

PRO V&V



6705 Odyssey Drive
Suite C
Huntsville, AL 35806
(256)713-1111

EAC VVSG 2.0 Certification Test Plan Election Systems & Software (ES&S) Voting System (EVS) 7.0.0.0

Document Number: TP-01-01-ESS-2025-01

EAC Project Number: ESSEVS7000

Document Version: 04

Date: 08/17/2026

U.S. Election Assistance Commission

VSTL

EAC Lab Code 1501



TESTING
NVLAP LAB CODE 200978-0

Disclaimer: The test report and test results resulting from this test plan must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the U.S. Government.

SIGNATURES

Approved by:

Michael L. Walker

Michael L. Walker, VSTL Program Manager

08/17/2026

Date

Approved by:

Wendy Owens

Wendy Owens, VSTL Program Director

08/17/2026

Date

Approved by:

Stacey Glover

Stacey Glover, QA Manager

08/17/2026

Date

Pro V&V attests to the following: 1) all testing prescribed by the approved and published test plan or amended test plan will be performed as identified or the divergence from the test plan will be properly documented in the resulting test report, 2) all identified voting system anomalies or failures will be reported and resolved, and 3) the resulting test report will be accurate and complete. There will be no opinions or interpretations included in the resulting report, except as noted under 'Recommendations'.

REVISIONS

Revision	Description	Date
00	Initial Release	05/11/2026
01	Changes made per comments from the EAC	06/16/2026
02	Changes made per comments from the EAC	07/13/2026
03	Changes made per comments from the EAC	07/21/2026
04	Changes made per comments from the EAC	08/17/2026

TABLE OF CONTENTS

SECTION I: INTRODUCTION.....	1
Section I.1 References.....	1
Section I.2 Terms and Abbreviations.....	2
Section I.3 Target of Evaluation Description.....	3
Section I.3.1 System Overview.....	3
Section I.3.1.1 Block Diagram.....	4
Section I.3.1.2 System Limits	6
Section I.3.1.3 Supported Languages.....	6
Section I.3.1.4 Supported Functionality.....	6
Section I.4 Scope of Testing	7
Section I.5 Testing Responsibilities.....	13
Section I.6 Third Party Tests.....	14
SECTION II: PRE-CERTIFICATION TESTING AND ISSUES	15
Section II.1 Evaluation of Prior VSTL Testing	15
Section II.2 Evaluation of Prior Non-VSTL Testing	15
Section II.3 Known Field Issues	15
SECTION III: MATERIALS REQUIRED FOR TESTING.....	15
Section III.1 Software	16
Section III.2 Hardware/Equipment	19
Section III.3 Materials/Consumables	19
Section III.4 Proprietary Data	20
SECTION IV: TEST SPECIFICATIONS.....	20
Section IV.1 Requirements	20
Section IV.2 Test Case Development and Design	21
Section IV.2.1 Hardware Environmental Test Case Design	21
Section IV.2.2 Software Module Test Case Design and Data	21
Section IV.2.3 Software Functional Test Case Design and Data.....	22
Section IV.2.4 System-Level Test Case Design	22
Section IV.3 Test Procedure Development and Validation	23

SECTION V: TEST PROCEDURES.....	23
Section V.1 Physical Configuration Audit (PCA)	23
Section V.2 Technical Data Package (TDP) Review	24
Section V.3 Source Code Review	27
Section V.4 Functional Configuration Audit (FCA).....	28
Section V.5 Security Review	29
Section V.6 Vulnerability Testing.....	31
Section V.7 Cryptographic Testing.....	32
Section V.8 Usability Review	32
Section V.9 Accessibility Review.....	33
Section V.10 System Integration Testing.....	33
Section V.11 Accuracy Test.....	34
Section V.12 Volume Test	35
Section V.13 Interoperability	36
Section V.14 Hardware Testing	37
Section V.14.1 Electrical Hardware Testing.....	38
Section V.14.2 Operational Hardware Testing	40
Section V.14.3 Non-Operational Hardware Testing	40
Section V.15 Product Safety Review	42
SECTION VI: TEST DATA	43
Section VI.1 Test Data Recording	43
Section VI.2 Test Data Criteria.....	43
Section VI.3 Test Data Reduction.....	43
SECTION VII: TEST CONDITIONS	44
Section VII.1 Facility Requirements.....	44
Section VII.2 Test Set-Up.....	44
Section VII.3 Test Sequence	44
SECTION VIII: TEST OPERATIONS PROCEDURES.....	45
APPENDIX A: PROJECT SCHEDULE	46

SECTION I: INTRODUCTION

The purpose of this Certification Test Plan is to document the procedures and test approach Pro V&V, Inc. will follow to perform certification testing during a new system test campaign on the Election Systems & Software (ES&S) Voting System (EVS) 7.0.0.0 (hereinafter referred to as ‘EVS 7000’) against the requirements set forth for voting systems in the U.S. Election Assistance Commission (EAC) Voluntary Voting System Guidelines (VVSG) Version 2.0. Certification testing of the ES&S EVS 7000 will be performed to ensure the applicable requirements of VVSG 2.0 and the EAC Testing and Certification Program Manual, Version 3.0 are met. Additionally, all EAC Request for Interpretations (RFI) and Notices of Clarification (NOC) relevant to the system under test will be incorporated in the test campaign.

Prior to submitting the voting system for testing, ES&S submitted the application package to the EAC for certification of the EVS 7000. The application was accepted by the EAC, and the project was assigned the unique Project Number of ESSEVS7000.

A Certification Test Report documenting the results of all testing performed as part of this test campaign, including any deviations from the published Test Plan, along with a recommendation for system certification, will be submitted to the EAC for consideration and review at test conclusion.

SECTION I.1 REFERENCES

- Election Assistance Commission (EAC) Voluntary Voting System Guidelines (VVSG) Version 2.0, “Principles and Guidelines” and “Requirements”
- Voluntary Voting System Guidelines Version 2.0 Test Assertions, Version 1.3 (Hardware Testing) Test Assertions, Version 1.4
- Election Assistance Commission (EAC) Voting System Testing and Certification Program Manual, Version 3.0
- Election Assistance Commission (EAC) Voting System Test Laboratory Program Manual, Version 3.1
- National Voluntary Laboratory Accreditation Program NIST Handbook 150, 2020 Edition, “NVLAP Procedures and General Requirements (NIST Handbook 150)”
- National Voluntary Laboratory Accreditation Program NIST Handbook 150-22, 2021 Edition, “Voting System Testing (NIST Handbook 150-22-2021)”
- United States 107th Congress Help America Vote Act (HAVA) of 2002 (Public Law 107-252), dated October 2002
- Pro V&V, Inc. Quality Assurance Manual
- EAC Requests for Interpretation (RFI) and Notices of Clarification (NOC) (listed on www.eac.gov)

- ES&S EVS 7000 EAC Application Approval Letter, dated 03/13/2026
- ES&S EVS 7000 Technical Data Package (*A listing of the ES&S EVS 7000 documents submitted for this test campaign is listed Table V-1 of this Test Plan.*)

SECTION I.2 TERMS AND ABBREVIATIONS

This subsection lists terms and abbreviations relevant to the hardware, the software, or this Test Plan.

- “ADA” – Americans with Disabilities Act 1990
- “ATI” – Audio-Tactile Interface
- “BMD” – Ballot Marking Device
- “CF” – Compact Flash
- “CM” – Configuration Management
- “COTS” – Commercial Off-The-Shelf
- “CVR” – Cast Vote Record
- “EAC” – United States Election Assistance Commission
- “EMS” – Election Management System
- “FCA” – Functional Configuration Audit
- “HAVA” – Help America Vote Act
- “NOC” – Notice of Clarification
- “NIST” – National Institute of Standards and Technology
- “NVLAP” – National Voluntary Laboratory Accreditation Program
- “PCA” – Physical Configuration Audit
- “QA” – Quality Assurance
- “RFI” – Request for Interpretation
- “TDP” – Technical Data Package
- “UPS” – Uninterruptible Power Supply
- “VSTL” – Voting System Test Laboratory
- “VVSG” – Voluntary Voting System Guidelines

SECTION I.3 TARGET OF EVALUATION DESCRIPTION

The system submitted for certification testing is described in the following subsections. All information presented was derived from the System Overview and/or other documents contained in the TDP.

EVS 7000 is composed of software applications, a polling place device with accompanying firmware, and COTS hardware and software. EVS 7000 is comprised of the following primary components: Election Navigator, Election Management Software (Election Navigator), and ExpressVote XL, Full-Face Universal Voting System (ExpressVote XL).

Functional subsystems of EVS 7000 include: Admin, Election, Ballot Design, Media Management, Tabulation, Election Night Results, and Post Election.

SECTION I.3.1 SYSTEM OVERVIEW

EVS 7000 primary components:

Election Navigator

Election Management System (EMS) software used for defining contests, candidates and ballot formats and performing post-election results processing, including results consolidation and reporting.

ExpressVote XL

Universal voting system that supports voting and tabulation functions for all voters, with independent voter verifiable paper record which is digitally scanned for tabulation on the ExpressVote XL. The Universal Voting Console (UVC) is an audio tactile keypad and ADA support peripheral for use with the ExpressVote XL.

EVS 7000 functional subsystems:

Admin

The Admin subsystem enables election administrators to install and configure the system, manage user access through role-based permissions, and define the political geography that underpins ballot generation and voter eligibility. Jurisdictions can create and maintain district groups, districts, precincts, split precincts, and polling locations, ensuring that every voter receives the correct ballot style and is assigned to the appropriate voting site. This subsystem houses a centralized system library and configurable parameters that streamline data entry and standardize operations across elections. In addition, the Admin subsystems provide comprehensive audit logging, allowing election administrators to monitor user activity, review system events and export logs for external analysis or archival purposes.

Election

The Election subsystem allows election administrators to manage existing elections and create new elections.

Ballot Design

Election administrators use Ballot Design to format machine ballot display options that support the ExpressVote XL screen layout.

Media Management

Media Management in Election Navigator allows election administrators to prepare USB flash drives with poll-specific election data. This module ensures each voting location receives the correct configuration before polls open.

Tabulation

Marked vote summary cards are scanned for tabulation at the polling place using the ExpressVote XL. Tabulators save poll or precinct-level results to a USB flash drive.

Election Night Results

The Load Results module in Election Night Results is where elections administrators import and process results from USB flash drives. Users can view election results and statistics, create and manage results reports, and generate results reports in CSV format.

Post Election

Post Election supports ballot review and data export. It provides tools for reviewing ballots, managing write-in votes and generating CDF data exports, including election results, EMS audit log, machine log and cast vote records.

SECTION I.3.1.1 BLOCK DIAGRAM

End-to-end functionality and system configuration of EVS 7000 are depicted in Figures I-1 and I-2, respectively.

