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

EAC VVSG 2.0 Certification Test Plan
Smartmatic Voting System Voting System Release (VSR)1 2.1

Document Number: TP-01-01-SMT-2023-01

EAC Project Number: SMT-VSR1-21

Test Plan Version: 02

Date: 09/04/2025

U.S. Election Assistance Commission
VSTL

EAC Lab Code 1501

NVLAP®

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 — 09/04/2025

Michael Walker, VSTL Program Manager — Date

Approved by: Wendy Owens — 09/04/2025

Wendy Owens, VSTL Program Director — Date

Approved by: Stacey Glover — 09/04/2025

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	09/07/2023
01	Updates to include additional functionality and Canon DR-G2140 COTS scanner	11/21/2024
02	Revised list of supported languages in Section I.3.1.3. updated tables as required based on final system configuration	09/04/2025

TABLE OF CONTENTS

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 Smartmatic USA Corporation (Smartmatic) Voting System Release (VSR)1 2.1 Voting System 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 Smartmatic VSR1 2.1 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, Smartmatic submitted an application package to the EAC for certification of the VSR1 2.1. The application was accepted by the EAC, and the project was assigned the unique Project Number of SMT-VSR1-21.

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

SECTION I.1 REFERENCES

- Election Assistance Commission (EAC) Voluntary Voting System Guidelines (VVSG) Version 2.0, "Principles and Guidelines" and "Requirements"
- Voluntary Voting System Guidelines Version 2.0 Test Assertions Version 1.3
- 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 3.0
- 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)
- EAC Application Approval Letter SMT-VSR1-21, dated 03/31/2023

- Smartmatic Voting System VSR1 2.1 Technical Data Package *(A listing of the Smartmatic Voting System VSR1 2.1 documents submitted for this test campaign is listed Table V-1of this Test Plan)*

SECTION I.2 TERMS AND ABBREVIATIONS

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

"ADA" – Americans with Disabilities Act 1990

"ATI" – Accessible-Tactile Interface

"BMD" – Ballot Marking Device

"CCOS" – Central Count Optical Scanner

"CM" – Configuration Management

"COTS" – Commercial Off-The-Shelf

"CVR" – Cast Vote Record

"EAC" – United States Election Assistance Commission

"ECS" – Election Configuration System

"EMP" – Election Management Platform

"FCA" – Functional Configuration Audit

"HAVA" – Help America Vote Act

"LAT" – Logic and Accuracy Test

"NOC" – Notice of Clarification

"NIST" – National Institute of Standards and Technology

"NVLAP" – National Voluntary Laboratory Accreditation Program

"PCA" – Physical Configuration Audit

"PCOS" – Precinct Count Optical Scanner

"QA" – Quality Assurance

"RFI" – Request for Interpretation

"RMS" – Results Management System

"TDP" – Technical Data Package

"UPS" – Uninterruptible Power Supply

"VSR" – Voting System Release

"VSTL" – Voting System Test Laboratory

"VVSG" – Voluntary Voting System Guidelines

SECTION I.3 TARGET OF EVALUATION DESCRIPTION

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

The Smartmatic Voting System VSR1 2.1 (Smartmatic VSR1 2.1) is made up of the following major components:

- Election Management Platform (EMP)
    - Election Configuration System (ECS)
    - Results Management System (RMS)
- Ballot Marking Device (BMD) - Model: BMD-155
- Precinct Count Optical Scanner (PCOS) - Model A4-800
- Central Count Optical Scanner (CCOS) - Scanner Model: Canon DR-G2140

SECTION I.3.1 SYSTEM OVERVIEW

Election Management Platform (EMP)

The Election Management Platform (EMP) is a system designed to support the Pre-Voting and Post-Voting phases of an electoral event. The platform aids election officials in properly designing, planning and managing all the tasks regarding an election. The EMP is a complete platform that includes all the tools required to prepare, conduct, and manage the election event. It contains the Election Configuration System (ECS) and the Results Management System (RMS) sub-components. The EMP is located at the election data center.

The EMP has three landing pages, which act as modules that an authorized user can access to perform different tasks, these modules are: System Administration, Jurisdiction Dashboard, and Election Dashboard. System Administration contains administrative tasks such as user management, visualization of audit logs, backup and restore management, and security policies management. Jurisdiction Dashboard contains all tasks that allow the configuration of the jurisdiction information in the system such as electoral subdivisions, districts, precincts, political parties, and languages to establish the baseline jurisdiction information. Election Dashboard contains all tasks that allow the configuration of an Electoral Event in the system utilizing the baseline jurisdiction information from the jurisdiction dashboard to generate electoral media and support the gathering, processing, and reporting of electoral results.

