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

# EAC VVSG 2.0 Certification Test Plan
# Unisyn Voting Solutions (Unisyn) Optio 1.0 Voting System

*Document Number: TP-01-01-UNI-2025-01*

EAC Project Number: UNS_Optio_1.0

Document Version: 04

Date: 11/20/2026

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 — 11/20/2026

Michael L. Walker, VSTL Program Manager — Date

Approved by: Wendy Owens — 11/20/2026

Wendy Owens, VSTL Program Director — Date

Approved by: Stacey Glover — 11/20/2026

Stacey Glover, QA Manager — 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 | 07/08/2026 |
| 01 | Updates per EAC comments; corrected grammatical errors; updated COTS table in Section III; updated Signature page; revised Sections V.2 (TDP), V.5 (Security Review), V.10 (System Integration), V.11 (Accuracy), V.14 (Hardware Testing), and Section VIII (Test Operations Procedure) | 10/22/2026 |
| 02 | Updates per EAC comments | 11/12/2026 |
| 03 | Updated COTS Software Table | 11/16/2026 |
| 04 | Updates per EAC comments | 11/20/2026 |
| | | |

**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 ..... 5
Section I.3.1.2 System Limits ..... 6
Section I.3.1.3 Supported Languages ..... 6
Section I.3.1.4 Supported Functionality ..... 7
Section I.4 Scope of Testing ..... 8
Section I.5 Testing Responsibilities ..... 13
Section I.6 Third Party Tests ..... 15
**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 ..... 16**
Section III.1 Software ..... 16
Section III.2 Hardware/Equipment ..... 17
Section III.2.1 Hardware/Equipment CONFIGURATIONS ..... 19
Section III.3 Materials/Consumables ..... 19
Section III.4 Proprietary Data ..... 19
**SECTION IV: TEST SPECIFICATIONS ..... 19**
Section IV.1 Requirements ..... 20
Section IV.2 Test Case Development and Design ..... 20
Section IV.2.1 Hardware Environmental Test Case Design ..... 20
Section IV.2.2 Software Module Test Case Design and Data ..... 21
Section IV.2.3 Software Functional Test Case Design and Data ..... 21
Section IV.2.4 System-Level Test Case Design ..... 22
Section IV.3 Test Procedure Development and Validation ..... 22

**SECTION V: TEST PROCEDURES ..... 22**
Section V.1 Physical Configuration Audit (PCA) ..... 22
Section V.2 Technical Data Package (TDP) Review ..... 23
Section V.3 Source Code Review ..... 25
Section V.4 Functional Configuration Audit (FCA) ..... 25
Section V.5 Security Review ..... 26
Section V.6 Vulnerability Testing ..... 29
Section V.7 Cryptographic Testing ..... 30
Section V.8 Usability Review ..... 30
Section V.9 Accessibility Review ..... 31
Section V.10 System Integration Testing ..... 31
Section V.11 Accuracy Test ..... 33
Section V.12 Volume Test ..... 34
Section V.13 Interoperability ..... 34
Section V.14 Hardware Testing ..... 34
Section V.14.1 Electrical Hardware Testing ..... 35
Section V.14.2 Operational Hardware Testing ..... 38
Section V.14.3 Non-Operational Hardware Testing ..... 38
Section V.15 Product Safety Review ..... 40
**SECTION VI: TEST DATA ..... 41**
Section VI.1 Test Data Recording ..... 41
Section VI.2 Test Data Criteria ..... 41
Section VI.3 Test Data Reduction ..... 42
**SECTION VII: TEST CONDITIONS ..... 42**
Section VII.1 Facility Requirements ..... 42
Section VII.2 Test Set-Up ..... 42
Section VII.3 Test Sequence ..... 43
**SECTION VIII: TEST OPERATIONS PROCEDURES ..... 43**
**APPENDIX A: PROJECT SCHEDULE ..... 44**

# 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 Unisyn Voting Solutions (Unisyn) Optio Voting System (hereinafter referred to as 'Unisyn Optio 1.0') 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 Unisyn Optio 1.0 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, Unisyn submitted the application package to the EAC for certification of the Unisyn Optio 1.0. The application was accepted by the EAC, and the project assigned the unique Project Number of UNS_Optio_1.0.

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 1.4
- 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)

- Unisyn Voting Solutions Optio Voting System 1.0 EAC Application Approval Letter, dated April 23, 2026
- Unisyn Optio 1.0 Technical Data Package *(A listing of the TDP documents submitted for this test campaign is listed in Section V.2 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

"ADA BMD" – Ballot Marking Device in ADA mode

"ATI" – Audio-Tactile Interface

"BMD" – Ballot Marking Device

"CM" – Configuration Management

"COTS" – Commercial Off-The-Shelf

"CS" – Central Scanner

"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

"PC" – Precinct Counter

"PCA" – Physical Configuration Audit

"QA" – Quality Assurance

"RFI" – Request for Interpretation

"TAB" – Tabulation & Aggregation

"TC" – Tabulator Client

"TDP" – Technical Data Package

"TM" – Transport Media

"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 Performance and/or other documents contained in the TDP.*

The Unisyn Optio 1.0 Voting System is a precinct voting system that uses touchscreen and scanning technology to scan and validate ballots, provides voter-assisted ballots for voters with special needs, tabulates precinct results, and produces election reports. Unisyn Optio 1.0 consists of the following major components: Optio Server, Optio Central Scanner (CS), Optio Precinct Counter (PC), and Optio Ballot Marking Device (BMD).