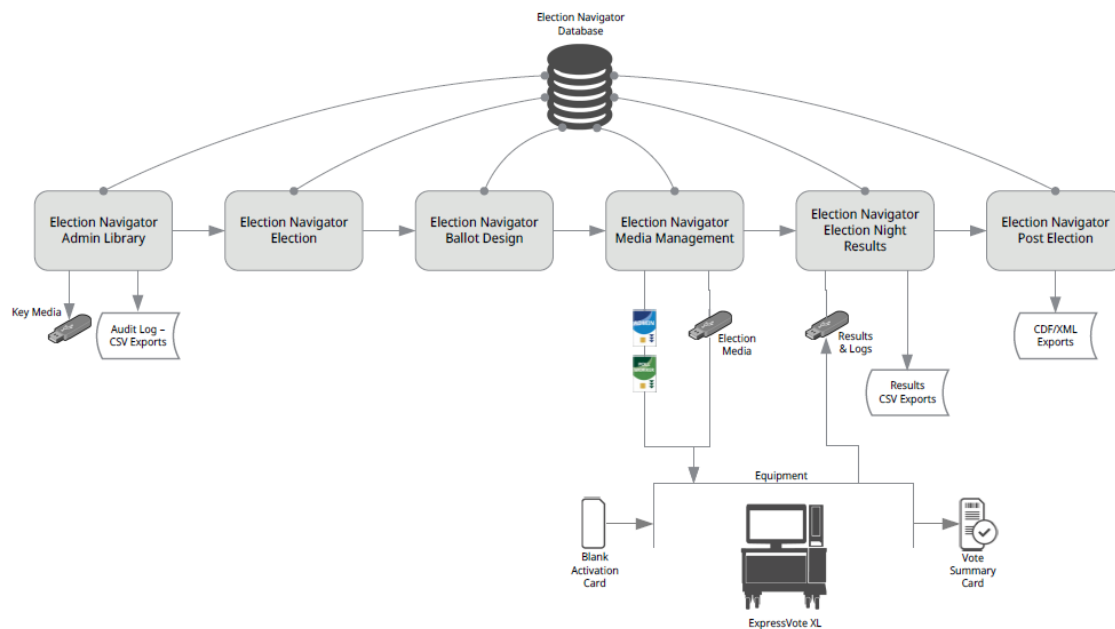


Figure I-1 EVS 7000 Functional Diagram

SECTION I.3.1.2 SYSTEM LIMITS

ES&S has defined the following performance characteristic limits and device capacities for EVS 7000 components:

Table I-1 EVS 7000 Voting System Limits

<i>Note: per the System Overview, the system limitations listed are defined for certification testing purposes. The architectural limits of this voting system exceed the stated limits.</i>		
System Characteristic	Limiting System Component	Boundary or Limitation
Max. precincts in an election	ExpressVote XL vote summary card	2,000
Max. ballot styles	ExpressVote XL vote summary card	2,000
Max. contests per ballot style	ExpressVote XL vote summary card	30
Max. 'vote for' per contest	ExpressVote XL vote summary card	30
Max. candidates (ballot choices) per contest	ExpressVote XL vote summary card	230
Max. number of parties	ExpressVote XL vote summary card	General election: 75 Primary election: 30
The voting system supports the following ballot sizes and scan rates:		
Ballot Size	Product	Scan Rate
4.25" x 17"	ExpressVote XL	Between 5 to 15 seconds

SECTION I.3.1.3 SUPPORTED LANGUAGES

Per the *System Overview*, EVS 7000 can display and print content that supports the following languages: English, Spanish, Chinese, and Vietnamese.

SECTION I.3.1.4 SUPPORTED FUNCTIONALITY

EVS 7000 is designed to support the following voting variations: General election, closed primary, precinct splits, write-in contest options, write-in reconciliation, partisan offices, non-partisan offices, and no candidate has filed.

During the test campaign, Pro V&V will execute tests designed to verify EVS 7000:

- Provides the capability to define and identify contests, contest options, candidates, and ballot questions using all voting variations identified by ES&S.
- Records contest selection information in the CVR that includes all contest selections made by the voter for all supported vote variations.
- Supports the tabulation function for all voting variations.

SECTION I.4 SCOPE OF TESTING

VVSG 2.0 consists of fifteen (15) Principles and fifty-three (53) Guidelines. Together, these Principles and Guidelines cover voting system design, development, and operations. Derived from the Principles and Guidelines are the VVSG 2.0 Requirements. The Requirements contain terms describing function, design, documentation, and testing attributes of voting system hardware, software, and telecommunications. Test Assertions, developed and published by the EAC, containing granular conditions that must be tested to determine conformance to specific requirements, will be utilized when developing VSTL Test Cases.

As a new system, the EVS 7000 will be evaluated against all applicable requirements contained in the principles and guidelines. To accomplish this, Pro V&V has defined multiple test areas relevant to each Principle. Tests will be executed within each test area to evaluate the applicable Requirements. Table I-2 details the VVSG 2.0 Principles, Guidelines, and associated test areas.

Table I-2 VVSG 2.0 Test Areas

VVSG 2.0 Guideline	VSTL Test Areas
Principle 1: High Quality Design <i>The voting system is designed to accurately, completely, and robustly carry out election processes.</i>	
1.1 - The voting system is designed using commonly accepted election process specifications.	FCA, Accuracy Test, System Integration Testing, TDP Review, Volume Test, Electrical Hardware Testing, Security Tests
1.2 - The voting system is designed to function correctly under real-world operating conditions.	
1.3 - Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not.	
Principle 2: High Quality Implementation <i>The voting system is implemented using high quality best practices.</i>	
2.1 - The voting system and its software are implemented using trustworthy materials and best practices in software development.	Source Code Review, TDP Review, FCA, Security Tests, Electrical Hardware Testing, Operational Environmental Hardware Testing, Non-Operational Environmental Hardware Testing
2.2 - The voting system is implemented using best practice user-centered design methods that consider a wide range of representative voters, including those with and without disabilities, and election workers.	
2.3 - Voting system logic is clear, meaningful, and well-structured.	
2.4 - Voting system structure is modular, scalable, and robust.	
2.5 – The voting system supports system processes and data with integrity.	

Table I-2 VVSG 2.0 Test Areas *(continued)*

VVSG 2.0 Guideline	VSTL Test Areas
2.6 - The voting system handles errors robustly and gracefully recovers from failure. 2.7 - The voting system performs reliably in anticipated physical environments.	
Principle 3: Transparent <i>The voting system and voting processes are designed to provide transparency.</i>	
3.1 - The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood. 3.2 - The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection. 3.3 - The public can understand and verify the operations of the voting system throughout the entirety of the election.	TDP Review, Usability, FCA, System Integration Testing
Principle 4: Interoperable <i>The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.</i>	
4.1 - Voting system data that is imported, exported, or otherwise reported, is in an interoperable format. 4.2 - Standard, publicly available formats for other types of data are used, where available. 4.3 - Widely-used hardware interfaces and communications protocols are used. 4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.	Interoperability, TDP Review, FCA, System Integration Testing, PCA
Principle 5: Equivalent and Consistent Voter Access <i>All voters can access and use the voting system regardless of their abilities.</i>	
5.1 - Voters have a consistent experience throughout the voting process within any method of voting. 5.2 - Voters receive equivalent information and options in all modes of voting	Usability, Accessibility, FCA, TDP Review
Principle 6: Voter Privacy <i>Voters can mark, verify, and cast their ballot privately and independently.</i>	
6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections. 6.2 - Voters can mark, verify, and cast their ballot or other associated cast vote record, without assistance from others	Usability, Accessibility, FCA, TDP Review

Table I-2 VVSG 2.0 Test Areas *(continued)*

VVSG 2.0 Guideline	VSTL Test Areas
Principle 7: Marked, Verified, and Cast as Intended <i>Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.</i>	
7.1 - The default voting system settings present a ballot usable for the widest range of voters, and voters can adjust settings and preferences to meet their needs. 7.2 - Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes and selections. 7.3 - Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.	Usability, Accessibility, FCA, TDP Review
Principle 8: Robust, Safe, Usable, and Accessible <i>The voting system and voting processes provide a robust, safe, usable, and accessible experience.</i>	
8.1 - The voting system's hardware, software, and accessories are robust and do not expose users to harmful conditions. 8.2 - The voting system meets currently accepted federal standards for accessibility. 8.3 - The voting system is evaluated for usability with a wide range of representative voters, including those with and without disabilities. 8.4 - The voting system is evaluated for usability with election workers.	Usability, Accessibility, FCA, TDP Review
Principle 9: Auditable <i>The voting system is auditable and enables evidence-based elections.</i>	
9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results. 9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities. 9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. 9.4 - The voting system supports efficient audits.	Source Code Review, TDP Review, FCA, Security Tests, Accuracy, Interoperability, Accessibility, Cryptographic Testing
Principle 10: Ballot Secrecy <i>The voting system protects the secrecy of voters' ballot selections.</i>	
10.1 - Ballot secrecy is maintained throughout the voting process.	FCA, Usability, Accessibility, TDP Review, Security Tests, Cryptographic Testing

Table I-2 VVSG 2.0 Test Areas *(continued)*

VVSG 2.0 Guideline	VSTL Test Areas
10.2 - The voting system does not contain nor produce records, notifications, information about the voter, or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.	
Principle 11: Access Control <i>The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.</i>	
11.1 - The voting system enables logging, monitoring, reviewing, and modifying of access privileges, accounts, activities, and authorizations. 11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access. 11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. 11.4 - The voting system's default access control policies enforce the principles of least privilege and separation of duties. 11.5 - Logical access to voting system assets are revoked when no longer required	Security Testing, Vulnerability Testing, FCA
Principle 12: Physical Security <i>The voting system prevents or detects attempts to tamper with voting system hardware.</i>	
12.1 - The voting system supports mechanisms to detect unauthorized physical access. 12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.	Security Testing, Vulnerability Testing, FCA, TDP Review, Penetration Testing
Principle 13: Data Protection <i>The voting system protects data from unauthorized access, modification, or deletion.</i>	
13.1 - The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. 13.2 - The source and integrity of electronic tabulation reports are verifiable. 13.3 - All cryptographic algorithms are public, well-vetted, and standardized.	Security Tests, FCA, TDP Review, Cryptographic Testing

Table I-2 VVSG 2.0 Test Areas *(continued)*

VVSG 2.0 Guideline	VSTL Test Areas
13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.	
Principle 14: System Integrity <i>The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.</i>	
14.1 - The voting system uses multiple layers of controls to provide resilience against security failures or vulnerabilities. 14.2 - The voting system is designed to limit its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls. 14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components. 14.4 - Voting system software updates are authorized by an administrator prior to installation.	Security Tests, Penetration Testing, TDP Review, Source Code Review, Vulnerability Testing, Cryptographic Testing, FCA
Principle 15: Detection and Monitoring <i>The voting system provides mechanisms to detect anomalous or malicious behavior.</i>	
15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing. 15.2 - The voting system generates, stores, and reports all error messages as they occur. 15.3 - The voting system is designed to protect against malware. 15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.	Security, FCA, Vulnerability Testing, Penetration Testing, TDP Review

Pro V&V determined the Requirements listed below are not applicable or not supported. These Requirements include the following:

- 1.1.1-L – Ballot rotation, Election definition Partisan open primary ballot
- 1.1.4-D – Ballot rotation, Casting
- 1.1.4-F – Partisan open primary ballot
- 1.1.4-G – Indicate party affiliations and endorsements
- 1.1.4-K – Straight-party voting, Casting
- 1.1.4-L – Cumulative voting contest. Casting
- 1.1.4-M – Ranked choice voting contest, Casting