Ballot Marking Device (BMD) - Model: BMD-155

The Ballot Marking Device (BMD) is an in-precinct voting machine offering usability and independent vote casting capabilities for all voters, including those with disabilities. The BMD allows voters to print a physical paper ballot. The BMD is located at the polling place.

The Smartmatic BMD-155 Ballot Marking Device is designed to assist voters in marking their choices on a paper ballot. It allows voters to use a touchscreen or other input methods to select candidates or options, after which the machine generates a voter reviewable marked paper ballot. Once the voter indicates that they agree with the selections printed on the ballot, the BMD transports the paper to an integral ballot box for secure storage until it is later tabulated. It is important to note that the BMD does not tabulate votes, as does the A4-800 Precinct Scanner or the Central Count scanning system, but instead provides only ballot accounting information once polls are closed.

Citizens with disabilities or special needs are often the primary users of a BMD as that class of vote capture device provides accessibility features such as adjustable font sizes, audio navigation of the ballot with speed and volume control, alternative input methods such as sip and puff, color contrast to aid voters who need high or low contrast display of the ballot. The BMD-155 also accommodates different languages, inviting the voter to choose a display language when the voter approaches the machine to vote.

The BMD process starts with the voter inserting their blank secure paper ballot into the unit on the right-hand side. The voter may also select their session language at this time, as noted above. The BMD will intake and secure the blank ballot and allow the voter to step through instructional pages then contest by contest through the ballot. The instructional pages are pre-programmed via the EMP, often in accordance with State law. For usability, there is always only one contest displayed per display page of the ballot. In accordance with the configuration set by the jurisdiction the BMD will or will not flag the voter regarding undervotes, but overvoting is never allowed by the BMD inherently. Attempts to overvote will cause warning messages to the voter. Review screens follow the ballot contest content. The review allows the voter to move back into the ballot and make changes to their selection before the ballot is marked by the machine.

Once the ballot review is affirmatively accepted by the voter on the screen the printer inside the BMD marks the secure ballot paper with those voter selections then moves the paper toward the voter, while maintaining control of the paper, for visual review by the voter. Audio review is also available to the voter. The voter is able to remove the paper from the BMD for closer inspection if desired. In fact, the marked ballot can even be placed in a different BMD in the polling place, if that BMD carries the same election configuration as the BMD the voter used to mark their ballot.

As noted above the BMD carries accessibility features. These are available at any time during the voter's session, or the voter can choose to move the BMD to its default configuration, also at any time during the voter session. Each BMD carries an Accessible-Tactile Interface (ATI) box to allow for navigation through the ballot with or without audio cues. The display may be turned off for enhanced privacy if the ATI is in use. Each BMD can also connect via a 3.5mm audio jack to headphones and/or a two-channel input device such as a sip and puff unit via a second 3.5mm jack specifically for this purpose. Each

3.5mm jack is marked, with audio to the left of the voter, and two channel devices to the right of the voter, on the front of the BMD. There is a second audio jack on the rear of the machine if the jurisdiction allows the polling place officials to use it to aid the audio voter. The ATI has both audio speed and volume controls to make the audio navigation experience more pleasant for the voter.

Precinct Count Optical Scanner (PCOS) - Model A4-800

The Precinct Count Optical Scanner (PCOS) is an in-precinct voting machine designed to count voter-marked paper ballots. The PCOS offers usability and independent vote casting capabilities for all voters, including those with disabilities. It simultaneously scans both sides of the ballots that have been marked electronically or by hand. The PCOS is located at the polling place.

The PCOS includes a touchscreen and buttons that provide an interface for voters. During the voting process, the PCOS scans and interprets the marked paper ballots. A secure ballot box is attached to the PCOS to store the scanned ballots once they are cast, and the ballot images are stored to USB memory devices. CVR reports and logs can be exported onto a USB memory device. After the voting process, the PCOS tabulates results and can be used to consolidate results from various PCOS machines in a polling place onto one Smartcard. The voting machine also includes an integrated thermal printer and an internal battery for continuity in case of a power outage.

Central Count Optical Scanner (CCOS) - Scanner Model: Canon DR-G2140

The Central Count Optical Scanner (CCOS) is a high-speed COTS scanner utilized to process physical ballots at a central location. It is configured with custom-made ballot processing software that permits processing and tabulation of large numbers of ballots. Batches of ballots processed by the CCOS are saved and sent to the EMP through a private network. Once the EMP sends confirmation that the batch was received successfully, a batch report is printed and stored physically with the scanned ballots. The CCOS is located at the central count location.

