B.15	identification of all COTS products (both hardware and software) included in the system or used as part of the system's operation, identifying the name, manufacturer, and version used for each such component;	3.1.1-C.5 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-B.16	benchmark directory listings for all software, firmware, and associated documentation included in the manufacturer's release in the order in which each piece of software or firmware would normally be installed upon system setup and installation.	3.1.1-C.9 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-B.17	System overview documentation must include full identification of all software and firmware items, indicating items that were:	3.1.1-D (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-B.18	written in-house including subcontracted;	3.1.1-D.1 (VVSG 2.0)		Doc/Demo

OM	6	OM-6.6-B.19	procured as COTS, unmodified; and	3.1.1-D.2 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-C.20	procured as COTS and modified, including descriptions of the modifications to the software or firmware and to the default configuration options.	3.1.1-D.3 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-C.21	Software installation documentation must include the following information for each piece of software to be installed or used to install software on programmed devices of the voting system:	3.1.4-B (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-C.22	software product name;	3.1.4-B.1 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-C.23	software version number	3.1.4-B.2 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-C.24	software manufacturer name;	3.1.4-B.3 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-C.25	software manufacturer contact information;	3.1.4-B.4 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-C.26	type of software (application logic, border logic, third party logic, COTS software, or installation software);	3.1.4-B.5 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-C.27	list of software documentation; and	3.1.4-B.6 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-C.28	component identifiers (such as filenames) of the software, and type of software component (executable code, source code, or data).	3.1.4-B.7 (VVSG 2.0)		Doc/Demo

OM	6	OM-6.6-C.29	Manufacturers must provide a specific system operations document for use by all personnel who support pre-election and election preparation, polling place activities, and central counting activities, as applicable, regarding all system functions and operations. It must:	3.1.5-A (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-D.30	provide a detailed description of procedures required to initiate, control, and verify proper system operation;	3.1.5-A.1 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-D.31	provide procedures that clearly enable the operator to assess the correct flow of system functions (as evidenced by system-generated status and information messages);	3.1.5-A.2 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-D.32	provide procedures that clearly enable the administrator to intervene in system operations to recover from an abnormal system state;	3.1.5-A.3 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-D.33	define and illustrate the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system;	3.1.5-A.4 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-D.34	define and illustrate procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved. (This information is provided for the interaction of the system with other data	3.1.5-A.5 (VVSG 2.0)		Doc/Demo

			processing systems or data interchange protocols.);			
OM	6	OM-6.6-D.35	provide administrative procedures and off-line operator duties (if any) if they relate to the initiation or termination of system operations, to the assessment of system status, or to the development of an audit trail;	3.1.5-A.6 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-D.36	support successful election definition and software installation and control by central election officials;	3.1.5-A.7 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-D.37	provide a schedule and steps for the software and ballot installation, including a table outlining the key dates relative to the start of voting, events, and deliverables; and	3.1.5-A.8 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-D.38	specify diagnostic tests that may be employed to identify problems in the system, verify the correction of problems, and isolate and diagnose faults from various system states.	3.1.5-A.9 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-D.39	The operations document must identify all facilities, furnishings, fixtures, and utilities that will be required for equipment operations, including a statement of all requirements and restrictions regarding:	3.1.5-G (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-E.40	environmental protection;	3.1.5-G.1 (VVSG 2.0)		Doc/Demo

OM	6	OM-6.6-E.41	electrical service;	3.1.5-G.2 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-E.42	recommended auxiliary power;	3.1.5-G.3 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-E.43	telecommunications service; and	3.1.5-G.4 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-E.44	any other facility or resource required for the proper installation and operation of the system.	3.1.5-G.5 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-E.45	the number and skill levels of personnel required for each task;	3.1.6-F.2 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-E.46	the parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance; and	3.1.6-F.3 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-E.47	any maintenance tasks that must be coordinated with the manufacturer or a third party (such as coordination that may be needed for COTS used in the system).	3.1.6-F.4 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-E.48	Maintenance documentation must identify specific procedures to be used in diagnosing and correcting problems in the system hardware, firmware, and software. Descriptions must include:	3.1.6-G (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-E.49	steps to replace failed or deficient equipment;	3.1.6-G.1 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-F.50	steps to correct deficiencies or faulty operations in software or firmware;	3.1.6-G.2 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-F.51	modifications that are necessary to coordinate any modified or upgraded	3.1.6-G.3 (VVSG 2.0)		Doc/Demo

			software or firmware with other modules;			
OM	6	OM-6.6-F.52	number and skill levels of personnel needed to accomplish each procedure;	3.1.6-G.4 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-F.53	special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure; and	3.1.6-G.5 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-F.54	any coordination required with the manufacturer, or other party, for COTS.	3.1.6-G.6 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-F.55	Maintenance documentation must identify and describe any special purpose test or maintenance equipment recommended for fault isolation and diagnostic purposes.	3.1.6-H (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-F.56	Maintenance documentation must include detailed documentation of parts and materials needed to operate and maintain the system.	3.1.6-I (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-F.57	Maintenance documentation must include a complete list of approved parts and materials needed to operate and maintain the system. This list must contain sufficient descriptive information to identify all parts by:	3.1.6-J (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-F.58	type,	3.1.6-J.1 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-F.59	size,	3.1.6-J.2 (VVSG 2.0)		Doc/Demo