### SECTION I.3.1 SYSTEM OVERVIEW

**Unisyn Optio 1.0 system components:**

Optio Server

Optio Server is a specially configured laptop running the Linux-based Optio Operating System (OptioOS), which runs the Optio software suite. It is located in a secure tabulation office at Election Headquarters. The suite includes two main applications: the Election Management System and the Tabulation & Aggregation applications, each with its own database that shares a common interface. The EMS is used to design the ballot, set the election's parameters, and create the election file. The TAB application tallies the vote data, generates election reports, and can be used to perform audits and recounts.

Optio Tabulator Client

Optio Tabulator Client (TC) is an application used at the election headquarters. It can reside on the Optio Server or on a standalone laptop that is connected to the Optio Server. It is responsible for importing the vote data from the Precinct Counter and the Central Scanner TMs and storing it until it can be uploaded to the TAB application for tabulation and aggregation.

Optio Precinct Counter (PC)

Optio Precinct Counter (PC) is a compact, full-page, dual-sided optical scanning system. It scans and validates ballots produced on in-precinct Ballot Marking Devices (BMD) as well as hand-marked full-page ballots. It summarizes all cast ballot pages during the current election session and produces various election night reports based on the data gathered on that PC.

Optio Ballot Marking Device (BMD)

The Optio Ballot Marking Device (BMD or ADA BMD**)** is a computer-based ballot marking device that allows voters to print their regional ballot on Election Day and during an early voting session at vote centers. Unisyn has designed two models of the BMD: an ADA BMD and the Vote Center BMD.

The ADA BMD complies with the Americans with Disabilities Act (ADA) to ensure accessibility for voters of varying abilities. It is designed to assist voters in making their ballot selections using various optional methods, such as sip-and-puff support, keypad functionality, and audio assistance for visually impaired voters. The only difference between the ADA BMD and Vote Center BMD is the printer automatically rotates facing downward when placed in ADA mode to allow the printed ballot to be dropped directly into the secure ballot box without requiring the voter to manually handle the ballot.

The Vote Center BMD presents an onscreen ballot that allows voters to make their choices electronically.

The BMD does not retain vote data; it records all activity each user performs in the Admin Logs. The log files are copied to a removable TM in a human-readable format that can be viewed and printed from a text application on a laptop. They are used to support an audit.

Optio Central Scanner (CS)

Optio Central Scanner (CS) is a ballot scanning system comprising the CS laptop, bulk scanner, and the Optio CS software. It is specifically designed for use in Election Headquarters to scan early voting ballots, absentee voting ballots, full-page Election Day ballots, and BMD ballots. The vote data can be directly uploaded to the TAB if it is networked to the CS. Or the vote data can be written to a USB Transfer Media (TM) and transferred to the Optio Server, where it is uploaded to the Tabulation Client (TC) application. The TC stores the vote data until it can be uploaded to the Tabulation & Aggregation application, where it is tabulated and various election reports are generated.

## SECTION I.3.1.1 BLOCK DIAGRAM

The Unisyn Optio 1.0 Voting System components and data flow are depicted in Figure I-1.
BMD