- 1.1.4-N – Party preference contest
- 1.1.4-O – Top-2 primary contest (blanket primary contest)
- 1.1.4-P – Presidential delegate contest, Casting
- 1.1.4-Q – Proportional voting contest (equal-and-even cumulative voting contest), Casting
- 1.1.4-R – Group voting contest, Casting
- 1.1.4-S – Top-2 IRV contest (supplementary or contingent vote contest)
- 1.1.6-C – Ballot separation when batch feeding
- 1.1.6-H – Accurately detect imperfect marks
- 1.1.6-I – Ignore extraneous marks inside voting targets
- 1.1.6-J – Marginal marks, without bias
- 1.1.6-K – Repeatability
- 1.1.8-B.2 – Tabulation of an open primary ballot
- 1.1.8-B.3 – Open primary ballot with party preference contest
- 1.1.8-D – Ballot rotation, Tabulation
- 1.1.8-E – Straight-party voting, Tabulation
- 1.1.8-F – Cross-party endorsement with straight-party voting
- 1.1.8-I – Cumulative voting contest, Tabulation
- 1.1.8-J – Ranked choice voting contest, Tabulation
- 1.1.8-K – Group voting contest, Tabulation
- 1.1.8-L – Presidential delegate contest, Tabulation
- 1.1.8-N – Proportional voting contest (equal-and-even cumulative voting contest), Tabulation
- 1.1.9-I – Ranked choice voting, report results
- 7.2-E – Touch screen gestures
- 7.2-F – Voter Speech
- 7.2-J – Paper ballot target areas
- 8.1-D – Secondary ID and biometrics
- 8.1-G – Telephone style handset
- 9.1.6 – Cryptographic E2E verifiable
- 9.1.6-A – Verified cryptographic protocol
- 9.1.6-B – Independent evaluation of E2E cryptographic protocol implementation
- 9.1.6-C, 9.1.6-C.1, 9.1.6-C.2 – Cryptographic ballot selection verification by voter
- 9.1.6-D, 9.1.6-D.1, 9.1.6-D.2 – Methods for cryptographic ballot selection verification
- 9.1.6-E, 9.1.6-E.1, 9.1.6-E.2, 9.1.6-E.3, 9.1.6-E.4, 9.1.6-E.5 – Ballot receipt

9.1.6-F – Disputes involving ballot receipts
9.1.6-G, 9.1.6-G.1, 9.1.6-G.2– Evidence export
9.1.6-H– Mandatory ballot availability
9.1.6-I, 9.1.6-I.1, 9.1.6-I.2 – Verification of encoded vote documentation
9.1.6-J, 9.1.6-J.1, 9.1.6-J.1.a, 9.1.6-J.1.b, 9.1.6-J.2 – Verifier reference implementation
9.1.6-K – Privacy preserving, universally verifiable ballot tabulation
9.4-D – Multipage ballots
10.2.1-B – Indirect voter associations
10.2.1-C – Use of indirect voter associations
10.2.1-D – Isolated storage location
10.2.1-E – Removal of indirect voter associations
10.2.1-F – Confidentiality for ballots with indirect voter associations
10.2.4-B – Voting information in receipts
10.2.4-C – Activation device records
13.3-B – E2E cryptographic voting protocols
15.4-D – Rule and policy updates

Additionally, a *VVSG 2.0 Cross Reference Matrix* specific to the EVS 7000 will be utilized during the test campaign to ensure that all applicable VVSG 2.0 requirements are addressed.

SECTION 1.5 TESTING RESPONSIBILITIES

Testing responsibilities and associated project tasks for this test campaign, including the VSTL personnel who will be responsible for each identified task and a detailed project schedule, are contained in the Project Schedule located in Appendix A. The Project Schedule allows for test case development, test procedure development and validation, and performance of any required third-party tests. The Project Schedule also identifies EAC and manufacturer dependencies for the test campaign. The dates on the schedule are not firm dates, but planned estimates based on the anticipated project workflow.

Owner Assignments

Responsibility for the administration and execution of this test project is assigned to qualified Pro V&V personnel. All testing activities will be conducted in accordance with the applicable requirements and the internal quality procedures of the accredited test laboratory. Personnel assigned to this project: 1) possess the appropriate training, technical qualifications, and experience necessary to perform voting system testing, 2) will perform their duties in accordance with the procedures, quality controls, and independence requirements defined by Pro V&V, and 3) operate independently of the voting system manufacturer and perform their duties in accordance with the independence and conflict-of-interest requirements applicable to accredited VSTLs.

Roles and responsibilities are defined as follows:

Program Manager: The Program Manager is responsible for the overall administration and oversight of the test project. This includes planning and coordination of testing activities, assignment of personnel and resources, monitoring of schedule and progress, and ensuring that testing is conducted in accordance with the approved test plan and applicable requirements. The Program Manager is also responsible for reviewing and approving test artifacts, resolving escalated issues, and ensuring that test results and reports are complete and accurate.

For this campaign, Michael Walker, the Pro V&V VSTL Program Manager, will be responsible for oversight of all testing activities.

Project Manager/Lead Test Engineers: Testing activities will be performed by Pro V&V Project Managers/Test Engineers with oversight from the Program Manager. All Test Engineers are qualified and trained in election system testing. Test Engineers are responsible for executing test procedures, documenting results, identifying and reporting anomalies, and maintaining accurate records of all testing activities. Test Engineers may also assist with test environment setup, configuration verification, and other supporting technical tasks necessary to complete the test campaign.

Each area of testing will be conducted by personnel with specific qualifications and training relevant to the type of testing being performed. Activities such as source code review will be carried out by test engineers who are trained and experienced in secure code analysis and code review methodologies. Security testing will be performed by test engineers who possess the appropriate certifications, technical expertise, and practical experience required to conduct comprehensive security assessments. Other specialized testing activities will likewise be assigned to engineers with demonstrated competency in the applicable discipline. Where testing requires independent validation of hardware components or other specialized capabilities, the work will be performed by vetted and approved third-party laboratories that meet the required technical and quality standards.

Quality and Documentation Support (as applicable): Additional support personnel may assist with quality assurance, documentation management, configuration control, and administrative coordination to ensure that all testing activities and deliverables meet organizational quality standards and program documentation requirements.

SECTION I.6 THIRD PARTY TESTS

Pro V&V will utilize third-party test facilities for performance of the electrical and environmental tests. Environmental and Electrical Hardware Testing will be performed at the Element Longmont facility located in Longmont, Colorado. All testing will be witnessed on-site by Pro V&V personnel, except for the Operational Environmental Hardware Testing (Continuous Operation – Varied Environmental Conditions) in which Pro V&V qualified staff will execute all testing.

SECTION II: PRE-CERTIFICATION TESTING AND ISSUES

This section describes any previous testing performed prior to submitting the voting system to the EAC.

SECTION II.1 EVALUATION OF PRIOR VSTL TESTING

EVS 7000 is a new voting system that has not previously been tested in the EAC Program. Full functional and hardware testing will be performed on the system and a complete TDP review will be performed on all submitted documentation.

Prior to approval of the application for testing, the EVS 7000 was subjected to Penetration Testing in accordance with Section 4.5 of the *EAC Voting System Testing and Certification Program Manual, Version 3.0*. The purpose of the test was to assess the security posture of the EVS 7000 prior to entering the EAC's Testing & Certification program. Penetration Testing was conducted in two phases: Phase I (Pre-Testing Assessment) and Phase II (Penetration Testing). The penetration testing report including identified vulnerabilities and risk ratings, as well as guidance on how to mitigate the discovered weaknesses, was then submitted to the EAC as part of the Test Readiness Review (TRR).

Pro V&V performed the Penetration Testing utilizing the Penetration Phases outlined in NIST Special Publication 800-115, *“Guide to Information Security Testing and Assessment Section 5.2: Penetration Testing”*.

SECTION II.2 EVALUATION OF PRIOR NON-VSTL TESTING

No prior non-VSTL testing of EVS 7000 was considered for this test campaign.

SECTION II.3 KNOWN FIELD ISSUES

The EVS 7000 is being submitted for evaluation as a new system that has not been fielded; therefore, there are no fielded systems preceding this system. The EVS 7000 may serve as the baseline to subsequent systems submitted for evaluation in the future. At that time, any known field issues on the baseline system or any subsequent certified versions derived from the EVS 7000 system will be addressed in the associated published test plans.

SECTION III: MATERIALS REQUIRED FOR TESTING

The section lists all materials needed to enable the test engagement to occur.

The materials required for testing EVS 7000 include all materials to enable the test campaign to occur. This includes the applicable hardware and software as well as the TDP and test support materials, as described in the following subsections.

SECTION III.1 SOFTWARE

This subsection lists the proprietary and COTS software provided by the manufacturer as part of the test campaign.

EVS 7000 includes the following software: Election Navigator (version 7.0.0.0).

Election Navigator is Election Management System (EMS) software used for defining contests, candidates and ballot formats and performing post-election results processing, including results consolidation and reporting. Election Navigator includes the following software items:

Table III-1 Election Navigator Software Items

Software	Proprietary or COTS	Written in-house	Procured and not modified	Procured and modified	Modification to Software	Modification to Default Configuration Options
Election Navigator API Version 7.0.0.0	Proprietary	✓			No modifications	Core API Library
Election Navigator UI Version 7.0.0.0	Proprietary	✓			No modifications	Core UI Application
Microsoft SQL Server 2022 (RTM-CU16) (KB5048033) - 16.0.4165.4 (X64)	COTS		✓		No modifications	No modification
Microsoft .NET 8.0.22 Runtime	COTS		✓		No modifications	No modification
Keycloak 26.3.2	COTS		✓		No modifications	Customized to match ES&S standards

Table III-2 ExpressVote XL Software Items

Software	Proprietary or COTS	Written in-house	Procured and not modified	Procured and modified	Description of Modification to Software and Default Configuration Options
Reusable Tabulator User Interface Component v7.0.0.0	Proprietary	✓			No modifications
Rules and Tabulation Engine Component V7.0.0.0	Proprietary	✓			No modifications

Table III-2 ExpressVote XL Software Items *(continued)*

Software	Proprietary or COTS	Written in-house	Procured and not modified	Procured and modified	Description of Modification to Software and Default Configuration Options
Common Controller Process Component V7.0.0.0	Proprietary	✓			No modifications
Image Processing Engine Component V7.0.0.0	Proprietary	✓			No modifications
Poll Media Information Service Component v7.0.0.0	Proprietary	✓			No modifications
Cryptographic Library v7.0.0.0	Proprietary	✓			No modifications
Expat 2.5.0	COTS		✓		No modifications
Ncurses 6.3+20220423	COTS		✓		No modifications
Readline 8.12	COTS		✓		No modifications
xtst 1.5.2	COTS		✓		No modifications
ICU 71.1	COTS		✓		No modifications
GraphicsMagick 1.3.25	COTS		✓		No modifications
Libusb1-1.0.26	COTS		✓		No modifications
WebsocketPP 0.8.2	COTS		✓		No modifications
Openssl 3.0.8	COTS		✓		No modifications
Openssl-FIPS 3.0.8	COTS		✓		No modifications
Boost 1.78	COTS		✓		No modifications
tiff 4.3.0	COTS		✓		No modifications
Jsoncpp 1.9.5	COTS		✓		No modifications
Xerces C 3.1.4	COTS		✓		No modifications
Freetype 2.11.1	COTS		✓		No modifications
KeyPair Cryptographic Module for OpenSSL (3.0.8 Certificate 4811)	COTS		✓		No modifications
TypeScript 5.5.4	COTS		✓		No modifications
QtWebengine 6.72	COTS		✓		No modifications
Angular 17.2.4	COTS		✓		No modifications
libppmScanAPI 1.0.4.1	COTS		✓		No modifications
PPM Interface 3.37	COTS		✓		No modifications

Table III-3 Compilers and Assemblers

Software	Description	Software Requirements Performed by the Client
GNU Compiler Collection - GCC 11.4.0	Compiler Tool	Compiles Tabulation Layer tools from text-based source files for use by Linux.
TypeScript v5.5.4	Graphical User Interface / Compiler Tool	Designed for development of large applications and transcompiles to JavaScript.