OM	6	OM-6.6-G.60	value or range,	3.1.6-J.3 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-G.61	manufacturer's designation,	3.1.6-J.4 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-G.62	individual quantities needed, and	3.1.6-J.5 (VVSG 2.0)		Doc/Demo
OM	6	OM-6.6-G.63	sources from which they may be obtained.	3.1.6-J.6 (VVSG 2.0)		Doc/Demo
RA	7	RA-7.7-A.1	Allow for the selection of at least three (3) rankings in a ranked choice voting (RCV) race.	1VAC20-100-10. Definitions (Ranked Choice Voting). "Ranked choice undervote" means a voter has left a ranking unassigned. 1VAC20-100-10. Definitions (Ranked Choice Voting). "Ranked choice voting" means a method of casting and tabulating votes in which ... voters rank candidates in order of preference .... 1VAC20-100-50(A). Ranked choice voting tabulation. For all elections for an office conducted by ranked choice voting, only first-choice rankings shall be counted in the first-choice ranking tabulation round.	1VAC20-100-70(B). Election Results (Ranked Choice Voting). A record of votes cast at all rankings, as tabulated in the first-choice ranking tabulation round, shall be created and retained for public inspection and copying. 1VAC20-100-65. Write-Ins (Ranked Choice Voting). Pursuant to § 24.2-644 C of the Code of Virginia, at all elections conducted by ranked choice voting except primary elections, any voter may vote for any person other than the listed candidates for the office by writing or hand printing the person's name on the official ballot. 1VAC20-100-10. Definitions (Ranked Choice Voting).	Test

					"Ranked choice overvote" means a voter assigned more than one candidate the same ranking.	
RA	7	RA-7.7-A.2	Tabulate and report on tapes the first-choice rankings, undervotes, overvotes, and write-in votes.	See RCV, Objective ID RA-7.7-A.1 (RCV)	See RCV, Objective ID RA-7.7-A.1 (RCV)	Test
RA	7	RA-7.7-A.3	Create a cast vote record (CVR) of all rankings, undervotes, overvotes, and write-ins.	See RCV, Objective ID RA-7.7-A.1 (RCV)	See RCV, Objective ID RA-7.7-A.1 (RCV)	Test
RA	7	RA-7.7-A.4	Allow for write-ins to be assigned rankings for tabulation in rank choice voting.	See RCV, Objective ID RA-7.7-A.1 (RCV)	See RCV, Objective ID RA-7.7-A.1 (RCV)	Test
RC	8	RC-8.8-A.1	The voting system can be programmed to recount a single contest.	§ 24.2-802.2. Procedure for recount. For ballot scanner machines, the recount officials shall rerun all the machine-readable ballots through a scanner programmed to count only the votes for the parties or issue in question in the recount and to set aside all ballots containing write-in votes, overvotes, and undervotes. The ballots that are set aside, any ballots not accepted by the scanner, and any ballots for which a scanner could not be programmed to meet	If the total number of machine-readable ballots reported as counted by the scanner plus the total number of ballots set aside by the scanner do not equal the total number of ballots rerun through the scanner, then all ballots cast on ballot scanner machines for that precinct shall be set aside to be counted by hand using the standards promulgated by the State Board pursuant to §24.2-802. Prior to running the machine-readable ballots through the ballot scanner machine, the recount officials shall ensure that logic and accuracy tests have been successfully performed on each	Test

				the programming requirements of this subdivision, shall be hand counted using the standards promulgated by the State Board pursuant to §24.2-802.	scanner after the scanner has been programmed. The result calculated for ballots accepted by the ballot scanner machine during the recount shall be considered correct for those machine-readable ballots unless the court finds sufficient cause to rule otherwise.	
RC	8	RC-8.8-A.2	II –Voting systems must be able to display on tape only the count and totals for contest that is to be recounted	§ 24.2-802.2. Procedure for recount.	See Recount, Objective ID RC-8.8-A.1 and Objective ID RCV, RA-7.7-A.1 (RCV)	Test
RE	9	RE-9.9-A.1	All reports must include the date and time of the report's generation, including hours, minutes, and seconds.	1.1.9-M (VVSG 2.0)		Test
RE	9	RE-9.9-A.2	Each test provided in a manufacturer-submitted report of internal testing performed (technical data package (TDP)) must, at least, include the following information:	1.3-A (VVSG 2.0)		Doc
RE	9	RE-9.9-A.3	requirement(s) under test;	1.3-A.1 (VVSG 2.0)		Doc
RE	9	RE-9.9-A.4	items under test to exercise a given requirement;	1.3-A.2 (VVSG 2.0)		Doc
RE	9	RE-9.9-A.5	pass-fail criteria necessary to determine whether requirement has passed the test of conformity to the requirement;	1.3-A.3 (VVSG 2.0)		Doc
RE	9	RE-9.9-A.6	evidence (observations, data) expected to provide justification for satisfying or failing a given pass-fail condition;	1.3-A.4 (VVSG 2.0)		Doc

RE	9	RE-9.9-A.7	test procedures necessary to provide, observe, record, analyze, and interpret this evidence relative to pass-fail criteria;	1.3-A.5 (VVSG 2.0)		Doc
RE	9	RE-9.9-A.8	where applicable, descriptions of the causes of variation, ambiguity, noise, or observed errors in observed and recorded evidence during tested procedures;	1.3-A.6 (VVSG 2.0)		Doc
RE	9	RE-9.9-A.9	where applicable, descriptions of any necessary techniques, procedures, or processes applied to normalize or clean data prior to subjecting it to data analysis and interpretation relative to pass-fail criteria;	1.3-A.7 (VVSG 2.0)		Doc
RE	9	RE-9.9-B.10	report of actual tests performed and their results; and	1.3-A.8 (VVSG 2.0)		Test
RE	9	RE-9.9-B.11	description and justification if a given test cannot be fully performed or exercised due to internal resource constraints, including description of alternative means of verification.	1.3-A.9 (VVSG 2.0)		Doc
RE	9	RE-9.9-B.12	The voting system can support the ability to print multiple results tapes. The voting system allows for the tapes to be printed in any format and position. Including list below:	§ 24.2-658. Machines with printed return sheets The voting system can support the ability to print multiple results tapes. The voting system allows for the tapes to be printed in at least the formats and positions listed	If machines that print returns are used, the printed inspection sheet and two copies of the printed return sheet containing the results of the election for each machine.	Test