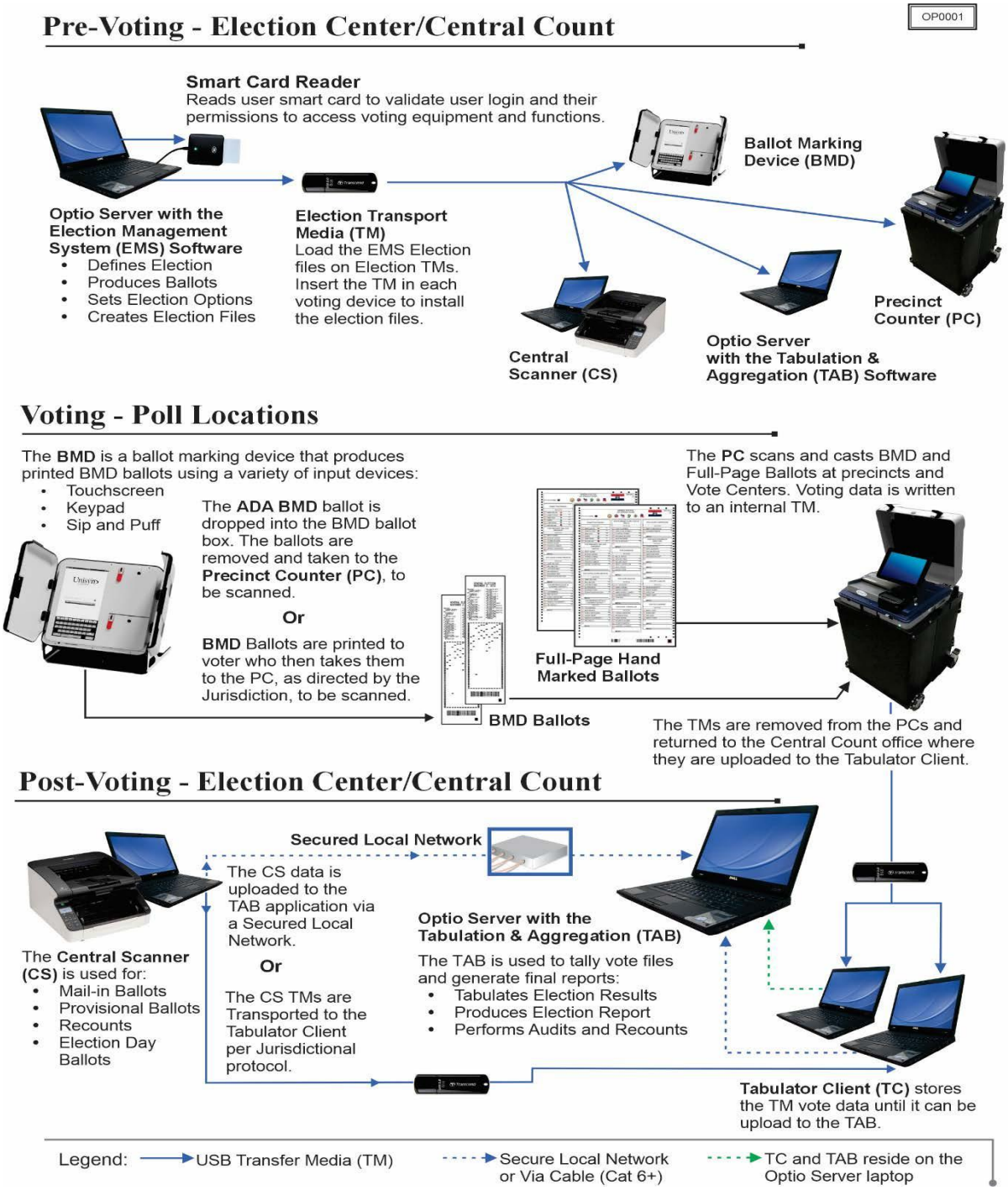


**Figure I-1 Unisyn Optio 1.0 Voting System Components and Data Flow**

## SECTION I.3.1.2 SYSTEM LIMITS

Unisyn has defined the following performance characteristic limits and device capacities for the Optio 1.0 components:

**Table I-1 Optio 1.0 Voting System Limits**

| System | Boundary or Limitation |
|---|---|
| Maximum Elections (EMS) | 8 |
| Maximum Precincts (EMS) | 2,000 |
| Maximum Splits per Precinct (EMS) | 9 |
| Maximum Districts (EMS) | 400 |
| Maximum Contests per District (EMS) | 20 |
| Maximum Parties (EMS) | 20 |
| Maximum Parties in primary (EMS) | 10 |
| Maximum Parties w/ Straight Ticket (EMS) | 10 |
| Maximum District Types (EMS) | 25 |
| Maximum Languages (EMS) | 10 |
| Maximum Ballot Styles per Election (EMS) | 400 |
| Maximum Contests per Election (EMS) | 150 |
| Maximum Measures per Election (EMS) | 30 |
| Maximum Instruction Blocks per Election (EMS) | 5 |
| Maximum Headers per Election (EMS) | 50 |
| Maximum Candidates per Election (EMS) | 3,000 |
| Maximum Candidates per Contest (EMS) | 120 |
| Maximum Ballot Pages (EMS) | 3 |
| Maximum Votes for N of M (EMS) | 35 |
| Maximum Ranks in RCV (EMS) | 10 |
| Maximum Ballot Pages per batch (CS and EMS) | 500 |
| Maximum Ballot Pages per session (CS) | 5,000 |
| Maximum Ballot Pages per session (PC) | 10,000 |
| Maximum expected scanning speed (ballot pages per hour – CS) | 2100 |
| Maximum Units simultaneously loading (EMS) | 20 |
| Maximum Precincts initialized per PC on Election Day (EMS) | 30 |
| Maximum Precincts initialized per PC in early voting (EMS) | 2,000 |

## SECTION I.3.1.3 SUPPORTED LANGUAGES

Per the *System Overview and Performance*, Unisyn Optio 1.0 BMD supports multiple languages for both visual and audio ballots, allowing voters to choose their preferred language from options including Chinese, English, Spanish, and Vietnamese. It also provides bilingual options, with English as the default language and one additional language featured on each ballot page.

## SECTION I.3.1.4 SUPPORTED FUNCTIONALITY

Per the *System Overview and Performance,* Unisyn Optio 1.0 is designed to support the following voting variations:

- General Elections or Not by Party Elections.
- Primary Elections or By Party Elections.
- Open Primaries.
- Closed Primaries.
- Modified Open Primaries.
- Partisan offices.
- Non-partisan offices.
- Write-in voting.
- Primary presidential delegation nominations.
- Ballot rotation.
- Straight party voting.
- Cross-party endorsement.
- Split precincts.
- Vote for 1 of N.
- Vote for N of M.
- Recall issues.
- Ranked Choice Voting (10 ranks). (Elimination Only, Andrae/Cincinnati Method, Weighted Inclusive Gregory Method (WIGM)). *Testing will be accomplished using the Cast Vote Record output and the open-source software from the ranked choice voting resource center.*
- Provisional or challenged ballots.
- Absentee ballots.
- Open primary multi-party ballots.

Additionally, the system accounts for:

- Straight Ticket support.
- Indiana Straight Ticket.
- Proportional Rotation.
- Checking and notification of overvote and undervote conditions.
- Multiple languages.

- Multi-lingual ballots.
- Multi-page ballots.
- Audio Ballots.