Table III-4 Interface Identification

Software	Interfaces to	Provides Data To	Receives Data From	Details/Notes
Reusable Tabulator User Interface Component	– Common Controller Process	✓	✓	Uses JSON socket process to communicate between components.
Rules and Tabulation Engine Component	– Common Controller Process – Image Processing Engine	✓	✓	Uses JSON socket process to communicate between components.
Common Event Log Service Component	– Common Controller Process – Image Processing Engine – Linux OS – Reusable Tabulator User Interface	✓	✓	Uses JSON socket process to communicate between components and implements election rules.
Poll Media Information Service Component	– Common Controller Process – Image Processing Engine – Cryptographic Library – Linux OS	✓	✓	Uses JSON socket process to communicate between components
Linux OS Component	– Common Controller Process – Cryptographic Library – Poll Media Information Service	✓	✓	Uses JSON socket process to communicate between components and provides programming access to the hardware.
Image Processing Engine	– Rules and Tabulation Engine – Image Processing Engine – Linux OS – Common Controller Process	✓	✓	Uses JSON socket process to communicate between components

Table III-4 Interface Identification *(continued)*

Software	Interfaces to	Provides Data To	Receives Data From	Details/Notes
Common Controller Process Component	- Cryptographic Library - Common Event Log Service - Rules and Tabulation Engine - Image Processing Engine - Linux OS - Reusable Tabulator User Interface	✓	✓	Uses JSON socket process to communicate between layers.

SECTION III.2 HARDWARE/EQUIPMENT

This subsection lists the proprietary and COTS equipment to be provided by the manufacturer as part of the test campaign.

EVS 7000 includes the following hardware: ExpressVote XL Full-Face Universal Voting System (ExpressVote XL) version 7.0.0.0.

The main assembly of the device is the complete ExpressVote XL. It is constructed of three primary subassemblies:

- ExpressVote XL tablet
- ExpressVote XL cart
- ExpressVote XL paper path module (PPM)

In addition to the main assembly, the following ancillary components are included:

- Universal Voting Console (UVC)
- Headphones
- Sip and Puff
- Vote session lamp

SECTION III.3 MATERIALS/CONSUMABLES

This subsection lists the materials and consumables required by the system being evaluated to be provided by the manufacturer as part of the test campaign.

Table III-5 EVS 7000 Materials/Consumables

Material	Description
Plastic Locks	Tamper Evident Lock for the ExpressVote XL, such as Spring Lok Seal
Plastic Locks	USB cable and RJ45 locks, such as Padjack Cable Lock and Seal and PadJack SVE RJ45 Lock
Tamper Evident Security Seals	Adhesive tamper evident security seal, such as Rifkin part# S93313-07
Smart Cards	Programmable Smart Cards for voters, poll workers, and technicians for the ExpressVote XL
Paper Rolls	Replacement Thermal Paper Rolls for the ExpressVote XL
Disposable Straws	Disposable straws for use with the Sip & Puff
Card Stock	Card Paper Stock for printing ExpressVote XL cards
A/C Power Cables	3-Prong A/C Power Cables
USB Thumb drives	Delkin USB Thumb drives

SECTION III.4 PROPRIETARY DATA

All data and documentation considered by the manufacturer to be proprietary will be identified and documented in an independent submission along with a Notice of Protected Information.

SECTION IV: TEST SPECIFICATIONS

Certification testing of the EVS 7000 submitted for evaluation will be performed to ensure the applicable requirements of the VVSG 2.0, the VVSG 2.0 Test Assertions, Version 1.4 (or current), and the EAC Testing and Certification Program Manual, Version 3.0, are met. Additionally, all EAC Request for Interpretations (RFI) and Notices of Clarification (NOC) relevant to the system under test will be incorporated in the test campaign. A complete listing of the EAC RFIs and NOCs is available on the EAC website.

SECTION IV.1 REQUIREMENTS

To evaluate the EVS 7000 test requirements, each Principle of the VVSG 2.0 will be analyzed in conjunction with a preliminary TDP review to determine the applicable Requirements. The preliminary TDP is performed to gather information concerning the system under test and its capabilities or design intentions. Additionally, a TDP review will be performed throughout the test campaign. The TDP Review includes the Initial Review, the Regulatory/Compliance Review, and the Final Review. This review is conducted to determine if the submitted technical documentation meets the regulatory, customer-stated, or end-user requirements and includes reviewing the documents for stated functionality review and verification.

The Pro V&V designated Test Areas utilized to evaluate the EVS 7000 to the requirements set forth in the VVSG 2.0 are described in the subsections that follow.

SECTION IV.2 TEST CASE DEVELOPMENT AND DESIGN

For each test area, Pro V&V will utilize baseline test cases augmented with specially designed test cases tailored to the specific design of the EVS 7000. Additionally, specific election definitions will be designed for the Operational Status Check, Volume & Stress Test, and the Logic & Accuracy Tests.

Test cases are designed based on the manufacturer's design specifications and the relevant technical requirements set forth by the VVSG 2.0. Test cases shall be based on the following aspects of the voting system: Hardware qualitative examination design, Hardware environmental test case design, Software module test case design and data, Software functional test case design, and System level test case design. Test cases shall provide information regarding the sequence of actions to be performed for the execution of a test, the requirements being met, the test objective, test configuration, equipment needed, special requirements, assumptions, and pass/fail criteria.

Once the test cases are finalized, they will be validated and published for use in the test campaign. The validation of the test case will be accomplished by technical review and approval. This validation will include the following: confirmation of adequate test coverage of all requirements; confirmation that test case results are not ambiguous and gave objective pass/fail criteria; and confirmation that any automated test suites will produce valid results. All ES&S submitted test cases will be reviewed and validated by Pro V&V.

SECTION IV.2.1 HARDWARE ENVIRONMENTAL TEST CASE DESIGN

No previous examinations have been performed on the EVS 7000. The voting system hardware shall be subjected to the tests specified in Section V.14. Testing will be performed by personnel verified by Pro V&V to be qualified to perform the test. Pro V&V will utilize a third-party test facility for performance of the electrical and environmental tests. All pre and post operational status checks shall be conducted by Pro V&V personnel.

SECTION IV.2.2 SOFTWARE MODULE TEST CASE DESIGN AND DATA

Pro V&V will review the manufacturer's program analysis, documentation, and module test case design and shall evaluate the test cases for each module with respect to flow control parameters and entry/exit data. Pro V&V will design additional test cases to as needed to satisfy all specified coverage criteria. Component Level Testing will be implemented during the FCA for each component and subcomponent. During the source code review, compliance builds, and security testing, Pro V&V will utilize limited structural-based techniques (white-box testing). Additionally, specification-based techniques (black-box testing) will be utilized for the individual software components.

Pro V&V shall define the expected result for each test and the ACCEPT/REJECT criteria for certification. If the system performs as expected, the results will be accepted. If the system does not perform as expected, an analysis will be carried out to determine the cause. The test will be repeated in an attempt to reproduce the results.

If the failure can be reproduced and the expected results are not met, the system will have failed the test. If the results cannot be reproduced, the test will continue. All errors encountered will be documented and tracked through resolution.

SECTION IV.2.3 SOFTWARE FUNCTIONAL TEST CASE DESIGN AND DATA

Pro V&V shall review the manufacturer-submitted test plans and data to verify that the individual performance requirements specified in the VVSG 2.0 and the TDP are reflected in the software. As part of this process, Pro V&V shall review the manufacturer's test case design and prepare a detailed matrix of system functions and the test cases that exercise them. Following analysis and validation of the ES&S submitted test cases and technical documentation, Pro V&V will make a determination on any functionality that is not covered or is not thoroughly covered. Pro V&V will then design additional test cases focusing on the functionality under review.

Pro V&V shall also prepare a test procedure describing all test ballots, operator procedures, and the data content of output reports. Pro V&V shall define abnormal input data and operator actions and then design test cases to verify that the system is able to handle and recover from these abnormal conditions. During this review, emphasis shall be placed on those functions where the manufacturer data on module development, such as the system release notes and comments within the source code, reflects significant debugging problems, and on functional tests that resulted in high error rates.

Pro V&V shall define the expected result for each test and the ACCEPT/REJECT criteria for certification. If the system performs as expected, the results will be accepted. If the system does not perform as expected, an analysis will be carried out to determine the cause. The test will be repeated in an attempt to reproduce the results. If the failure can be reproduced and the expected results are not met, the system will have failed the test. If the results cannot be reproduced, the test will continue. All errors encountered will be documented and tracked through resolution.

SECTION IV.2.4 SYSTEM-LEVEL TEST CASE DESIGN

System Level testing will be implemented to evaluate the complete system. This testing will include all proprietary components and COTS components (software, hardware, and peripherals) in a configuration of the system's intended use. For software system tests, the tests shall be designed according to the stated design objective without consideration of its functional specification. The system level hardware and software test cases shall be prepared independently to assess the response of the hardware and software to conditions related to functionality of the system as a whole.

SECTION IV.3 TEST PROCEDURE DEVELOPMENT AND VALIDATION

Pro V&V will utilize internally developed VSTL Test Procedures during the duration of the test campaign. These procedures are developed to the VVSG 2.0 standards and are designed to cover designated test areas. The validation of the VSTL Test Procedures is accomplished by Technical Review and Approval. If necessary and where practical, a validation might include execution to attempt to achieve the expected results using the selected tool of the testing methodology.

For example: a test deck may be created to validate the accuracy test marking pattern and expected results. The entire test would not be executed at that time but utilized to validate the test deck and expected results. Test Procedures and Test Cases will be validated prior to execution. This validation will include the following:

- Confirmation of adequate test coverage of all requirements.
- Confirmation that test case results are not ambiguous and have objective pass/fail criteria.
- Confirmation that any automated test suites will produce valid results.

SECTION V: TEST PROCEDURES

Descriptions of the tests required to evaluate the submitted system to the scope defined in Section I.4 are provided in the sections below.

SECTION V.1 PHYSICAL CONFIGURATION AUDIT (PCA)

The Physical Configuration Audit (PCA) compares the voting system components submitted for evaluation to the manufacturer's technical documentation. The PCA includes the following activities:

- Establish a configuration baseline of software and hardware to be tested; confirm whether the manufacturer's documentation is sufficient for the user to install, validate, operate, and maintain the voting system.
- Verify software conforms to the manufacturer's specifications; inspect all records of manufacturer's release control system; if changes have been made to the baseline version, verify manufacturer's engineering and test data are for the software version submitted for certification.
- Review drawings, specifications, technical data, and test data associated with system hardware (if non-COTS) to establish system hardware baseline associated with software baseline.
- Review manufacturer documents of user acceptance test procedures and data against system's functional specifications; resolve any discrepancy or inadequacy in manufacturer's plan or data prior to beginning system integration functional and performance tests.
- Subsequent changes to baseline software configuration made during testing, as well as system hardware changes that may produce a change in software operation, are subject to re-examination.

The PCA will be conducted in two phases: Initial (to baseline the system prior to test commencement) and Final (to verify final software and hardware configurations).

Additionally, Pro V&V will perform a physical examination of the hardware to determine if any component of the voting system contains any wireless technologies. When applicable, the inspection may include taking off covers and disassembling devices. If such technologies are discovered, Pro V&V will perform an inspection, functional verification, and security evaluation of the noted capability.

SECTION V.2 TECHNICAL DATA PACKAGE (TDP) REVIEW

To determine full compliance with the VVSG 2.0, three phases of TDP review shall be conducted. As part of the review process, Pro V&V will utilize a TDP Review Checklist that contains TDP requirements specified in the VVSG 2.0. Results of the review of each document will be entered on the TDP Review Checklist and reported to the manufacturer for disposition of any anomalies. This process will be ongoing until all anomalies are resolved. The three phases are described below:

- Initial TDP Review

The first review is performed to determine whether the TDP submitted is complete enough to perform TDP review. This is an abbreviated review. Each document is read to determine whether it provides enough description of the submitted voting system components and whether it at least generically addresses VVSG requirements. The results of the review are used in determining contractual requirements for the test campaign.