RE	9	RE-9.9-B.13	a. Total precinct ballots cast: (how many ballots were fed through the machine). Can be printed in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-B.14	b. Contest: Contest of ballots cast (all ballots fed into machine that had that contest on it, including overvotes and undervotes). Can be printed in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-B.15	c. Contest: Write-in total. Can print in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-B.16	d. Contest: Votes cast for each candidate. Can print in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-B.17	e. Contest: Overvote totals. Can print in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-B.18	f. Multi-seat contest: Ballots cast. Can print in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-B.19	g. Multi-seat contest: Votes cast for each candidate. Can print in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-C.20	h. Multi-seat contest: Write-ins. Can print Write-ins, in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-C.21	i. Multi-seat contest: Overvotes. Can print in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test

RE	9	RE-9.9-C.22	j. Multi-seat contest: Undervotes. Can print in any format or order required on tape. For example, a "vote for 3" for which a ballot has only voted for one candidate would have 2 undervotes displayed on the tape. This way it adds up to the total ballots cast for the contest x the amount of seats to be held (in this case 1 vote+2undervotes= 1 ballots cast x 3 seats to be filled)	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-C.23	k. Ranked Choice Votes: Ballots cast. Can print in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-C.24	l. Ranked Choice Votes (RCV): First round votes Cast. Can print first round votes cast in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-C.25	m. Ranked Choice Votes: Write-ins. Can print in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-C.26	n. Ranked Choice Votes: First round overvotes. Can print in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-C.27	o. Ranked Choice Votes (RCV): First round undervotes (if first round is skipped, it is counted as one undervote). Can be printed in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-C.28	p. Ranked Choice Votes (RCV): Write-in image. Can print in any format or order required on tape.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test

RE	9	RE-9.9-C.29	q. RLA: Vote totals by contest by batch or report that does the same. Can print in any format or order required on tape and in a report.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-D.30	r. RLA: Ability to batch on tabulator and print batch information in any format or order as required on tape and in a report.	See Reporting, Objective ID RE-9.9-B.12	See Reporting, Objective ID RE-9.9-B.12	Test
RE	9	RE-9.9-D.31	The voting system can export the CVR to a portable transport media. The voting system must produce a CVR in human-readable format.	The CVR must integrate in a readable format.		Test
RE	9	RE-9.9-D.32	The tabulation component of the voting system must have a public counter. Upon opening of the polls, the tabulator must print a zero-proof report and the voting system must provide a means by which the report and the counter can be reconciled.	§ 24.2-637. Furniture and equipment to be at polling places.	Before the time to open the polls, each electoral board shall ensure that the general registrar has the voting and counting equipment and all necessary furniture and materials at the polling places, with counters on the voting or counting devices set at zero (000).	Test
RE	9	RE-9.9-D.33	The voting system must produce a CVR in human-readable format.	The voting system must create a Cast Vote Record (CVR) defined as, a Permanent record of all votes produced by a single voter whether in electronic, paper or other form, for each ballot for all elections.		Test
RL	10	RL-10.10-A.1	The voting system must be capable of producing a CVR for purposes of conducting	§ 24.2-671.2. Risk-limiting Audits C. The Department shall provide that the	for which certification by the State Board is required under § 24.2-680; and	Test

			a post-election risk-limiting audit.	following risk-limiting audits be conducted: 1. In the year of a general election for members of the United States House of Representatives, a risk-limiting audit of at least one randomly selected contested race for such office; 2. In the year of a general election for members of the General Assembly, a risk-limiting audit of at least one randomly selected contested race for such office; 3. In any year in which there is not a general election for a statewide office, a risk-limiting audit of at least one randomly selected contested race for a local office, including constitutional offices,	4. In any year, any other risk-limiting audit of a contested race that is necessary to ensure that each locality participates in a risk-limiting audit of an office within its jurisdiction at least once every five years or that the State Board finds appropriate. Such audits must be approved by at least a two-thirds majority vote of all members of the Board. D. A local electoral board may request that the State Board approve the conduct of a risk-limiting audit for a contested race within the local electoral board's jurisdiction. The state board shall promulgate regulations for submitting such requests. The State Board shall grant an extension of the local electoral board's certification deadline under § 24.2-671 as necessary to accommodate the conduct of a risk-limiting audit conducted pursuant to this subsection. The Department may count a risk limit voting audit conducted pursuant to this subsection toward the	

					requirement in subdivision C 4.	
SI	11	SI-11.11-A.1	The voting system must prevent:	11.1-C (VVSG 2.0)		Demo
SI	11	SI-11.11-A.2	the logging capability from being disabled;	11.1-C.1 (VVSG 2.0)		Test
SI	11	SI-11.11-A.3	the log entries from being modified in an undetectable manner; and	11.1-C.2 (VVSG 2.0)		Demo
SI	11	SI-11.11-A.4	The deletion of logs; with the exception of log rotation.	11.1-C.3 (VVSG 2.0)		Demo
SI	11	SI-11.11-A.5	The voting system access control mechanisms must distinguish at least the following voting stages from Table 11-1:	11.2.1-C (VVSG 2.0)		Demo
SI	11	SI-11.11-A.6	Pre-voting - Loading, and configuring device software, maintenance, loading election-specific files, preparing for election day usage	11.2.1-C.1 (VVSG 2.0)		Demo
SI	11	SI-11.11-A.7	Activated - Activating the ballot, printing, casting, spoiling the ballot	11.2.1-C.2 (VVSG 2.0)		Demo
SI	11	SI-11.11-A.8	Suspended - Occurring when an election official suspends voting	11.2.1-C.3 (VVSG 2.0)		Demo
SI	11	SI-11.11-A.9	Post-voting - Closing polls, tabulating votes, printing records	11.2.1-C.4 (VVSG 2.0)		Demo
SI	11	SI-11.11-B.10	The voting system must allow only an administrator to configure the permissions and functionality for each identity, group or role, or process to include account and group or role creation, modification, disablement, and deletion.	11.2.1-D (VVSG 2.0)		Demo