During the test campaign, Pro V&V will execute tests designed to verify Unisyn Optio 1.0:

- Provides the capability to define and identify contests, contest options, candidates, and ballot questions using all voting variations identified by Unisyn.
- 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 Unisyn Optio 1.0 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<br>*The voting system is designed to accurately, completely, and robustly carry out election processes.* | |
| 1.1 - The voting system is designed using commonly accepted election process specifications.<br><br>1.2 - The voting system is designed to function correctly under real-world operating conditions.<br><br>1.3 - Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not. | FCA, Accuracy Test, System Integration Testing, TDP Review, Volume Test, Electrical Hardware Testing, Security Tests |

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

| VVSG 2.0 Guideline | VSTL Test Areas |
|---|---|
| Principle 2: High-Quality Implementation<br>*The voting system is implemented using high-quality best practices.* | |
| 2.1 - The voting system and its software are implemented using trustworthy materials and best practices in software development.<br><br>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.<br><br>2.3 - Voting system logic is clear, meaningful, and well-structured.<br><br>2.4 - Voting system structure is modular, scalable, and robust.<br><br>2.5 – The voting system supports system processes and data with integrity.<br><br>2.6 - The voting system handles errors robustly and gracefully recovers from failure.<br><br>2.7 - The voting system performs reliably in anticipated physical environments. | Source Code Review, TDP Review, FCA, Security Tests, Electrical Hardware Testing, Operational Environmental Hardware Testing, Non-Operational Environmental Hardware Testing |
| Principle 3: Transparent<br>*The voting system and voting processes are designed to provide transparency.* | |
| 3.1 - The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.<br><br>3.2 - The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.<br><br>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<br>*The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.* | |
| 4.1 - Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.<br><br>4.2 - Standard, publicly available formats for other types of data are used, where available.<br><br>4.3 - Widely-used hardware interfaces and communications protocols are used.<br><br>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 |

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

| VVSG 2.0 Guideline | VSTL Test Areas |
|---|---|
| Principle 5: Equivalent and Consistent Voter Access<br>*All voters can access and use the voting system regardless of their abilities.* | |
| 5.1 - Voters have a consistent experience throughout the voting process within any method of voting.<br><br>5.2 - Voters receive equivalent information and options in all modes of voting | Usability, Accessibility, FCA, TDP Review |
| Principle 6: Voter Privacy<br>*Voters can mark, verify, and cast their ballot privately and independently.* | |
| 6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections.<br><br>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 |
| Principle 7: Marked, Verified, and Cast as Intended<br>*Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.* | |
| 7.1 - The default voting system settings present a ballot usable for the widest range of voters, and voters can adjust settings and preferences to meet their needs.<br><br>7.2 - Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes and selections.<br><br>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<br>*The voting system and voting processes provide a robust, safe, usable, and accessible experience.* | |
| 8.1 - The voting system's hardware, software, and accessories are robust and do not expose users to harmful conditions.<br><br>8.2 - The voting system meets currently accepted federal standards for accessibility.<br><br>8.3 - The voting system is evaluated for usability with a wide range of representative voters, including those with and without disabilities.<br><br>8.4 - The voting system is evaluated for usability with election workers. | Usability, Accessibility, FCA, TDP Review |

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

| VVSG 2.0 Guideline | VSTL Test Areas |
|---|---|
| Principle 9: Auditable<br>*The voting system is auditable and enables evidence-based elections.* | |
| 9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.<br><br>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.<br><br>9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.<br><br>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<br>*The voting system protects the secrecy of voters' ballot selections.* | |
| 10.1 - Ballot secrecy is maintained throughout the voting process.<br><br>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. | FCA, Usability, Accessibility, TDP Review, Security Tests, Cryptographic Testing |
| Principle 11: Access Control<br>*The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.* | |
| 11.1 - The voting system enables logging, monitoring, reviewing, and modifying of access privileges, accounts, activities, and authorizations.<br><br>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.<br><br>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.<br><br>11.4 - The voting system's default access control policies enforce the principles of least privilege and separation of duties.<br><br>11.5 - Logical access to voting system assets are revoked when no longer required | Security Testing, Vulnerability Testing, FCA |

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

| VVSG 2.0 Guideline | VSTL Test Areas |
|---|---|
| Principle 12: Physical Security<br>*The voting system prevents or detects attempts to tamper with voting system hardware.* | |
| 12.1 - The voting system supports mechanisms to detect unauthorized physical access.<br><br>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<br>*The voting system protects data from unauthorized access, modification, or deletion.* | |
| 13.1 –The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.<br><br>13.2 - The source and integrity of electronic tabulation reports are verifiable.<br><br>13.3 - All cryptographic algorithms are public, well-vetted, and standardized.<br><br>13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks. | Security Tests, FCA, TDP Review, Cryptographic Testing |
| Principle 14: System Integrity<br>*The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.* | |
| 14.1 - The voting system uses multiple layers of controls to provide resilience against security failures or vulnerabilities.<br><br>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.<br><br>14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.<br><br>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<br>*The voting system provides mechanisms to detect anomalous or malicious behavior.* | |
| 15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.<br><br>15.2 - The voting system generates, stores, and reports all error messages as they occur.<br><br>15.3 - The voting system is designed to protect against malware. | Security, FCA, Vulnerability Testing, Penetration Testing, TDP Review |

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

| VVSG 2.0 Guideline | VSTL Test Areas |
|---|---|
| 15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice. | |

Unisyn Optio 1.0 is not an E2E Verifiable Voting System; therefore, Pro V&V has determined that Requirements associated with E2E Verifiable Voting Systems functionality are not applicable to Unisyn Optio 1.0. These Requirements include the following:

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

10.2.4-B – Voting information in receipts

13.3-B – E2E cryptographic voting protocols

Additionally, a *VVSG 2.0 Cross Reference Matrix* specific to the Unisyn Optio 1.0 will be utilized during the test campaign to ensure that all applicable VVSG 2.0 requirements are addressed.

## SECTION I.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

Unisyn Optio 1.0 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 Unisyn Optio 1.0 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 Optio 1.0 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 Unisyn Optio 1.0 was considered for this test campaign.