- Compliance Review

This review is conducted on a document-by-document basis to determine if every Federal, State, or manufacturer-stated requirement has been met based on the context of each requirement. This review does not address consistency or completeness of documents. The review is more complex than the initial TDP review. Results of the review of each document are entered on the TDP Review Checklist and are reported to the manufacturer for disposition of any anomalies. This process is ongoing until all anomalies are resolved.

Any revised documents during the TDP review process are compared with the previous document revision to determine changes made, and the document is re-reviewed to determine whether subject requirements have been met.

- Consistency/Completeness Review

The third TDP review is completed after the review for compliance has been performed (the Consistency/Completeness TDP Review may overlap the Compliance Review in part). This review is to ensure the information included in the TDP documents is consistent across documents, especially in component naming, software and firmware versioning, and the hardware, software, and firmware included with the voting system submitted for testing. Any revisions to a document during the TDP review process which affect other documents must also be revised. As with the other TDP reviews, the TDP Review Checklist is utilized to report any anomalies to the manufacturer for resolution, if required. The TDP review continues until all anomalies have been satisfactorily resolved.

A listing of all documents contained in EVS 7000 is provided below:

EAC Required Files

ESSVS_7'0'0'0_Implementation Statement: *Implementation Statement ES&S Voting System 7.0.0.0*

TDP

System Overview

ESSVS_7'0'0'0_D_SysOvr: *System Overview EVS 7.0.0.0*

System Hardware Specification

ESSVS_2'0_SPC_DurabilityEstimation: *Durability Estimation ES&S Standards and Procedures*

EVOTEXL_1'0_SPC_HWSpec: *ExpressVote XL Hardware Specification Hardware Version 1.0*

System Specifications

ESSVS_2'0_P_Coding Standards: *Coding Standards EVS Version 7.0.0.0*

ESSVS_2'0_SPC_BallImgProc: *Ballot Image Processing Specification EVS Version 7.0.0.0*

ESSVS_2'0_SPC_Barcode: *Barcode Specification EVS Version 7.0.0.0*

ESSVS_2'0_SPC_CommonDataFormat: *Common Data Format Specification EVS Version 7.0.0.0*

ESSVS_2'0_SPC_EventCodeSpecification: *Event Code Specification ES&S Event Logging Capabilities VVSG Version 2.0*

ESSVS_2'0_SPC_LicenseAgreements: *License Agreements for Procured Software EVS Version 7.0.0.0*

ESSVS_2'0_SPC_DatabaseConfiguration: *Database Configuration Software Design Specification Software Version 7.0.0.0*

System Test and Usability

ESSVS_2'0_SPC_UCD Report: *User-Centered Design Specification and Report ES&S Standards and Procedures*

ESSVS_7'0'0'0_D_TestPlan: *Voting System Test Plan ES&S Standards and Procedures ES&S Voting System 7.0.0.0*

EVOTEXL_1'0_D_CIFRpt_POLLWORKER: *Usability Test Report of ExpressVote XL ES&S Election Voting System 7.0.0.0 Usability Test with Poll Workers*

EVOTEXL_1'0_D_CIFRpt_VOTER: *Usability Test Report of ExpressVote XL ES&S Election Voting System 7.0.0.0 Usability Test with Voters*

System Test and Usability: Usability Reports

EVOTEXL_1'0_D_CIFRpt_POLLWORKER: *Usability Test with Poll Workers ExpressVote XL ES&S Election Voting System 7.0.0.0*

EVOTEXL_1'0_D_CIFRpt_VOTER: *Usability Test with Voters ExpressVote XL ES&S Election Voting System Version 7.0.0.0*

System Test and Usability: QA Test Cases

ESSVS_7'0'0'0_TC_QA_Regression: *QA Test Cases Regression ES&S Voting System 7.0.0.0*

System Security and Inspection

ESSVS_2'0_L_DISA-STIG: *DISA-STIG ES&S Standards and Procedures*

ESSVS_2'0_SPC_SysRiskAsmt: *System Risk Assessment ES&S Standards and Procedures*

ESSVS_2'0_SPC_Supply Chain Risk Management: *Supply Chain Risk Management and Criticality Analysis VVSG 2.0*

ESSVS_2'0_SPC_VulnerabilityManagement: *Vulnerability Management Plan ES&S Standards and Procedures*

ESSVS_7'0'0'0_SPC_SecBestPrac: *Security Best Practices Physical Security Guide ES&S Voting System 7.0.0.0*

ESSVS_7'0'0'0_SPC_SetupInspectionProcedures: *Setup Inspection Procedures ES&S Standards and Procedures ES&S Voting System 7.0.0.0*

ESSVS_7'0'0'0_SPC_SystemSecurity: *Security Specification ES&S Voting System Security ES&S Voting System 7.0.0.0*

System Security and Inspection: Setup & Configuration Guides

ESSVS_7'0'0'0_SPC_SetupConfigGuide_StandaloneWorkstation: *Secure Setup and Configuration Guide EMS Standalone Workstation ES&S Voting System 7.0.0.0*

System Security and Inspection: Verification Procedures & Scripts

ESSVS_7'0'0'0_D_VerProc_EMS: *Election Management System Verification Procedures Software Version 7.0.0.0*

ESSVS_7'0'0'0_D_VerProc_EMS_Admin: *Election Management System Administrator's Guide Verification Procedures Software Version 7.0.0.0*

ESSVS_7'0'0'0_D_VerProc_EVOTEXL: *ExpressVote XL Verification Procedures Firmware Version 7.0.0.0*

System Security and Inspection: Validation FileLists

EMS_7'0'0'0_L_ValFileList_Standalone: *Election Management System-Standalone Static/Dynamic File List Software Version 7.0.0.0*

EVOTEXL_7'0'0'0_L_ValFileList: *ExpressVote XL Static/Dynamic File List Firmware Version 7.0.0.0*

System Security and Inspection: Verification Packs

EMS-7.0.0.0-Generate-HashTrusted-Pack: *EMS-7.0.0.0-Generate-HashTrusted-Pack*

XL-7.0.0.0-Verification-Pack: *XL-7.0.0.0-Verification-Pack (zip file)*

System Operations Procedures

ELNAV_7'0'0'0_SOP_01Admin: *Election Navigator Vol. I: Administrator Guide Software Version 7.0.0.0*

ELNAV_7'0'0'0_SOP_02User: *Election Navigator Vol II: User Guide Software Version 7.0.0.0*

EVOTEXL_7'0'0'0_SOP: *ExpressVote XL Operator's Guide Firmware Version 7.0.0.0*

System Maintenance Manuals

ELNAV_7'0'0'0_SMM: *Election Navigator Maintenance Manual Software Version 7.0.0.0*

EVOTEXL_7'0'0'0_SMM: *ExpressVote XL Maintenance Manual Firmware Version 7.0.0.0*

Program Manuals

ESSVS_2'0_P_QualityControlProgram: *Quality Control Program ES&S Standards and Procedures*

ESSVS_2'0_P_TrainingProgram: *Personnel Deployment and Training Program ES&S Standards and Procedures*

TDP Appendices

ESSVS_2'0_SPC_BPG: *Ballot Production Guide Printing Guidelines*

TDP Appendices: Bill of Materials

ESSVS_7'0'0'0_L_BOM_FW: *Bill of Materials: Firmware (CoRE)*

ESSVS_7'0'0'0_L_BOM_SW: *Bill of Materials: Software (Election Navigator)*

EVOTEXL_1'0_L_BOM: *Bill of Materials: ExpressVote XL HW Rev 1.0*

TDP Appendices: Approved Parts Lists

EVOTEXL_1'0_L_APL: *Approved Parts List: ExpressVote XL HW Rev 1.0*

Resources

Resources: TDP Support

ESSVS_7'0'0'0_L_RequirementsMatrix_TDP: *TDP Requirements Trace EVS 7.0.0.0*

Resources: HW Support

EVOTEXL_1'0_D_PDXPkg: *ExpressVote XL Assembly*

Resources: Security Support

ESSVS_7'0'0'0_SPC_Modified_Windows_OS_ISO_EMS: *Modified Windows OS ISOs Election Management System ES&S Voting System 7.0.0.0*

SECTION V.3 SOURCE CODE REVIEW

Pro V&V will review the submitted source code to VVSG 2.0 and the manufacturer-submitted coding standards. Prior to initiating the software review, Pro V&V shall verify that the submitted documentation is sufficient to enable (1) a review of the source code and (2) Pro V&V to design and conduct tests at every level of the software structure to verify that design specifications and performance guidelines are met.

The submitted source code will be subjected to a compliance review. Once the compliance review is performed and the source is deemed stable enough to proceed with testing, the source code and all additional packages will be compiled into a Compliance Build. Following successful completion of the FCA, a Trusted Build will be performed. The trusted build consists of inspecting the submitted source code, COTS, and third-party software products and combining them to create the executable code following the

documented process from the “*United States Election Assistance Commission Voting System Testing and Certification Program Manual Version 3.0*” Section 4.8. Performance of the trusted build includes the build documentation review.

A combination of automated source code review and manual source code review methods will be used to review the submitted source code. The complete source code will be reviewed utilizing the automated source code tools. These tools include Parasoft C/C++test and dotTEST both of which are listed on the Mitre Common Weakness Enumeration (CWE) Compatibility Product and Services List. To validate the tools, Pro V&V utilized Samate Software Assurance Reference Dataset (SARD). This dataset provides ‘Pristine vs. Dirty’ sample test data, in this case source code, and a ‘Flawed and Fixed’ dataset. These samples allow for the tool to be validated. Pro V&V will then follow the EVS 7000 TDP to install the automatic source code review tools. Once the tools are installed, validated, and the review executed, Pro V&V will verify the results obtained match the expected results. No modifications to the tools are required, only importing of the ES&S rule set. Findings from the automated review tool will be manually reviewed to ensure that all source code is VVSG 2.0 compliant.

The manual source code review will consist of randomly selecting 10% of the source code and performing a line-by-line code review to verify software flow, robustness, code integrity, output protections, readability, maintainability, modularity, logic requirements, scalability, integrity in processes and data, error handling, and functionality.

SECTION V.4 FUNCTIONAL CONFIGURATION AUDIT (FCA)

The Functional Configuration Audit (FCA) encompasses an examination of manufacturer tests, and the conduct of additional tests, to verify that the system hardware and software perform all the functions described in the manufacturer’s documentation submitted in the TDP (such as system operations, voter manual, maintenance, and diagnostic testing manuals). It includes a test of system operations in the sequence in which they would normally be performed. These system operations and functional capabilities are categorized as follows by the phase of election activity in which they are required:

- Overall System Capabilities: These functional capabilities apply throughout the election process. They include security, accuracy, integrity, system audit ability, election management system, vote tabulation, ballot counters, telecommunications, and data retention.
- Pre-voting Capabilities: These functional capabilities are used to prepare the voting system for voting. They include ballot preparation, the preparation of election-specific software (including firmware), the production of ballots, the installation of ballots and ballot counting software (including firmware), and system and equipment tests.
- Voting System Capabilities: These functional capabilities include all operations conducted at the polling place by voters and officials including the generation of status messages.
- Post-voting Capabilities: These functional capabilities apply after all votes have been cast. They include closing the polling place; obtaining reports by voting machine, polling place, and precinct; obtaining consolidated reports; and obtaining reports of audit trails.

- Maintenance, Transportation and Storage Capabilities: These capabilities are necessary to maintain, transport, and store voting system equipment.