SI	11	SI-11.11-B.11	The voting system must allow only an administrator to create or modify permissions assigned to specific groups or roles.	11.2.1-E (VVSG 2.0)		Test
SI	11	SI-11.11-B.12	The voting system must allow only an administrator to create or assign the groups or roles.	11.2.1-F (VVSG 2.0)		Test
SI	11	SI-11.11-B.13	Voting systems that implement role-based access control must support the recommendations for Core Role Based Access Control (RBAC) in the ANSI INCITS 359-2004 American National Standard for Information Technology – Role Based Access Control [ANSI04] document.	11.2.2-A (VVSG 2.0)		Demo
SI	11	SI-11.11-B.14	At minimum, voting systems that implement RBAC must define groups or roles with the role descriptions within Table 11-2.	11.2.2-B (VVSG 2.0)		Demo
SI	11	SI-11.11-B.15	At minimum, the voting system must use the groups or roles from Table 11-2 – Minimum voting system groups or roles for RBAC and the voting stages from Table 11-1 – Voting stage descriptions, to assign the minimum permissions in Table 11-3.	11.2.2-C (VVSG 2.0)		Demo
SI	11	SI-11.11-B.16	Administrator (Table 11-3)	11.2.2-C.1 (VVSG 2.0)		Demo
SI	11	SI-11.11-B.17	System - EMS; Pre-Voting - Full Access; Activated - Full Access; Suspended - Full Access; Post-Voting - Full Access	11.2.2-C.1.a (VVSG 2.0)		Demo

SI	11	SI-11.11-B.18	System - Electronic BMD; Pre-Voting - Full Access; Activated - Full Access; Suspended - Full Access; Post-Voting - Full Access	11.2.2-C.1.b (VVSG 2.0)		Demo
SI	11	SI-11.11-B.19	System - Voter-Facing Scanner; Pre-Voting - Full Access; Activated - Full Access; Suspended - Full Access; Post-Voting - Full Access	11.2.2-C.1.c (VVSG 2.0)		Demo
SI	11	SI-11.11-C.20	At a minimum, the voting system, to include scanners, tabulators, EMS must be capable of using multi-factor authentication to verify a user has authorized access to perform critical operations, including:	11.3.1-B (VVSG 2.0)		Test
SI	11	SI-11.11-C.21	runtime software updates to the certified voting system;	11.3.1-B.1 (VVSG 2.0)		Test
SI	11	SI-11.11-C.22	aggregation and tabulation;	11.3.1-B.2 (VVSG 2.0)		Test
SI	11	SI-11.11-C.23	enabling network functions;	11.3.1-B.3 (VVSG 2.0)		Test
SI	11	SI-11.11-C.24	changing device states, including opening and closing the polls;	11.3.1-B.4 (VVSG 2.0)		Test
SI	11	SI-11.11-C.25	deleting or modifying the CVRs and ballot images; and	11.3.1-B.5 (VVSG 2.0)		Test
SI	11	SI-11.11-C.26	modifying authentication mechanisms.	11.3.1-B.6 (VVSG 2.0)		Test
SI	11	SI-11.11-C.27	The voting system must authenticate the administrator with a multi-factor authentication mechanism.	11.3.1-C (VVSG 2.0)		Test

SI	11	SI-11.11-C.28	The voting system must, at minimum, meet the password complexity requirements within the latest version of NIST SP 800-63B Digital Identity Guidelines standards.	11.3.2-B (VVSG 2.0)		Test
SI	11	SI-11.11-C.29	The voting system must store authentication data in a way that ensures confidentiality and integrity are preserved.	11.3.2-C (VVSG 2.0)		Doc
SI	11	SI-11.11-D.30	The voting system must compare all passwords against a manufacturer-specified list of well- known weak passwords and disallow the use of these weak passwords.	11.3.2-D (VVSG 2.0)		Test
SI	11	SI-11.11-D.31	Any unauthorized physical access to voting systems must leave physical evidence that an unauthorized event has taken place.	12.1-A (VVSG 2.0)		Test
SI	11	SI-11.11-D.32	The voting system must allow only authenticated system administrators to access and modify voting device configuration files.	13.1.1-A (VVSG 2.0)		Test
SI	11	SI-11.11-D.33	If a voting system has network functionality, the voting system application must visually show an indicator within the management interface to confirm that wireless networking functionality is disabled.	14.2-D (VVSG 2.0)		Test
SI	11	SI-11.11-D.34	The voting system software must import only library components that are necessary.	14.2-I (VVSG 2.0)		Doc

SI	11	SI-11.11-D.35	The voting system documentation must include the plan for how to address vulnerabilities found in the voting system and at minimum include the following:	14.2-J (VVSG 2.0)		Doc
SI	11	SI-11.11-D.36	how the voting system design process identifies and addresses well-known vulnerabilities;	14.2-J.1 (VVSG 2.0)		Doc
SI	11	SI-11.11-D.37	disclosure of all known vulnerabilities within the system,	14.2-J.2 (VVSG 2.0)		Doc
SI	11	SI-11.11-D.38	a patch management plan; and	14.2-J.3 (VVSG 2.0)		Doc
SI	11	SI-11.11-D.39	the method to receive and send reports of vulnerabilities.	14.2-J.4 (VVSG 2.0)		Doc
SI	11	SI-11.11-E.40	The underlying voting system platform must be free of well-known vulnerabilities as identified in the vulnerability management plan.	14.2-K (VVSG 2.0)		Doc
SI	11	SI-11.11-E.41	The voting system must protect the integrity and authenticity of the allowlist configuration files.	14.3.2-D (VVSG 2.0)		Doc
SI	11	SI-11.11-E.42	The voting system's documentation must contain a supply chain risk management strategy that at minimum includes the following:	14.3-A (VVSG 2.0)		Doc
SI	11	SI-11.11-E.43	a reference to the template or standard used, if any, to develop the supply chain risk management strategy;	14.3-A.1 (VVSG 2.0)		Doc
SI	11	SI-11.11-E.44	the assurance requirements to mitigate supply chain risks;	14.3-A.2 (VVSG 2.0)		Doc