## SECTION II.3 KNOWN FIELD ISSUES

The Unisyn Optio 1.0 is being submitted for evaluation as a new system that has not been fielded; therefore, there are no fielded systems preceding this system. The Unisyn Optio 1.0 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 Optio 1.0 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 Unisyn Optio 1.0 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.*

The Unisyn Optio 1.0 software package supports election definition, ballot preparation, vote tabulation, aggregation, and reporting for the Optio PC, Optio BMD, and Optio CS systems. The software consists of two primary applications: the Election Management System (EMS) and the Tabulation & Aggregation (TAB) application. EMS is used to create, validate, and manage election definitions, ballot styles, language translations, and election media used by voting devices. TAB operates from a separate database and is used to import finalized election data, consolidate vote results, manage election runs, tabulate election data, and generate official election reports. The software supports logic and accuracy testing, live election tabulation, and recount activities, while providing export capabilities for election results, turnout reports, and cast vote records in standard data formats.

The table below shows the Proprietary Software Component and Version for the Unisyn Optio 1.0 system:

| Component | Version |
|---|---|
| Optio Election Management System (EMS) | Optio 1.0 |
| Optio Tabulation & Aggregation (TAB) | Optio 1.0 |
| Ballot Marking Device (BMD) | Optio 1.0 |
| Precinct Counter (PC) | Optio 1.0 |
| Central Scanner (CS) | Optio 1.0 |
| Optio Tabulator Client (TC) | Optio 1.0 |

COTS

Unisyn Optio 1.0 utilizes a combination of commercial off-the-shelf (COTS) software components to support the Optio PC, Optio BMD, Optio CS, Election Management System (EMS), Tabulator Client (TC) and Tabulation & Aggregation (TAB) applications. The table below shows the COTS software used in the Optio 1.0 system.

**Table III-1 Unisyn Optio 1.0 COTS Software List**

| Software | Component | Version |
|---|---|---|
| Ubuntu Linux Operating System | BMD, PC, CS, TC, EMS & TAB | 22.04.3 LTS |
| AppArmor | BMD, CS, TC, PC, EMS & TAB | 3.0.4-2ubuntu2.4 |
| Java Programming Language with Google coding convention | PC, BMD, CS, TC, EMS & TAB | JDK 11 |
| JavaScript (NodeJS) with CRA, ESLint, and Prettier coding convention | BMD, EMS & TAB | v18.20.8 |
| Apache-Tomcat Application | CS, TC, EMS & TAB | 9.0.86 |
| MariaDB Database | BMD, EMS & TAB | 10.6.7 |
| JasperReports | CS | 2.0.5 |
| OpenSSL | CS, TC, EMS & TAB | 3.0 |
| Firefox | EMS & TAB | 119.0.1 |
| MD5 | CS, TC, PC, EMS & TAB | 8.32 |
| PDF Document Viewer | EMS | 42.3 |
| Libre OpenOffice | EMS | 7.3.7.2 |

## 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.*

Optio Server

The Optio Server hardware consists of a laptop workstation and smart card reader used to support election administration and results processing. The laptop serves as the host platform for the Election Management System (EMS), Tabulator Client (TC), Central Scanner (CS), and Tabulation & Aggregation (TAB) applications. Transport Media devices, implemented as USB storage devices, are used to distribute election definitions to voting devices and to transfer election data and audit information between election systems. Together, these hardware components provide the infrastructure for election configuration, data transport, results collection, tabulation, and reporting.

Optio Precinct Counter (PC)

The Optio PC is composed of a touchscreen computer, dual-sided ballot scanner, USB-based transport media, thermal printer, optional ballot identifier printer, and integrated battery backup. These components support ballot scanning, vote capture, election data storage, reporting, and secure transfer of election results to the tabulation system.

The Optio PC ballot box provides two slots for inserting ballots, a Ballot Reader slot, and a Secondary Ballot Slot in the back of the ballot box.

Optio Ballot Marking Device (BMD)

The Optio BMD consists of a touchscreen computer, contact smart card reader/writer, thermal ballot printer, optional accessibility peripherals (ADA keypad, audio interface and AirVoter binary input device), and an integrated battery backup system. These components support voter authentication, ballot presentation and marking, ballot printing, accessibility functions, and uninterrupted operation during temporary power loss.

Optio Central Scanner (CS)

The Optio CS hardware consists of a laptop running the CS application, a high-speed dual-sided bulk ballot scanner, and a unique identifier printer. These components support centralized ballot scanning, vote tabulation, reporting, auditing, and the transfer of election results to the tabulation system.

COTS

The Optio voting system is built using COTS hardware components that provide computing, ballot scanning, printing, storage, power management, and accessibility functions. Hardware deployed across the Optio PC, Optio BMD, Optio CS, and Optio Server includes commercial computers, scanners, printers, storage media, power subsystems, and peripheral devices. These components provide the physical infrastructure required to support election configuration, ballot marking, vote capture, tabulation, reporting, auditing, and secure data transport. Specific manufacturer and model information is identified in Table III-2.