The FCA for this test campaign will include an assessment of the submitted modifications and will include inputs of both normal and abnormal data during test performance. This evaluation will utilize baseline test cases as well as specifically designed test cases and will include predefined election definitions for the input data. As part of the FCA, primary and general elections will be executed to verify successful system operation. During the performance of the FCA, qualified personnel shall:

- Review the manufacturer's test procedures and test results to determine if the manufacturer's specified functional requirements have been adequately tested. This examination shall include an assessment of the adequacy of the vendor's test cases and input data to exercise all system functions and to detect program logic and data processing errors, if such are present.
- Perform or supervise the performance of additional tests to verify nominal system performance in all operating modes and to verify on a sampling basis the manufacturer's data reports. If manufacturer developmental test data is incomplete, qualified personnel shall design and conduct all appropriate module and integrated functional tests.

SECTION V.5 SECURITY REVIEW

The purpose of the Security Review is to assess the access controls (the process of granting or denying specific requests to obtain and use information and related information processing services; and enter specific physical facilities) and security controls (management, operational, and technical controls, such as safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information) of the system under evaluation.

Security requirements are interwoven throughout VVSG 2.0; however, security testing is primarily addressed in the following Principles:

Principle 11 – Access Control: The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

Principle 12 – Physical Security: The voting system prevents or detects attempts to tamper with voting system hardware.

Principle 13 – Data Protection: The voting system protects data from unauthorized access, modification, or deletion.

Principle 14: System Integrity: The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

Principle 15: Detection and Monitoring: The voting system provides mechanisms to detect anomalous or malicious behavior.

The test methods for performing the Security Testing are execution and review. Prior to performance of Security testing, the examiner will verify that security hardening scripts have been properly applied to system components per the system documentation. The examiner will review the submitted TDP to verify that documented access and physical controls are in place.

Following the documented procedures, the examiner will configure the voting system for use and functionality to verify that the documented controls are in place and adequate and meet the stated requirements. The Security Review consists of an Administrative Review, Technical Review, and Physical Review, described as follows:

Administrative Evaluation

The Administrative Security Evaluation begins with reviewing the TDP package for assessor orientation to the system while evaluating the breadth and depth of security topics covered. The documentation will be assessed for coverage, clarity, correctness, consistency, and effectiveness of the documented security controls. The assessment evaluates the security controls' effectiveness in protecting confidentiality, integrity, availability, and accountability within the system. The evaluation also assesses that ample and appropriate controls are implemented within the system to provide adequate protection to the system. This evaluation spans all security defenses and phases mentioned above. The assessment extends beyond the TDP Review to evaluate the compliance in fulfilling the requirements outlined in the VVSG and/or related requirements. The assessment includes a review of the vendor's submitted threat matrix provided in the TDP to evaluate security controls for effectiveness in protecting against threats.

During the Administrative Security Evaluation specific experiential tests are derived from the controls specified in the documentation. These tests are executed during the technical/logical evaluation phases through hands-on applied assessment. Tasks performed on each component during the Administrative Security Evaluation may include, but are not limited to, the following:

- Election Navigator: Privilege Escalation, Permissions & Roles, Access Controls
- ExpressVote XL: Permissions & Roles, Access Controls

Examples of these attacks are provided below:

Privilege Escalation, Permission & Roles, and Access Controls – Attempt to gain access to elevated rights and tasks from a standard user.

Physical Evaluation

The Physical Security Evaluation consists of configuring the physical security of the system components in accordance with the TDP documentation and evaluating the effectiveness of the physical security controls. This test includes an assessment of preventative and detective controls against physical breach to a component. Physical Security Evaluation tasks may include, but are not limited to, altering the physical components to allow for unauthorized access to the system, and real word threat actor scenarios. For each component the following tasks may include:

- Election Navigator: Removing Protective Measures, Detection & Prevention
- ExpressVote XL: Removing Protective Measures, Detection & Prevention

Examples of these attacks are provided below:

Removing Protective Measures – Physically manipulating the security measures in place to gain access.

Detection & Prevention – While attempting to gain physical access to the system, we will monitor how long it will take and if the attempt is noticeable.

Technical/Logical Evaluation

The Technical/Logical Security Evaluation takes the output from the Administrative Security Evaluation process to evaluate that the controls specified in the TDP are implemented on the system components.

To perform the Security Review, qualified test personnel will develop and execute specifically designed test cases in an attempt to defeat the access controls and security measures documented in the system TDP. The test cases will be developed utilizing the requirements found in Principles 11-15 to verify that each identified security feature and procedure meets requirements and functions as expected and documented. Qualified personnel will also perform each type of identified evaluation (Administrative, Physical, and Technical/Logical) on the EVS 7000 system.

Additionally, the EVS 7000 submitted threat matrix identifying the system's risks and vulnerabilities was evaluated for completeness and to determine that mitigating controls were adequately implemented. The evaluation of the system shall be accomplished by utilizing a combination of functional testing and source code review. All findings will be reported to the EAC and ES&S.

Pro V&V will use multiple security techniques to examine various security measures of the EVS 7000 Voting System. Examples of possible attack vectors may include, but are not limited, to SQL Injection Attacks, Network Scans, Packet Captures, and Brute Force Attacks. For each component the following tasks may include:

- Election Navigator: SQL Injection Attacks, Network Scans
- ExpressVote XL: Brute Force Attack

Examples of these attacks are provided below:

SQL Injection - Using SQL Injection on the Election Navigator to try to modify the database

Network Scans - Scans to see if there are any open ports that would allow for a threat actor to manipulate the system

Brute Force Attack - Using a Rubber Ducky to manipulate the system to perform actions that the system is not intended to do

SECTION V.6 VULNERABILITY TESTING

Vulnerability is a system weakness related to security procedures, internal controls, flaws, features, or user errors that can potentially be exploited by a threat source. To assess the vulnerability of the EVS 7000 system, qualified personnel will evaluate the system by executing test cases developed to specific requirements contained in the Principles listed below:

Principle 2: High Quality Implementation: The voting system is implemented using high quality best practices.

Principle 14: System Integrity: The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

The test cases will be executed to verify the system meets the requirements and functions as expected and documented. Additionally, qualified personnel will perform each type of identified evaluation (Administrative (to include a review of the system vulnerability management plan submitted as part of the system TDP), Physical, and Technical/Logical) on the EVS 7000 system.

Automated Vulnerability scans will be taken of all networked machines to determine if there are any vulnerabilities or unauthorized open network ports. Vulnerabilities discovered will have security techniques used to determine the severity of each vulnerability. All findings will be reported back to the EAC and ES&S for evaluation.

SECTION V.7 CRYPTOGRAPHIC TESTING

Cryptographic testing will be performed to assess the EVS 7000 System to the following Principle:

Principle 13: Data Protection, Guidelines 13.3 - All cryptographic algorithms are public, well-vetted, and standardized

To perform the Cryptographic Testing, qualified personnel will evaluate the system by executing test cases developed to the specified requirements contained within the principle to verify the system meets the requirements and functions as expected and documented. Qualified personnel will also perform each type of identified evaluation (Administrative, Physical, and Technical/Logical) on the EVS 7000 system.

SECTION V.8 USABILITY REVIEW

A Usability Review will be performed to examine how users interact with the system in accordance with the following Principle:

Principle 8: Robust, Safe, Usable, and Accessible – The voting system and voting processes provide a robust, safe, usable, and accessible experience.

The purpose of the Usability Review is to assess the usability of the EVS 7000 system. Usability is defined in the VVSG 2.0 as, “Effectiveness, efficiency, and satisfaction with which a specified set of users can achieve a specified set of tasks in a particular environment. Usability in the context of voting refers to voters being able to cast valid votes as they intended quickly, without errors, and with confidence that their contest selections were recorded correctly. It also refers to the usability of the setup and operation of voting equipment in the polling place.” The Usability Review consists of tasks that address voter confidentiality (privacy and independence), integrity (accuracy), and availability (usability).

To perform the Usability Review, test personnel will perform a documentation review to identify the voting system’s usability features and procedures. The documentation must include:

- A report on the results of realistic usability tests, with both voters and election workers.
- A report documenting that the system was developed following a user-centered design process.

- Descriptions and instructions for all accessibility features describing recommended procedures that fully implement accessibility for voters with disabilities, and how the voting system supports those procedures.

Following the documented instructions contained in the system TDP, the test personnel shall setup and configure the voting system, with all the identified usability features, as for normal operation at the polling place. The test personnel shall perform test cases developed utilizing the requirements found in Principle 8 and all accessibility requirements located within the VVSG to verify that each identified usability feature and procedure meet requirements and functions as expected and documented.

SECTION V.9 ACCESSIBILITY REVIEW

Per VVSG 2.0, the voting system shall be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters. Accessibility is dependent upon voter confidentiality (privacy and independence), integrity (accuracy), and availability (usability). Accessibility features must be integrated into the manufacturer's voting system so that accessibility for voters with disabilities is supported throughout the voting session, including any steps to activate the ballot at the voting station, ballot marking, verification, and casting. This requirement ensures accessibility to the voter throughout the entire session. Not only are individual system components (such as ballot markers, paper records, and optical scanners) accessible, but they also support voters with disabilities throughout the process of voting from activation through casting.

Requirements for individual system components are described in **Principle 5: Equivalent and Consistent Voter Access**, **Principle 7: Marked, Verified, and Cast as Intended**; and processes that provide a robust, safe, usable and accessible experience are described in **Principle 8, Robust, Safe, Usable, and Accessible**.

To perform the Accessibility Review, test personnel will perform a documentation review to identify the voting system's accessibility features and procedures. The documentation must include:

- A report documenting that the system was developed following a user-centered design process.
- Descriptions and instructions for all accessibility features describing recommended procedures that fully implement accessibility for voters with disabilities, and how the voting system supports those procedures.

Following the documented instructions contained in the system TDP, test personnel shall setup and configure the voting system, with all of the identified accessibility features, as for normal operation at the polling place. The test personnel shall develop, validate, and perform test cases utilizing the requirements found in Principle 5, Principle 7, and Principle 8, as well as all accessibility requirements located within the VVSG that are not included in these Principles, to verify that each identified accessibility feature and procedure meets requirements and functions as expected and documented. Additionally, test personnel will verify accessibility features are integrated into the voting system so accessibility for voters with disabilities is supported throughout the voting session, including any steps to activate the ballot at the voting station, ballot marking, verification, and casting.

SECTION V.10 SYSTEM INTEGRATION TESTING

The System Integration area of testing is a system level test that evaluates the integrated operation of both hardware and software. Compatibility of the voting system software components or subsystems with one another, and with other components of the voting system environment, shall be determined through functional tests integrating the voting system software with the remainder of the system. Additionally, the system will be configured exactly as it would for normal field use per the procedures detailed in the EVS 7000 technical documentation. This includes connecting all supporting equipment and peripherals including ballot boxes, voting booths (regular and accessible), and any physical security equipment such as locks and ties.

To accomplish the test objective, two General Elections and two Primary Elections will be exercised on the voting system, as described below. Each election is designed to test different voting variations. The descriptions included in this section are high level descriptions designed to provide an overview. The specific information will be included in the election definitions, which will be designed to accommodate system functionality, limitations, or specific functionality being tested.

Three general elections with the following breakdowns:

- General Election GEN-01: A General Election held in four precincts, one of which is a split precinct. This election contains nineteen contests compiled into four ballot styles. Five of the contests are in all four ballot styles. The other fourteen contests are split between at least two of the precincts with a maximum of four different contests spread across the four precincts.
- General Election GEN-03: A General Election held in two precincts. This election contains eight contests compiled into two ballot styles. Four of the contests are in both ballot styles. The other four contests are split between the two precincts. This election is designed to functionally test the handling of multiple ballot styles, support for at least three languages including a character-based language, support for common voting variations, and audio support for at least three languages and an ADA binary input device.