SI	11	SI-11.11-E.45	the contract language that requires suppliers and partners to provide the appropriate information to meet the assurance requirements of the supply chain risk management strategy;	14.3-A.3 (VVSG 2.0)		Doc
SI	11	SI-11.11-E.46	the plan for reviewing and auditing suppliers and partners; and	14.3-A.4 (VVSG 2.0)		Doc
SI	11	SI-11.11-E.47	the response and recovery plan for a supply chain risk incident.	14.3-A.5 (VVSG 2.0)		Doc
SI	11	SI-11.11-E.48	The voting system's documentation must include a list of critical components and suppliers defined by a criticality analysis and supplier impact analysis	14.3-B (VVSG 2.0)		Doc
SI	11	SI-11.11-E.49	The voting system must authenticate administrators before an operating system update is performed.	14.4-A (VVSG 2.0)		Test
SI	11	SI-11.11-F.50	The voting system must authenticate administrators before a software update to the voting system application and related software.	14.4-B (VVSG 2.0)		Test
SI	11	SI-11.11-F.51	The voting system must authenticate administrators before a firmware or driver update.	14.4-C (VVSG 2.0)		Test
SI	11	SI-11.11-F.52	The voting system must be capable of updating rules and policies for network appliances.	15.4-D (VVSG 2.0)		Test
SI	11	SI-11.11-F.53	Application logic must contain no unstructured control constructs.	2.3.1-A (VVSG 2.0)		Doc
SI	11	SI-11.11-F.54	Arbitrary branches (also known as go to's) must not be used.	2.3.1-B (VVSG 2.0)		Doc

SI	11	SI-11.11-F.55	Exceptions must only be used for abnormal conditions. Exceptions must not be used to redirect the flow of control in normal ("non-exceptional") conditions.	2.3.1-C (VVSG 2.0)		Doc
SI	11	SI-11.11-F.56	Unstructured exception handling (for example, On Error GoTo, setjmp/longjmp, or explicit tests for error conditions after every executable statement) is prohibited.	2.3.1-D (VVSG 2.0)		Doc
SI	11	SI-11.11-F.57	Voting system software must not contain hard-coded, including the use of:	2.3-D (VVSG 2.0)		Doc
SI	11	SI-11.11-F.58	passwords, or	2.3-D.1 (VVSG 2.0)		Doc
SI	11	SI-11.11-F.59	cryptographic keys.	2.3-D.2 (VVSG 2.0)		Doc
SI	11	SI-11.11-G.60	The voting system application must defend against SQL injection.	2.5.4-N (VVSG 2.0)		Doc
SI	11	SI-11.11-G.61	Any structured statement or command being prepared using dynamic data (including user input) to be sent to a database or other process must parameterize the data inputs and apply strict type casting and content filters on the data (such as prepared statements).	2.5.4-O (VVSG 2.0)		Doc
SI	11	SI-11.11-G.62	When recovering from non-catastrophic failure of a device or from any error or malfunction that is within the operator's ability to correct, the system must restore the device to the last known good state existing	2.6-C (VVSG 2.0)		Test

			immediately before the error or failure, without loss or corruption of voting data previously stored in the device.			
SI	11	SI-11.11-G.63	The E2E cryptographic protocol used by the cryptographic E2E verifiable voting system must be evaluated and approved through a public process established by the EAC.	9.1.6-A (VVSG 2.0)		Doc
SI	11	SI-11.11-G.64	A cryptographic E2E verifiable voting system must undergo an independent evaluation to verify it correctly and securely implements approved E2E cryptographic protocol.	9.1.6-B (VVSG 2.0)		Doc
SI	11	SI-11.11-G.65	G- Hardware Memory Devices Memory devices or USB drives provided with the voting system and/or supplied to localities must follow these standards:	G- Hardware Guidelines		Test
SI	11	SI-11.11-G.66	1. Must be pre-formatted and blank per the DoD 5220.22-M wiping standard to prevent any preloaded software from being inadvertently installed on the system. Also, the system must use DoD 5220.22-M wiping standards to create blank systems	G- Hardware Guidelines		Test
SI	11	SI-11.11-G.67	2. Must be cryptographic and FIPS 140-2 v2 compliant	G- Hardware Guidelines		Test
SI	11	SI-11.11-G.68	3. Must use SHA 256 hashing algorithm or higher	G- Hardware Guidelines		Test

SI	11	SI-11.11-G.69	4. Must comply with applicable Commonwealth information security standards	G- Hardware Guidelines		Test
SI	11	SI-11.11-H.70	5. Must comply with applicable policies, guidelines, and directives as adopted and modified by the SBE from time to time	G- Hardware Guidelines		Test
SI	11	SI-11.11-H.71	E - Software Patching Guidelines All vendors must comply with the policies, guidelines, and directives regarding software patching of voting systems as adopted and modified by the EAC and the SBE from time to time	All vendors must comply with the policies, guidelines, and directives regarding software patching of voting systems as adopted and modified by the EAC and the SBE from time to time		Test
SI	11	SI-11.11-H.72	Only those with administrative rights can alter the instruction to voters.	The voting system must allow instruction to voters to be modified through administrative rights.		Test
SI	11	SI-11.11-H.73	The tabulation component of the voting system must have the ability to be physically locked and require a key.	§ 24.2-634. Locking and securing after preparation.	When voting equipment has been properly prepared for an election, it shall be locked against voting and sealed, or if a voting or counting machine cannot be sealed with a numbered seal, it shall be locked with a key. The equipment keys and any electronic activation devices shall be retained in the custody of the general registrar and delivered to the officers of election as provided in §	Test