**Table III-2 Unisyn Optio 1.0 COTS Hardware List**

| Hardware | Make | Model |
|---|---|---|
| ***Central Scanner*** | | |
| Large Volume Scanner | Canon | DR-G2140 w/ Imprinter |
| Laptop | Penguin | Penguin T4 GNU/Linux |
| ***Optio Server*** | | |
| Laptop | Penguin | Penguin T4 GNU/Linux |
| ***USB*** | | |
| 8 GB USB TM | Transcend | TS8GJF180I |
| 64 GB USB-C TM | Transcend | TS64GJF790C |
| ***Peripheral Devices*** | | |
| Sip-and-puff (Optional) | Origin Instruments | AirVoter |
| Headphones (Optional) | Koss Stereo Headphones | KPH7 |
| Smart Card Reader | Advanced Card Reader | ACR39U ICC |

## SECTION III.2.1 HARDWARE/EQUIPMENT CONFIGURATIONS

The minimum Optio Server hardware configuration includes a dedicated laptop with a 2.0 GHz or faster processor, 120 GB or larger storage device, 2 GB or more of RAM, Ethernet networking capability, and USB ports for peripheral and transport media connectivity.

The Optio PC voting device hardware configuration consists of a client platform with a 1.5 GHz or higher processor, a minimum of 512 MB RAM, a 250 GB or larger SSD, 1 GB or larger USB storage, USB and serial connectivity, video output, and Ethernet networking capability. The device also includes dedicated USB transport media for the secure transfer of election results and ballot image data to the central tabulation environment.

The Optio BMD voting device hardware configuration consists of a client platform with a 1.6 GHz processor, 2 GB RAM, a 16 GB SSD, USB-C connectivity, and SD card storage. This configuration provides the processing, storage, and interface capabilities required for ballot marking and voter accessibility functions.

## 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-3 Unisyn Optio 1.0 Materials/Consumables**

| Material | Description |
|---|---|
| Smart Cards | Programmable Smart Cards for voters, poll workers, and technicians for the Optio PC, Optio BMD, Optio CS |
| Paper Rolls | Replacement Thermal Paper Rolls for the Optio BMD and Optio PC |
| Disposable Straws | Disposable straws for use with the Sip & Puff |
| A/C Power Cables | 3-Prong A/C Power Cables |
| Headphone Covers | Disposable covers for headphone earpieces. |
| USB drives | Transcend 8GB USB 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 Unisyn Optio 1.0 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 Unisyn Optio 1.0 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 and verification.

The Pro V&V designated Test Areas utilized to evaluate the Unisyn Optio 1.0 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 Unisyn Optio 1.0. 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 provide objective pass/fail criteria; and confirmation that any automated test suites will produce valid results. All Unisyn 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 Unisyn Optio 1.0. 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 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, testing may continue while the anomaly remains documented and subject to evaluation and disposition. 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 Unisyn 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, testing may continue while the anomaly remains documented and subject to evaluation and disposition.

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 Unisyn Optio 1.0 is provided below:

04-00649: *Acronyms, Definitions, and Abbreviations*

04-00650: *Standard Operating Procedure: Optio Ballot Marking Device*

04-00651: *Standard Operating Procedure: Optio Central Scanner*

04-00652: *Standard Operating Procedure: Election Management System User Guide*

04-00653: *Optio Hardware Description and Preventive Maintenance Procedures* **(CONFIDENTIAL)**

04-00654: *Personnel Training and Operations Requirements* **(CONFIDENTIAL)**

04-00655: *Standard Operating Procedure: Optio Precinct Counter*

04-00656: *Risk Management Plan* **(CONFIDENTIAL)**

04-00657: *System Overview and Performance*

04-00658: *System Security Specification* **(CONFIDENTIAL)**

04-00659: *System Software Installation User Guide* **(CONFIDENTIAL)**

04-00660: *Tabulation & Aggregation User Guide*

04-00662: *Technical Data Package: Document List and Version Control*

04-00663: *Public Document: Optio's Logs, Barcodes, and Common Data Format*

04-00665: *Tabulator Client User Guide*

*Usability Test Report of Unisyn Optio Voting System*

## 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 JTest 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 Unisyn Optio 1.0 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. Parasoft JTest includes a VVSG 2.0 Ruleset built into the software. 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 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 scope of addressed threats 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:

- EMS & TAB: Privilege Escalation, Permissions & Roles, Access Controls
- Tabulator Client: Privilege Escalation, Permissions & Roles, Access Controls
- Optio Precinct Counter: Privilege Escalation, Permissions & Roles, Access Controls
- Optio BMD: Privilege Escalation, Permissions & Roles, Access Controls
- Optio Central Scan: Privilege Escalation, 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-world threat actor scenarios.

For each component the following tasks may include:

- Optio Precinct Counter: Removing Protective Measures, Detection & Prevention
- Optio BMD: Removing Protective Measures, Detection & Prevention
- Optio Central Scan: 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 Unisyn Optio 1.0.

Additionally, the Optio 1.0 submitted scope of addressed threats 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 Unisyn.

Pro V&V will employ multiple security testing techniques to evaluate the security controls of the Unisyn Optio 1.0 Voting System. Security testing techniques may include, but are not limited to, SQL Injection, Network Scanning, Brute-Force Attacks, USB-Based Attacks, Privilege Escalation, and Authentication Bypass.