Two primary elections with the following breakdowns:

- Primary Election PRIM-01: This election is designed to functionally test a Closed Primary Election with multiple ballots and support for common voting variations. This election contains thirty-one contests and six parties compiled into eighteen ballot styles, each ballot containing six contests.
- Primary Election PRIM-03: A Closed Primary Election held in two precincts. This election contains ten contests and is compiled into two ballot styles. Two of the contests are in both ballot styles. The other eight contests are split between the two parties' ballots. This election is designed to functionally test the handling of multiple ballot styles, support for at least three languages including a character-based language, support for common voting variations, and audio support for at least three languages and an ADA binary input device.

SECTION V.11 ACCURACY TEST

The Accuracy Test is designed to test the ability of the voting system to capture, record, store, consolidate, and report the specific selections, and absence of selections, made by the voter for each ballot position without error. Per the EAC VVSG 2.0, the following requirements apply:

Principle 1: High Quality Design

Guideline 1.2 – The voting system is designed to function correctly under real-world operating conditions.

1.2-A – Assessment of accuracy

The voting system's accuracy must be assessed by using a combination of evidence items gathered during the entire course of testing, including:

1. A measurement of how accurately voter marks are recognized as valid or not valid according to manufacturer specifications.
2. A measurement of how accurately voter marks are tabulated and reported as results.
3. An assessment of whether the remaining VVSG requirements are satisfied.

1.2-B – Reliably detectable marks

The voting system must detect marks on the ballot consistent with system mark specifications and differentiate between voter-made marks constituting votes versus voter-made marginal marks or other marks on the ballot.

1.2-C – Minimum ballot positions

A minimum of 10,000,000 ballot positions must be read by the voting system and tabulated accurately. Each ballot will have a total of 496 votable ballot positions. A total of 16 contests with 31 candidates in each contest. One candidate will be voted for in each contest. A minimum total of 20,162 ballots will be printed and tabulated using six ExpressVote XLs.

1.2-G – Misfeed rate benchmark

The voting system misfeed rate must not exceed 0.002 (1 / 500).

Multiple feeds, misfeeds (jams), and rejections of ballots that meet all manufacturer specifications are all treated collectively as "misfeeds" for benchmarking purposes; that is, only a single count is maintained.

Prior to test initiation, a Test Case and Election Definition specific to the Accuracy Test will be developed. The accuracy requirements for the EVS 7000 will be met by executing the Test Case utilizing a test deck composed of blank and pre-printed cards of each ballot length supported by the system. This test deck will be processed until the required minimum number of ballot positions to be tabulated is met.

SECTION V.12 VOLUME TEST

The Volume & Stress test investigates the system's response to conditions that tend to overload the system's capacity to process, store, and report data. The test parameters will focus on the system's stated limits and the ballot logic for areas such as the maximum number of active voting positions, maximum number of ballot styles, maximum candidates, maximum contests, and stated limits within the EMS. This test will be utilized to ensure the system can achieve the manufacturer's TDP claims of what the system can support. Testing will be performed by exercising multiple election definitions developed specifically to test for volume and stress conditions of the system being tested.

SECTION V.13 INTEROPERABILITY

VVSG 2.0 defines Interoperability as the extent to which systems from different manufacturers and devices with different system configurations can communicate with each other. VVSG 2.0 contains the following Principle and associated Guidelines for evaluating the Interoperability of a system:

Principle 4: Interoperable

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

Guideline 4.1 - Voting system data that is imported, exported, or otherwise reported is in an interoperable format.

Guideline 4.2 - Standard, publicly available formats for other types of data are used, where available.

Guideline 4.3 – Widely used hardware interfaces and communications protocols are used.

Guideline 4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.

Interoperability testing will be performed on all applicable Common Data Format (CDF) implementations supported by the voting system to verify compliance with VVSG 2.0 Principle 4. Where implemented, testing will include Voter Records Interchange (VRI), Cast Vote Records (CVR), Election Results Reporting (ERR), and Election Event Logging (EEL). Testing will verify that imported, exported, and reported data conforms to the applicable specifications and is processed correctly by the voting system.

To perform the Interoperability Review, qualified personnel will evaluate the system by executing test cases developed to the specified requirements to verify the system meets the requirements and functions as expected and documented. The general procedure to be followed for performing conformance and interoperability testing of common data format import and export implementations is outlined in the steps below:

1. Review the manufacturer's documentation for import and export features and data format.
2. Use the designated method to produce an export for the applicable CDF implementation (VRI, CVR, ERR, or EEL).
3. Compare the exported file(s) to the applicable CDF specification and manufacturer documentation.
4. Document any discrepancies between the exported data and the applicable specification.

5. Alter a value for any entity in the data export.
6. Use the altered data export file to now import the changed data.
7. Use the designated method to import the data.
8. Compare the imported data and verify that the modified data is accurately represented within the appropriate system data structures. For CVR, verify cast vote record data; for EEL, verify event log records; for VRI, verify voter record data; and for ERR, verify election results data as applicable.
9. When applicable, verify the election results for export are in the common data format for election night results reporting.

SECTION V.14 HARDWARE TESTING

The EVS 7000 is a new system submitted for testing to the VVSG 2.0; therefore, the full suite of Hardware Testing will be required for all components. VVSG 2.0 Hardware Testing consists of electrical hardware testing, an operational environmental test, and various non-operational environmental tests, as described below:

Electrical Hardware Tests

Electrical Hardware Tests consist of Electrical Supply (Battery Backup), Electrical Power Disturbance (Voltage Dips), Electrical Fast Transient (EFT), Lightning Surge, Electrostatic Discharge (ESD), Electromagnetic Emissions (Radiated and Conducted), Electromagnetic Susceptibility (Radiated Immunity), and Conducted RF Immunity.

Non-Operational Environmental Hardware Tests

Non-Operational Environmental Hardware Tests include Bench Handling, Transportation Vibration, Low Temperature, and High Temperature.

Operational Environmental Hardware Test

Operational Hardware Testing consists of a Continuous Operation - Varied Environmental Conditions Test. The table below provides a breakdown of the components and the applicable hardware tests:

Table V-2 EVS 7000 Hardware Testing Overview

Hardware Test	VVSG 2.0 Requirement	ExpressVote XL
Radiated Emissions	1.2-I	Yes
Conducted Emissions	1.2-I	Yes
Radiated Immunity	2.7-G	Yes
Electrical Supply (Battery Backup)	2.7-H	Yes
Lightning Surge	2.7-I	Yes
Electrical Fast Transient	2.7-I	Yes
Electrical Power Disturbance	2.7-I	Yes
Conducted RF Immunity	2.7-J	Yes
Electrostatic Discharge	2.7-K	Yes

Table V-2 EVS 7000 Hardware Testing Overview (continued)

Hardware Test	VVSG 2.0 Requirement	ExpressVote XL
Non-Operational Low Temperature	2.7-F	Yes
Non-Operational High Temperature	2.7-F	Yes
Non-Operational Bench Handling	2.7-D	Yes
Non-Operational Transportation Vibration	2.7-E	Yes
Continuous Operation – Varied Environmental Conditions	2.7-C	Yes

SECTION V.14.1 ELECTRICAL HARDWARE TESTING

The EVS 7000 is a new system submitted for testing to the VVSG 2.0; therefore, the full suite of Electrical Hardware Testing will be required for components as listed in the above table. VVSG 2.0 Electrical Hardware Testing consists of the following tests:

- **Electromagnetic Emissions (Radiated and Conducted)**

Requirement 1.2-I (FCC Part 15 Class A and B Conformance)

This test demonstrates the ability of the system to comply with the Rules and Regulations of the Federal Communications Commission, Part 15, Class A or Class B requirements for both radiated and conducted emissions.

Note: Class A shall be utilized for non-polling locations and Class B shall be utilized for polling locations.

Testing shall be conducted per ANSI C63.4-2014.

- **Electromagnetic Susceptibility (Radiated Immunity)**

Requirement 2.7-G (Electrical disturbances)

This test demonstrates the ability of the system to be able to withstand, without disruption of normal operation or loss of data.

The test for Electromagnetic Susceptibility shall be conducted in compliance with the test specified in IEC 61000-4-3, Latest Edition.

- **Electrical Supply (Battery Backup)**

Requirement 2.7-H (Power outages, sags, and swells)

Electrical Supply will be performed to assess the ability of the system to operate with the electrical supply ordinarily found at end user deployment sites, withstand disruption of normal operation or loss of data, a complete loss of power lasting two hours, retain the contents of all memories intact when backup power is exhausted, and if the voting system uses a powered physical security countermeasure, that physical countermeasure must maintain its state when power is removed and must have a backup power supply. In addition, when primary power is unavailable the system must automatically switch to the backup power supply, produce an alert, and generate an event log entry, if possible.

- **Electrical Power Disturbance (Voltage Dips)**

Requirement 2.7-I (Withstand conducted electrical disturbances)

This test demonstrates the ability of the system to be able to withstand the voltage dips and surge conditions without disruption of normal operation or loss of data:

The test for Electrical Power Disturbance shall be conducted in compliance with the test specified in IEC 61000-4-11, Latest Edition.

- The voting system MUST NOT be disturbed by a temporary overvoltage of 120 % normal line voltage lasting from 3 ms to 0.5 s, applied in gradual steps of overvoltage across the line and neutral terminals.
- The voting system MUST NOT be disturbed nor overheat for a permanent overvoltage of 10% above the nominal 120 V rating of the voting system, applied in gradual steps of overvoltage across the line and neutral terminals.

- **Electrical Fast Transient (EFT)**

Requirement 2.7-I (Withstand conducted electrical disturbances)

This test demonstrates the ability of the system to be able to withstand, without disruption of normal operation or loss of data.

The test for Electrical Fast Transient shall be conducted in compliance with the test specified in IEC 61000-4-4, Latest Edition.

- **Lightning Surge**

Requirement 2.7-I (Withstand conducted electrical disturbances)

This test demonstrates the ability of the system to be able to withstand, without damage or loss of data.

The test for Lightning Surge shall be conducted in compliance with the test specified in IEC 61000-4-5, Latest Edition.

- **Conducted RF Immunity**

Requirement 2.7-J (Emissions from other connected equipment)

This test demonstrates the ability of the system to be able to withstand, without disruption of normal operation or loss of data.

The test for Conducted RF Immunity shall be conducted in compliance with the test specified in IEC 61000-4-6, Latest Edition.

- **Electrostatic Discharge (ESD)**

Requirement 2.7-K (Electrostatic discharge immunity)

This test demonstrates the ability of the system to be able to withstand, without damage or loss of data.

Note: The equipment may reset or have momentary interruption so long as normal operation is resumed without human intervention or loss of data (votes that have been completed and confirmed to the voter).

The test for Electrostatic Disruption shall be conducted in compliance with the test specified in IEC 61000-4-2, Latest Edition.

Electrical Hardware Testing will be performed by personnel verified by Pro V&V to be qualified to perform the test. Pro V&V will utilize third-party test facilities for performance of the Electrical Hardware Testing, except for Electrical Supply. Testing will be performed at the Element Longmont facility located in Longmont, Colorado. All testing at the Element Longmont facility will be witnessed on-site by Pro V&V personnel. Electrical Supply will be performed at the Pro V&V laboratory. All pre-test and post-test operational status checks shall be conducted by Pro V&V personnel.

SECTION V.14.2 OPERATIONAL HARDWARE TESTING

Operational Hardware Testing

Operational Hardware Testing consists of an Operational Hardware Test intended to simulate stress faced during operation of tabulators (precinct and central) and BMDs. The test consists of continuous operation in varied environmental conditions.