					24.2-639. After the voting equipment has been delivered to the polling places, the general registrar shall provide ample protection against tampering with or damage to the equipment.	
SI	11	SI-11.11-H.74	The voting system can be verified to comply with the SCAP checklist and all manufacturer procedures and specifications.	The voting system must be hardened using the voting system provider's procedures and specifications.		Test
SI	11	SI-11.11-H.75	The Security Content Automation Protocol (SCAP) for the voting system must be provided.	The voting system must be hardened using the voting system provider's procedures and specifications.		Test
SI	11	SI-11.11-H.76	The voting system must require a minimum 8-character password.	The voting system must comply with the latest password protection standards.		Test
SI	11	SI-11.11-H.77	The voting system will not transfer information between or among voting machines wirelessly. Here, wirelessly means "via electromagnetic waves without the use of electrical conductors."	§ 24.2-625.2. Wireless communications at polling places.	There shall be no wireless communications on election day, while the polls are open, between or among voting machines within the polling place or between any voting machine within the polling place and any equipment outside the polling place. For purposes of this section, the term wireless communication shall	Test

					mean the ability to transfer information via electromagnetic waves without the use of electrical conductors.	
SI	11	SI-11.11-H.78	The voting system will be unable to communicate wirelessly between devices inside and outside the polling place. Here, wirelessly means “via electromagnetic waves without the use of electrical conductors.”	§ 24.2-625.2. Wireless communications at polling places. The voting system cannot have built-in wireless communications capabilities. The system must not have software or firmware that allows wireless capability. Software or firmware that disables wireless capability does not meet the criteria.	There shall be no wireless communications on election day, while the polls are open, between or among voting machines within the polling place or between any voting machine within the polling place and any equipment outside the polling place. For purposes of this section, the term wireless communication shall mean the ability to transfer information via electromagnetic waves without the use of electrical conductors.	Test
SI	11	SI-11.11-H.79	No component of the voting system, scanner or tabulator can have wireless communications hardware, to include, wireless network cards, Bluetooth, infrared, etc.	The voting system cannot have the built-in wireless communications abilities.	The voting system cannot have built-in wireless communications capabilities. The system must not have software or firmware that allows wireless capability. Software or firmware that disables wireless capability does not meet the criteria.	Test
SI	11	SI-11.11-I.80	All modules are cryptographic and are FIPS 140-2 v2 compliant.	The voting system must comply with the latest encryption standard.		Test

SI	11	SI-11.11-I.81	All stored images are digitally signed.	The voting system must comply with the latest encryption standard.		Test
SI	11	SI-11.11-I.82	All digital hashes use SHA256 hashing algorithm or higher.	The voting system must comply with the latest encryption standard.		Test
SI	11	SI-11.11-I.83	Hash testing performed on voting system to ensure software is the same as EAC certified software version presented for certification	The voting system must comply with the latest encryption standard.		Test
VP	12	VP-12.12-A.1	System use of voter information The voting system must be incapable of accepting, processing, storing, and reporting identifying information about a specific voter.	10.1-A (VVSG 2.0)		Demo
VP	12	VP-12.12-A.2	Identifiers used for audits. Identifiers used for tying a cast vote record (CVR) and ballot images to physical paper ballots must be distinct from identifiers used for indirect associations.	10.2.2-A (VVSG 2.0)		Test
VP	12	VP-12.12-A.3	The voting system must not log any information:	15.1-C (VVSG 2.0)		Demo
VP	12	VP-12.12-A.4	identifying a specific voter, and	15.1-C.1 (VVSG 2.0)		Demo
VP	12	VP-12.12-A.5	connecting a voter to a specific ballot.	15.1-C.2 (VVSG 2.0)		Demo
VP	12	VP-12.12-A.6	The voter cannot be identified in any manner on a ballot.	§ 24.2-629 (B)(11). State Board approval process of electronic voting systems.	It shall ensure voting in absolute secrecy. Ballot scanner machines shall provide for the secrecy of the ballot and a method	Test

					to conceal the voted ballot.	
VP	12	VP-12.12-A.7	The voting system audit records contain no information on a specific voter.	§ 24.2-629 (B)(11). State Board approval process of electronic voting systems.	It shall ensure voting in absolute secrecy. Ballot scanner machines shall provide for the secrecy of the ballot and a method to conceal the voted ballot.	Test
VP	12	VP-12.12-A.8	The voting system must provide a “privacy sleeve.”	§ 24.2-629 (B)(11). State Board approval process of electronic voting systems.	It shall ensure voting in absolute secrecy. Ballot scanner machines shall provide for the secrecy of the ballot and a method to conceal the voted ballot.	Test

Appendix E – Software Patching Guidelines

All vendors must comply with the policies, guidelines, and directives regarding software patching of voting systems as adopted and modified by the EAC and the SBE from time to time.

Appendix F – Recertification Guidelines

All vendors must comply with the policies, guidelines, and directives regarding recertification of voting systems as adopted and modified by the SBE from time to time.

If there is evidence of a material non-compliance, ELECT will work with the vendor to resolve the issue, and ultimately the SBE reserves the right to decertify the voting system.

A voting system that has been decertified by the SBE cannot be used for elections held in the Commonwealth of Virginia and cannot be purchased by localities to conduct elections.

Appendix G – Hardware Guidelines

Memory devices or USB drives provided with the voting system supplied to localities must follow these standards:

1. Must be pre-formatted and blank per the DoD 5220.22-M wiping standard to prevent any preloaded software from being inadvertently installed on the systems.
2. The system must use DoD 5220.22-M wiping standards to create blank systems.
3. Must be cryptographic and FIPS 140-2 v2 compliant.
4. Must use SHA256 hashing algorithm or higher.
5. Must comply with applicable Commonwealth information security standards.
6. Must comply with applicable policies, guidelines, and directives as adopted and modified by the SBE from time to time.