Potential testing techniques for each component may include the following:

- EMS & TAB: SQL Injection, Network Scanning, Brute-Force Attacks, Privilege Escalation, USB-Based Attacks, Authentication Bypass
- Optio Precinct Count: Brute-Force Attacks, USB-Based Attacks, Authentication Bypass
- Optio BMD: Brute-Force Attacks, USB-Based Attacks, Authentication Bypass

- Optio Central Scan: Brute-Force Attacks, USB-Based Attacks, Authentication Bypass

Examples of these testing techniques are provided below:

- **SQL Injection:** Attempt to manipulate database queries through available application inputs to determine whether unauthorized access to or modification of election data is possible.
- **Network Scanning:** Perform scans of applicable network interfaces to identify open ports, exposed services, and potential vulnerabilities that could allow unauthorized access or manipulation of the voting system.
- **USB-Based Attacks (Including Rubber Ducky):** Attempt to use USB devices, including devices that emulate keyboards, to execute unauthorized commands, bypass security controls, introduce unauthorized functionality, or cause the voting system to perform unintended operations.
- **Brute-Force Attacks:** Attempt repeated authentication using different credentials to determine whether security controls prevent unauthorized access.
- **Authentication Bypass:** Attempt to access restricted system functions without successfully completing the required authentication process.
- **Privilege Escalation:** Attempt to obtain elevated user privileges or administrative access beyond the permissions assigned to an authenticated user. Testing will evaluate whether users with limited privileges can access restricted functions, modify system configurations, manipulate election data, or execute unauthorized administrative operations.

The applicability of each testing technique will be determined based on the component's functionality, available interfaces, and identified potential vulnerabilities. Additional techniques may be performed as warranted by the security assessment.

## 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 Unisyn Optio 1.0 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 Unisyn Optio 1.0 system.

Automated Vulnerability scans will be performed 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 Unisyn for evaluation.

## SECTION V.7 CRYPTOGRAPHIC TESTING

Cryptographic testing will be performed to assess the Unisyn Optio 1.0 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 Unisyn Optio 1.0 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 Unisyn Optio 1.0 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 meets 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 set up and configure the voting system, with all 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 Unisyn Optio 1.0 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, three General Elections and three 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-02: A basic election held in three precincts. This election contains fifteen contests compiled into three ballot styles. Ten of the contests are in all three ballot styles with the other five split across the 3 precincts. This election also includes ballot rotation, if supported by the system under test.
- 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.

Three 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-02: An Open Primary held in two precincts. This election contains 13 contests compiled into 3 ballot styles. 1 contest is in all 3 ballot styles all other contests are independent. This election is designed to functionally test the handling of multiple ballot styles, support for Primary presidential delegation nominations, support for two languages, support for complex voting variations, and audio support for multiple languages.
- 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.

1.2-G – Misfeed rate benchmark

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

To meet the requirements of 1.2-C, the Unisyn Optio 1.0 system under test must read a minimum of 10,000,000 ballot positions and tabulate accurately. All tabulators shall receive a minimum of 1.6 million ballot positions during the accuracy test using a combination of hand-marked and machine marked (BMD) ballots.

## 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

The Interoperability Test Suite evaluates the voting system's conformance with the interoperability requirements defined in VVSG 2.0. Testing focuses on two primary areas: common data formats and common hardware interfaces/Commercial Off-the-Shelf (COTS) products.

**Common Data Formats**

Common data format testing evaluates the ability of VVSG 2.0 voting system components to exchange election-related data using standardized, interoperable formats. Testing verifies that applicable components have the capability to import and/or export data in the required common data formats and that the resulting data can be transferred, interpreted, and utilized by other compliant systems or applications. The manufacturer shall provide sufficient documentation describing its implementation of each applicable data format. Any encoding methods used for exported or imported data shall be publicly available and accessible without cost or proprietary restrictions.

**Common Hardware Interfaces and COTS Products**

Common hardware interface testing evaluates the use of standardized interfaces and communication methods to promote compatibility and interchangeability between voting system components and supported peripheral devices. Testing verifies that applicable hardware interfaces conform to VVSG 2.0 requirements and operate as documented by the manufacturer.

Where COTS hardware or devices are incorporated into the voting system, testing also verifies that their integration and use do not adversely affect the system's compliance with applicable VVSG 2.0 requirements. COTS components shall be evaluated, as applicable, within the configured voting system to confirm continued compliance with relevant functional, security, reliability, and interoperability requirements.

## SECTION V.14 HARDWARE TESTING

The Unisyn Optio 1.0 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 as follows:

**Electrical Hardware Tests**

Electrical Hardware Tests consist of Electrical Supply (Battery Backup), Electrical Power Disturbance (Voltage Dips and Surges), 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, Humidity, 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 Unisyn Optio 1.0 Hardware Testing Overview**

| Hardware Test | VVSG 2.0 Requirement | Optio PC | Optio BMD | Optio CS |
|---|---|---|---|---|
| Radiated Emissions | 1.2-I | Yes | Yes | No |
| Conducted Emissions | 1.2-I | Yes | Yes | No |
| Radiated Immunity | 2.7-G | Yes | Yes | No |
| Conducted RF Immunity | 2.7-J | Yes | Yes | No |
| Lightning Surge | 2.7-I | Yes | Yes | No |
| Electrical Fast Transient | 2.7-I | Yes | Yes | No |
| Electrostatic Disruption | 2.7-K | Yes | Yes | No |
| Electrical Power Disturbance | 2.7-I | Yes | Yes | No |
| Non-Operational Low Temperature | 2.7-F | Yes | Yes | No |
| Non-Operational High Temperature | 2.7-F | Yes | Yes | No |
| Non-Operational Humidity | 2.7-F | Yes | Yes | No |
| Non-Operational Bench Handling | 2.7-D | Yes | Yes | No |
| Non-Operational Transportation Vibration | 2.7-E | Yes | Yes | No |
| Continuous Operation – Varied Environmental Conditions | 2.7-C | Yes | Yes | Yes |
| Electrical Supply (Battery Backup) | 2.7-H | Yes | Yes | Yes* |

*The Optio CS shall be tested for a graceful shutdown versus a battery backup test.