- **Operational Hardware Test**

- Requirement 2.7-C (Continuous Operation – Varied Environmental Conditions Test)**

- This test must be performed in accordance with the high and low temperature specifications of MIL-STD-810-H, Methods 501.7 and 502.7, Procedure II – Operation, cyclic temperature and humidity exposure. This procedure tests system operation under various environmental conditions for at least 104 hours. During 72 hours of operating time, the equipment shall be in a test chamber under the test conditions imposed for both temperature and humidity. For the remaining 32 hours, the equipment shall be operated at room temperature or in ambient condition. The system shall be powered for the entire period of this test; the power may be disconnected for maintenance or if necessary for removal of the system from the test chamber during the ambient portion of testing.

- Operation shall consist of exercising ballot-counting cycles, which vary by system type, for 15 minutes of each hour, and at the maximum rate calculated from the manufacturer's documented throughput rates.

Prior to test initiation, a pre-test operational status check will be performed to verify the system producing accurate results and is operating as designed. The system will then be subjected to the required test parameters. Upon completion of testing, test personnel will perform the process of closing the polls. If the component is a tabulator the results shall be processed and validated to be accurate with expected results. After completion of all testing activities, a post-test operational status check will be performed.

Non-Operational Hardware Testing

Non-Operational Hardware Testing consists of the following: Bench Handling, Transportation Vibration, Low Temperature, and High Temperature. These tests are intended to simulate exposure to conditions typically encountered during the handling and transportation of voting equipment between storage facilities and polling places, including physical shock and vibration associated with handling and transportation of equipment between a storage facility and a deployment site and temperature/humidity conditions that may be encountered during storage in an uncontrolled environment.

- **Bench Handling Test (Non-Operational)**

Requirement 2.7-D (Ability to support maintenance and repair physical environment conditions)

This test simulates stresses faced during maintenance and repair of system components. This test is equivalent to the procedure of MIL-STD-810H, Method 516.8, Procedure VI.

- **Transportation Vibration Test (Non-Operational)**

Requirement 2.7-E (Ability to support transport and storage physical environment conditions)

This test simulates stresses faced during transport of system components between storage facilities and deployment sites. This test is equivalent to the procedure of MIL-STD-810H, Method 514.8, Procedure 1- Basic Transportation, Common Carrier.

- **Low Temperature Test (Non-Operational)**

Requirement 2.7-F (Ability to support storage temperatures in physical environment)

This test simulates non-operating physical environmental conditions simulating temperature-related and humidity-related stresses faced during storage of system components. This test is equivalent to the procedure of MIL-STD-810H, Method 502.7, Procedure I-Storage. The minimum temperature for this test shall be -4° F.

- **High Temperature Test (Non-Operational)**

Requirement 2.7-F (Ability to support storage temperatures in physical environment)

This test simulates non-operating physical environmental conditions simulating temperature-related and humidity-related stresses faced during storage of system components. This test is equivalent to the procedure of MIL-STD-810H, Method 501.7, Procedure I-Storage. The maximum temperature for this test shall be 140° F.

Prior to test initiation, a pre-test operational status check will be performed to verify the system producing accurate results and is operating as designed. Upon completion of testing, a post- test operational status check will be performed to verify the system is operating without issue. Any issues encountered during the post operational status check will be documented. If it is determined a failure has occurred, ES&S will be required to mitigate the issue, provide a root cause analysis, and the test will be repeated.

Environmental Hardware Testing will be performed by personnel verified by Pro V&V to be qualified to perform the test. Pro V&V will utilize third-party test facilities for performance of the Environmental Hardware Testing. Testing will be performed at the Element Longmont facility located in Longmont, Colorado. Testing at the Element Longmont facility will be witnessed on-site by Pro V&V personnel, except for the Operational Environmental Test (Continuous Operation – Varied Environmental Conditions) in which Pro V&V qualified staff will execute all testing. All pre-test and post-test operational status checks shall be conducted by Pro V&V personnel.

SECTION V.15 PRODUCT SAFETY REVIEW

The Product Safety Review ensures the submitted voting system's hardware, software, and accessories are robust and do not expose users to harmful conditions. To meet this objective, the system submitted will be subjected to a Product Safety Review of the following requirements:

- **Requirement 8.1-K (Eliminating Hazards)**

Devices associated with the voting system must be certified in accordance with the requirements of *IEC/UL 62368-1 [UL19], Edition 3: Standard for Audio/video, Information and Communication Technology Equipment - Part 1: Safety requirements* by a certification organization accredited by the Department of Labor, Occupational Safety and Health Administration's Nationally Recognized Testing Laboratory program.

Additionally, the submitted system will be evaluated to ensure it meets the product marking and workmanship set forth in Requirements 2.1.1 (Workmanship) and 2.1.2-C (Nameplate and labels) of the VVSG 2.0, as described below:

- **Requirement 2.1.1 (Workmanship)**

2.1.1-A – General build quality

All manufacturers of voting systems must practice proper workmanship by:

1. Adopting and adhering to practices and procedures that ensure their products are free from damage or defects that could make them unsatisfactory for their intended purpose; and
2. Ensuring that components provided by external suppliers are free from damage or defects that could make them unsatisfactory or hazardous when used for their intended purpose.

2.1.1-B – Durability estimation

A manufacturer must submit a warranty model to the EAC, testing labs, and customers, which includes for each product its relevant components, and associated consumables:

1. Estimated replacement rates (e.g., 3 years, 10 years);
2. Estimated costs per replacement;
3. Estimated warranty types and costs;
4. Associated replacement policies, services, and available maintenance agreements; and

5. Plans for collecting, maintaining, and reporting data to the EAC to support and validate estimates.

2.1.1-C – Durability of paper

Paper specified for use with the voting system must conform to the applicable specifications contained within the Government Paper Specification Standards, February 1999 No. 11, or the government standards that have superseded them.

2.1.1-D – Ensure compatibility of specified paper and ink

Ink specified for use with the voting system must be compatible with the paper specifications provided by the manufacturer.

2.1.2-C – Nameplate and labels

All voting devices must:

1. Display a permanently affixed nameplate or label containing the name of the manufacturer, the name of the device, its part or model number, its revision identifier, its serial number, and if applicable, its power requirements.
2. If service or preventative maintenance is required, display a separate data plate containing a schedule for and list of operations required to service or to perform preventive maintenance, or a reference to where this can be found in the voting equipment user documentation.
3. Display advisory caution and warning instructions to ensure safe operation of the equipment and to avoid exposure to hazardous electrical voltages and moving parts at all locations where operation or exposure may occur

For this test campaign, Pro V&V will review the submitted Product Safety Review Report and technical documentation included in the TDP to ensure the system has been evaluated against the relevant requirements and provides sufficient documentation.

SECTION VI: TEST DATA

The following subsections provide information concerning test data recording, criteria, and reduction.

SECTION VI.1 TEST DATA RECORDING

All equipment utilized for test data recording shall be identified in the test data package. The output test data shall be recorded in an appropriate manner as to allow data analysis. For source code and TDP reviews, results shall be compiled in reports and submitted to ES&S for resolution.

SECTION VI.2 TEST DATA CRITERIA

EVS 7000 shall be evaluated against all applicable requirements contained in VVSG 2.0. A *VVSG 2.0 Cross Reference Matrix* specific to the EVS 7000 will be utilized during the test campaign to ensure that all applicable VVSG 2.0 requirements are addressed. The matrix will contain the requirement number, title,

and text for each VVSG 2.0 requirement, a listing of applicable system components, Artifact and Result Artifact IDs (Test Case IDs, Test Result IDs, Test Reports, etc.), and any applicable notes.

The acceptable range for system performance and the expected results for each test case shall be derived from the manufacturer-submitted technical documentation and the VVSG 2.0.

SECTION VI.3 TEST DATA REDUCTION

Test data shall be processed and recorded in the Engineering Notebook on the EVS 7000 dedicated project Smartsheet and the relevant Test Cases.

SECTION VII: TEST CONDITIONS

The following subsections detail the facility requirements, test setup conditions, and sequence of testing.

SECTION VII.1 FACILITY REQUIREMENTS

Unless otherwise annotated, all testing shall be conducted at the Pro V&V test facility located in Huntsville, AL, by personnel verified by Pro V&V to be qualified to perform the test. Unless otherwise specified herein, testing shall be performed at the following standard ambient conditions and tolerances:

- Temperature: 68-75° F ($\pm 3.6^\circ$ F)
- Relative Humidity: Local Site Humidity
- Atmospheric Pressure: Local Site Pressure
- Time Allowable Tolerance: 5%

Testing performed at third-party laboratories will be subject to the test parameters and tolerances defined by VVSG. If not specified in VVSG, the test facilities' standard parameters and tolerances will be used. These shall be reported in the final Test Report.

SECTION VII.2 TEST SET-UP

All voting system equipment shall be received and documented using Pro V&V established QA procedures. Upon receipt of all hardware, an inspection will be performed to verify that the equipment received is free from obvious signs of damage and/or degradation that may have occurred during transit. If present, this damage shall be recorded, photographed, and reported to the ES&S Representative. Additionally, a comparison shall be made between the recorded serial numbers/part numbers and those listed on shipper's manifestation and any discrepancies shall be reported to the ES&S Representative. TDP items and all source code received shall be inventoried and maintained by Pro V&V during the test campaign.

During test performance, the system shall be configured as it would be for normal field use. This includes connecting all supporting equipment and peripherals.

SECTION VII.3 TEST SEQUENCE

EVS 7000 will be evaluated against all applicable requirements in VVSG 2.0. There is no required sequence for test performance; however, there may be prerequisite tasks for some testing. If so, the predecessor task will be identified within the test case.

SECTION VIII: TEST OPERATIONS PROCEDURES

Pro V&V will identify PASS/FAIL criteria for each executed test case. The PASS/FAIL criteria will be based on the specific expected results of the system. In the case of an unexpected result that deviates from what is considered standard, normal, or expected, a root cause analysis will be performed. Pro V&V will evaluate every VVSG 2.0 requirement applicable to the EVS 7000 voting system. Any deficiencies noted will be reported to the EAC and the manufacturer. If it is determined that there is insufficient data to determine compliance, this test plan will be altered, and additional testing will be performed.

APPENDIX A: PROJECT SCHEDULE

Project Commencement	01/22/26	03/13/26		
EAC Kickoff Meeting	01/22/26	01/22/26	Michael Walker	Program Manager
Application Approval from EAC	03/13/26	03/13/26	Michael Walker	Program Manager
TDP	01/07/26	06/09/26		
TDP Submission	01/07/26	01/07/26	Michael Walker	Program Manager
TDP Review (Initial, Compliance, Final)	01/08/26	06/09/26	Michael Walker	Program Manager
Test Plan	03/23/26	06/12/26		
Test Plan Creation	03/23/26	04/17/26	Michael Walker	Program Manager
Test Plan (Review and Approval)	04/20/26	06/12/26	Michael Walker	Program Manager
Source Code	01/12/26	03/12/26		
Source Code Submission	01/12/26	01/12/26	Michael Walker	Program Manager
Source Code (Review and Compliance Build)	01/13/26	03/12/26	Michael Walker	Program Manager
System Delivery & Setup	01/07/26	03/17/26		
PCA	01/07/26	01/07/26	Michael Walker	Program Manager
System Setup	01/08/26	01/08/26	Michael Walker	Program Manager
System Loads & Hardening	03/16/26	03/17/26	Michael Walker	Program Manager
System Level Testing	03/18/26	06/15/26		
System Level Test Design and Execution	03/18/26	06/15/26	Michael Walker	Program Manager
Trusted Build and System Integration	06/04/26	06/15/26		
Trusted Build	06/04/26	06/05/26	Michael Walker	Program Manager
System Integration	06/11/26	06/15/26	Michael Walker	Program Manager
Test Report	06/16/26	08/17/26		
Test Report Creation	06/16/26	06/22/26	Michael Walker	Program Manager
Test Report (Review and Approval)	06/23/26	08/17/26	Michael Walker	Program Manager