Appendix H – Voting System Modifications & Product End of Life Planning

Voting System Modifications

The process of reporting modifications will be determined by the Department of Elections based upon policies, guidelines, and directives as adopted and modified by the SBE from time to time.

Product End of Life Planning

"End of life" (EOL) is a term used with respect to product (hardware/software/component) supplied to customers, indicating that the product is in the end of its useful life (from the vendor's point of view), and a vendor stops sustaining it. (i.e. vendor limits or ends support or production for the product)

Product support during EOL varies by product. Depending on the vendor, EOL may differ from end of service life, which has the added distinction that a vendor of systems or software will no longer provide maintenance, troubleshooting or other support. For example, Extended Support is the period following end of Mainstream Support.

The definitions of Last Date of Mainstream Support and Extended Support, as applicable to decertification/recertification and associated policies and procedures, will be determined by the ELECT based upon policies, guidelines, and directives as adopted and modified by the SBE from time to time. As of initial adoption of this standard by the SBE, the definitions are as follows:

Mainstream Support: The first phase of the product lifecycle; when support is complimentary
Extended Support: The phase following Mainstream Support, in which support is no longer complimentary
Last Date of Mainstream Support: The last day of Mainstream Support

Policies and procedures applicable to decertification/recertification of voting systems which contain software or hardware components that have or will reach the Last Date of Mainstream Support within 18 months, will be determined by the ELECT based upon policies, guidelines, and directives as adopted and modified by the SBE from time to time.

A voting system could still be decertified even if an upgrade plan is submitted. This could happen for a variety of reasons, such as a vendor not showing progress in meeting their upgrade plan.

★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

Vendor Notification of "End of Life"

We have certified equipment with the SBE and have determined that the following (hardware/ software/components) in our certified system will, within 18 months, be at "End of Life" status. Complete this form (for the areas applicable), attach the upgrade plan and send to:

Secretary of SBE, 1100 Bank Street, 1st Floor, Richmond, VA 23219

"End of life" (EOL) is a term used with respect to product (hardware/software/component) supplied to customers, indicating that the product is in the end of its useful life (from the vendor's point of view), and a vendor stops sustaining it; i.e. vendor limits or ends support or production for the product.

Mainstream Support: The first phase of the product lifecycle; when support is complimentary
Extended Support: The phase following Mainstream Support, in which support is no longer complimentary
Last Date of Mainstream Support: The last day of Mainstream Support

Vendor_____Date:_____

Certified Voting Systems Impacted:_____

Certified Version(s) Software:_____ Firmware:_____

Certified Product:_____

Certified EPB System Impacted:_____

Certified Version(s):_____

DATE(S) FOR "END OF LIFE":

☐ Operating System

☐ (description)_____ Software

☐ (Modules or Packages) (description)_____

Product(s) (components)

(description)_____

Vendor must submit an upgrade plan to the SBE 12 months in advance of "End of Life". The plan should include timeline(s), list of impacted localities, estimated cost for localities (if any), and VSTL report(s) showing the upgrade(s) will ensure all systems operate properly with the new upgrade(s) and/or replacements(s).*

*A voting system could still be decertified even if an upgrade plan is submitted. This could happen for a variety of reasons, such as a vendor is not showing progress in meeting their upgrade plan.

ELECT Personnel Received and Reviewed by_____ Date:_____

EOL Upgrade Plan ☐ Approved ☐ REJECTED SBE Meeting:_____

Appendix I – Voting System Certification Application Form

Certification ☐ Recertification ☐

The company officer or designee responsible for the voting system should complete this form. With this signature, the company officer agrees to a release for the VSTL, as well as other states that may have decertified the voting system, to respond to questions by ELECT. This application must be signed by a company officer and be enclosed with the Voting System Certification Request Package.

☐ Check if you prefer to have the VSTL testing performed at another site to be specified which may require additional cost for the testing.

Name of Company: _____

Name and Title of Corporate Officer: _____

Contact Phone Number: _____

Email Address: _____

Primary Address of Company: _____

City, State, Zip Code: _____

Name of voting system to be certified: _____

Version Number/Name of Voting System to be certified: _____

I reviewed and confirmed that the voting system meets the requirements of the Virginia Voting System Certification Standard. My company will comply with additional requests in a timely manner to complete this certification.

Signature of Corporate Officer: _____

Date: _____

Appendix J – De Minimis Change Guideline

The SBE has adopted the EAC's De Minimis Change Guideline and applicable EAC Notice of Clarification of De Minimis Change Guidelines to manage minimal hardware, software, or both changes to a certified voting system in a consistent and efficient manner. Software De Minimis Changes should have the following general characteristics:

1. Update a discrete component of the system and do not impact overall system functionality
2. Do not modify the counting or tally logic of a component or the system (formatting changes to reports are allowable)
3. Do not affect the accuracy of the component or system
4. Do not negatively impact the functionality, performance, accessibility, usability, safety, or security of a component or system
5. Do not alter the overall configuration of the certified system (e.g. adding ballot marking device functionality to a previously certified DRE component) 6. Can be reviewed and/or tested by VSTL personnel in a short amount of time (approximately less than 100 hours).

A vendor must submit the VSTL's endorsed package to ELECT for approval along with a copy of the EAC determination. A proposed De Minimis Change may not be implemented to the certified voting system until the change has been approved in writing by ELECT.

VSTL Endorsed Changes

The vendor will forward to ELECT any change that has been endorsed as De Minimis Change by VSTL. The VSTL's endorsed package must include:

1. The vendor's initial description of the De Minimis Change, a narrative of facts giving rise to, or necessitating, the change, and the determination that the change will not alter the system's reliability, functionality, or operation.
2. The written determination of the VSTL's endorsement of the De Minimis Change. The endorsement document must explain why the VSTL, in its engineering judgment, determined that the proposed De Minimis Change meets the definition in this section and otherwise does not require additional testing and recertification.