## SECTION V.14.1 ELECTRICAL HARDWARE TESTING

The Unisyn Optio 1.0 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 (2020).

- **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 and Surges)**

  **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 surges 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 (2020).

  - 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 (2012).

- **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 (2014).

- **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 (2013).

- **Electrostatic Disruption (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 (2008).

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 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 502.7, Procedure II – Operation performed at a constant temperature of 50 degrees Fahrenheit for 24 hours, MIL-STD-810-H, Methods 507.6 Procedure 1 – Natural Cycle B2 for 24 hours with humidity ranges from 25% to 80%, MIL-STD-810-H, Methods 507.6 Procedure 1 – Natural Cycle B1 for 24 hours with humidity ranges from 75% to 80%. This procedure tests system operation under various environmental conditions for 96 consecutive 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 24 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.

## SECTION V.14.3 NON-OPERATIONAL HARDWARE TESTING

**Non-Operational Hardware Testing**

Non-Operational Hardware Testing consists of the following: Bench Handling, Transportation Vibration, Humidity, 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.

- **Humidity 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 507.6, Procedure I- Natural (Hot-Humid) Storage. The humidity will test the ranges of 25% RH to 80% RH during each 24-hour cycle. The minimum duration for this test is 10 days or 10 x 24-hour cycles.

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, Unisyn 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 Report Review ensures the submitted voting system's hardware, software, and accessories are robust and do not expose users to harmful conditions. To achieve this objective, the system submitted will be subjected to a Product Safety Report 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 Unisyn for resolution.

## SECTION VI.2 TEST DATA CRITERIA

Unisyn Optio 1.0 shall be evaluated against all applicable requirements contained in VVSG 2.0. A *VVSG 2.0 Cross Reference Matrix* specific to the Optio 1.0 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, 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 (±3.6° 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 Unisyn Representative.

Additionally, a comparison shall be made between the recorded serial numbers/part numbers and those listed on shipping manifest and any discrepancies shall be reported to the Unisyn 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

Unisyn Optio 1.0 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 establish objective PASS/FAIL criteria for each test case to evaluate compliance with the applicable VVSG 2.0 requirements. Anomalies identified during testing will be documented and evaluated to determine their cause and impact. Deficiencies, defined as failures to conform to applicable VVSG 2.0 requirements, will be documented, tracked, and classified as Major or Minor in accordance with Section 4.9.3 of the EAC Voting System Testing and Certification Program Manual, Version 3.0. Identified deficiencies will be reported to the EAC and the manufacturer in accordance with applicable program requirements.

Manufacturer corrections will be evaluated through appropriate verification activities, including regression testing, source code review, and/or TDP review, as applicable. The disposition of identified deficiencies and verification results will be documented in the Certification Test Report.

If sufficient evidence is unavailable to determine compliance, additional evaluation or testing will be performed as necessary, with any required changes to the approved Test Plan documented accordingly.

## APPENDIX A: PROJECT SCHEDULE

| Task Name | Start Date | End Date | Assigned To | Title |
|---|---|---|---|---|
| **Project Commencement** | **01/20/26** | **03/11/26** | | |
| EAC Kickoff Meeting | 01/20/26 | 01/20/26 | Michael Walker | Program Manager |
| Application Approval from EAC | 03/11/26 | 03/11/26 | Michael Walker | Program Manager |
| **TDP** | **12/22/25** | **08/27/26** | | |
| TDP Submission | 12/22/25 | 12/22/25 | Michael Walker | Program Manager |
| Review (Initial, Compliance, Final) | 12/23/25 | 08/27/26 | Michael Walker | Program Manager |
| **Test Plan** | **06/05/26** | **09/04/26** | | |
| Test Plan Creation | 06/05/26 | 07/02/26 | Michael Walker | Program Manager |
| Test Plan (Review and Approval) | 07/08/26 | 11/04/26 | Michael Walker | Program Manager |
| **Source Code** | **12/22/25** | **09/16/26** | | |
| Source Code Submission | 12/22/25 | 12/22/25 | Michael Walker | Program Manager |
| Review & Compliance Builds | 12/23/25 | 09/16/26 | Michael Walker | Program Manager |
| **System Delivery & Setup** | **07/20/26** | **12/02/26** | | |
| PCA | 09/21/26 | 11/23/26 | Michael Walker | Program Manager |
| System Setup | 11/24/26 | 11/25/26 | Michael Walker | Program Manager |
| System Loads & Hardening | 11/30/26 | 12/02/26 | Michael Walker | Program Manager |
| **Hardware Testing** | **07/20/26** | **11/13/26** | | |
| Electrical Testing | 07/20/26 | 11/13/26 | Michael Walker | Program Manager |
| Environmental Testing | 07/31/26 | 10/30/26 | Michael Walker | Program Manager |
| **System Level Testing** | **12/03/26** | **03/17/27** | | |
| System Level Test Design/Execution | 12/03/26 | 03/17/27 | Michael Walker | Program Manager |
| **Trusted Build and System Integration** | **04/07/27** | **06/14/27** | | |
| Trusted Build | 03/18/27 | 03/22/27 | Michael Walker | Program Manager |
| System Integration | 03/31/27 | 04/06/27 | Michael Walker | Program Manager |
| **Test Report** | **12/22/25** | **08/27/26** | | |
| Test Report Creation | 04/07/27 | 04/22/27 | Michael Walker | Program Manager |
| Test Report (Review & Approval) | 04/23/27 | 06/14/27 | Michael Walker | Program Manager |