VSTL Review

The vendor must submit the proposed De Minimis Change to a VSTL with complete disclosures, including:

1. Detailed description of the change
2. Description of the facts giving rise to or necessitating the change

3. The basis for its determination that the change will not alter the system's reliability, functionality, or operation
4. Upon request of the VSTL, the voting system model at issue or any relevant technical information needed to make the determination
5. Document any potential impact to election officials currently using the system and any required notifications to those officials
6. Description of how this change will impact any relevant system documentation
7. Any other information the VSTL needs to make a determination.

The VSTL will review the proposed De Minimis Change and make an independent determination as to whether the change meets the definition of De Minimis Change or requires the voting system to undergo additional testing as a system modification. If the VSTL determines that a De Minimis Change is appropriate, it shall endorse the proposed change as a De Minimis Change. If the VSTL determines that modification testing and certification should be performed, it shall reclassify the proposed change as a modification. Endorsed De Minimis Change shall be forwarded to ELECT for final approval. Rejected changes shall be returned to the vendor for resubmission as system modifications.

ELECT's Action

ELECT will review the proposed De Minimis Change endorsed by a VSTL. ELECT has sole authority to determine whether any VSTL endorsed change constitutes a De Minimis Change under this section.

ELECT's Approval: ELECT shall provide a written notice to the vendor that ELECT accepted the change as a De Minimis Change. ELECT will maintain the copies of approved De Minimis Change and track such changes.

ELECT's Denial: ELECT will inform the vendor in writing that the proposed change cannot be approved as De Minimis Change. The proposed change will be considered a modification and requires testing and recertification consistent with this Certification Standard.

De Minimis Change is not applicable to the voting system currently undergoing the State Certification testing; it is merely a change to an uncertified system and may require an application update.

★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

Virginia State Board of Elections | Request for De Minimis Change

In accordance with the State Certification of Voting System and Electronic Pollbook Requirements and Procedures, SBE has adopted guidelines to manage hardware and software related changes to certified Voting System and Electronic Pollbook System. To request a De Minimis Change, the procedure begins with a letter from the vendor to the Secretary of the State Board of Elections and the VSTL endorsed package for the De Minimis Change. This letter begins the process to evaluate whether the De Minimis Change will be approved for use on Voting Systems or Electronic Pollbooks certified in Virginia.

De Minimis Changes should have the following characteristics:

1. Update a discrete component of the system and do not impact overall system functionality.
2. Do not affect the accuracy of the component or system.
3. Do not negatively impact the functionality, performance, accessibility, usability, safety, or security of a component or system.
4. Do not alter the overall configuration of the certified system.
5. Can be reviewed and tested by VSTL personnel in a short amount of time (approx. less than 100 hours).

Vendor description of the De Minimis Change:_____

_____

Description of the facts giving rise to or necessitating the change: _____

_____

Document any potential impact to election official currently using the system and any required notifications to those officials. _____

_____

☐ VSTL endorsed package included.

Signature of Company Officer: _____ Date:_____

ELECT's Action: Received by: _____ _____ _____ Date: _____

Reviewed by: _____ _____ _____ Date: _____

☐ APPROVED ☐ REJECTED

Vendor Notified of Status by: (initials) _____ Date: _____

Rev. 09/01/2025

Appendix K – Cast Vote Record Clarification

1. A permanent record of all votes produced by a single voter
2. Electronic CVRs are called ballot images
3. CVR is evidence that a ballot was available for review by the voter
4. CVR should have an identifier that can be linked to an identifier on the corresponding paper ballot provided; the scanner creating the CVR can impress an identifier on the ballot as it is scanned
5. CVR and system should include indications of what actions the scanner took if the scanner does contest-rule post-processing of the ballot selections
6. CVR or system has indications of marginal marks, mark quality and density (if scanner is capable).
7. A CVR can include signed and hashed references to an associated image of the ballot or images of write-ins made by the voter on a paper ballot

Appendix L - Annual Voting System Vendor Certification

Certified Voting System/Version:	Vendor:
Mailing Address:	Contact Person: Title: Telephone: Email:
For the period beginning _____ and ending _____ Must be submitted annually **no later than January 31**.	

Pursuant to the Virginia Department of Elections (ELECT) Voting System Certification Standard, Section 1.3. Decertification, Vendors are required to provide an annual submission of items that will allow ELECT to ensure they have accurate information on changes, incidents, upgrades, and corporate information.

*I certify the following:

a. Vendor has notified ELECT of all incidents, anomalies or security-related breaches experienced in an election jurisdiction, if any (if not, Vendor has attached all necessary supporting documentation to this Certification regarding such incident/anomaly/security-related breach).
b. Vendor has notified ELECT of all changes to Corporate Information, if any (if not, Vendor has attached all necessary supporting documentation to this Certification regarding any changes to Corporate Information).
c. Vendor has provided ELECT with modifications to the certified voting system, if any (if not, Vendor has attached necessary documentation to this Certification regarding modifications and is actively pursuing compliance with the Standard, Section 1.3, and Appendix H).
d. Vendor has provided ELECT with an upgrade plan for all operating systems or components that have reached or will reach the Last Date of Mainstream Support within 18 months, if any (if not, Vendor has attached necessary documentation to this Certification regarding such systems or components and is actively pursuing compliance with the Standard, Section 1.3, and Appendix H).
e. Vendor has updated all software for the certified voting system with the latest patching and vulnerability updates (if not, Vendor has attached necessary supporting documentation to this Certification regarding necessary updates and is actively pursuing compliance with the Standard, Section 1.3, and Appendix E).

Name:	Title:
Signature:	Date:
Note: Please ensure all necessary supporting documentation is attached.	