SECTION I.3.1.1 BLOCK DIAGRAM

The components and the operational process of the Smartmatic VSR1 2.1 are depicted in Figures I-1 and I-2, respectively. This solution deployment diagram, depicted in Figure I-3, provides a complete overview of system components and processes and portrays the relationships and interactions among them. This figure includes all of the hardware platforms and software components and a minimum data interchange as well as all network communications.

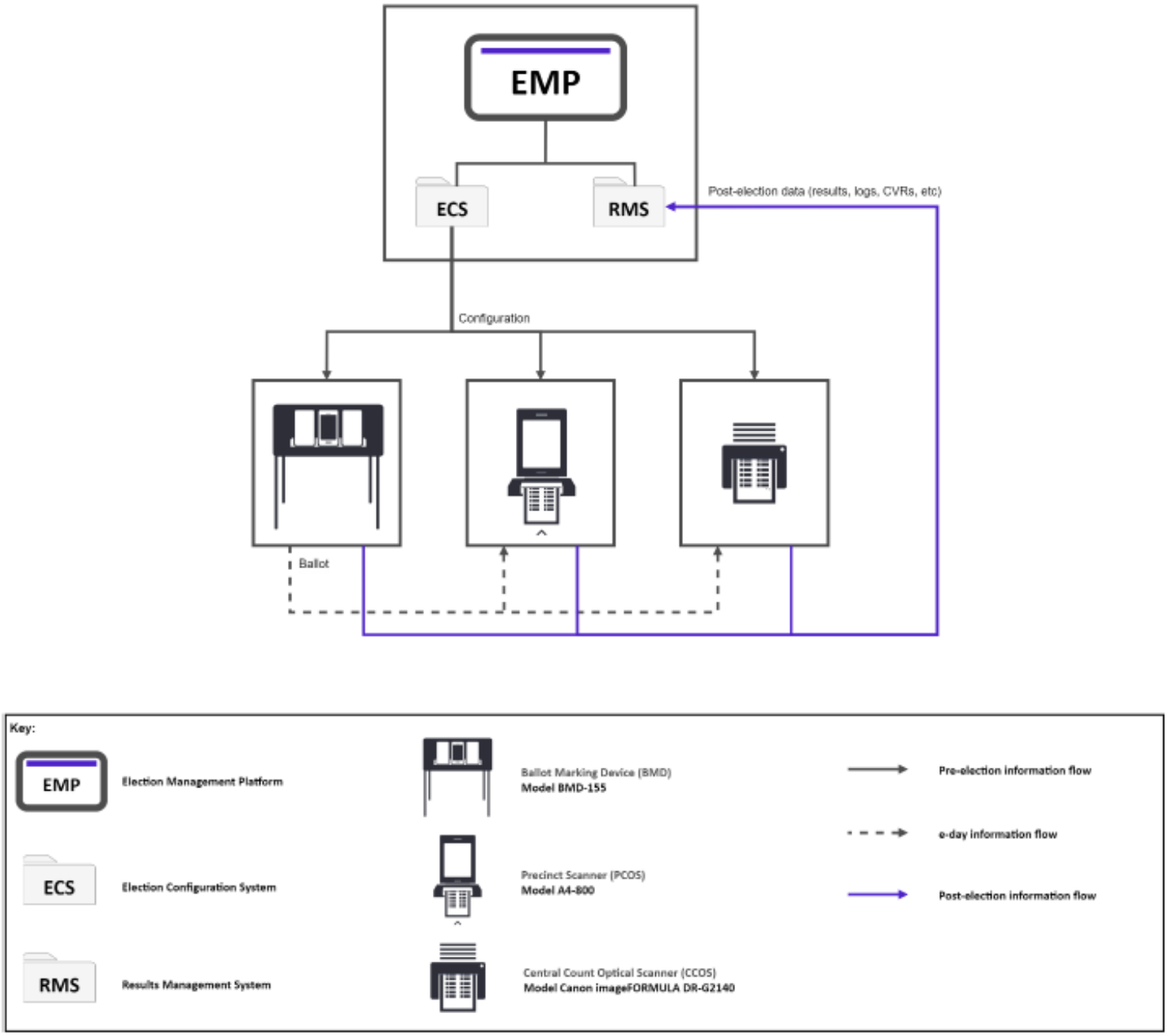

Figure I-1 Components of the Smartmatic VSR1 2.1

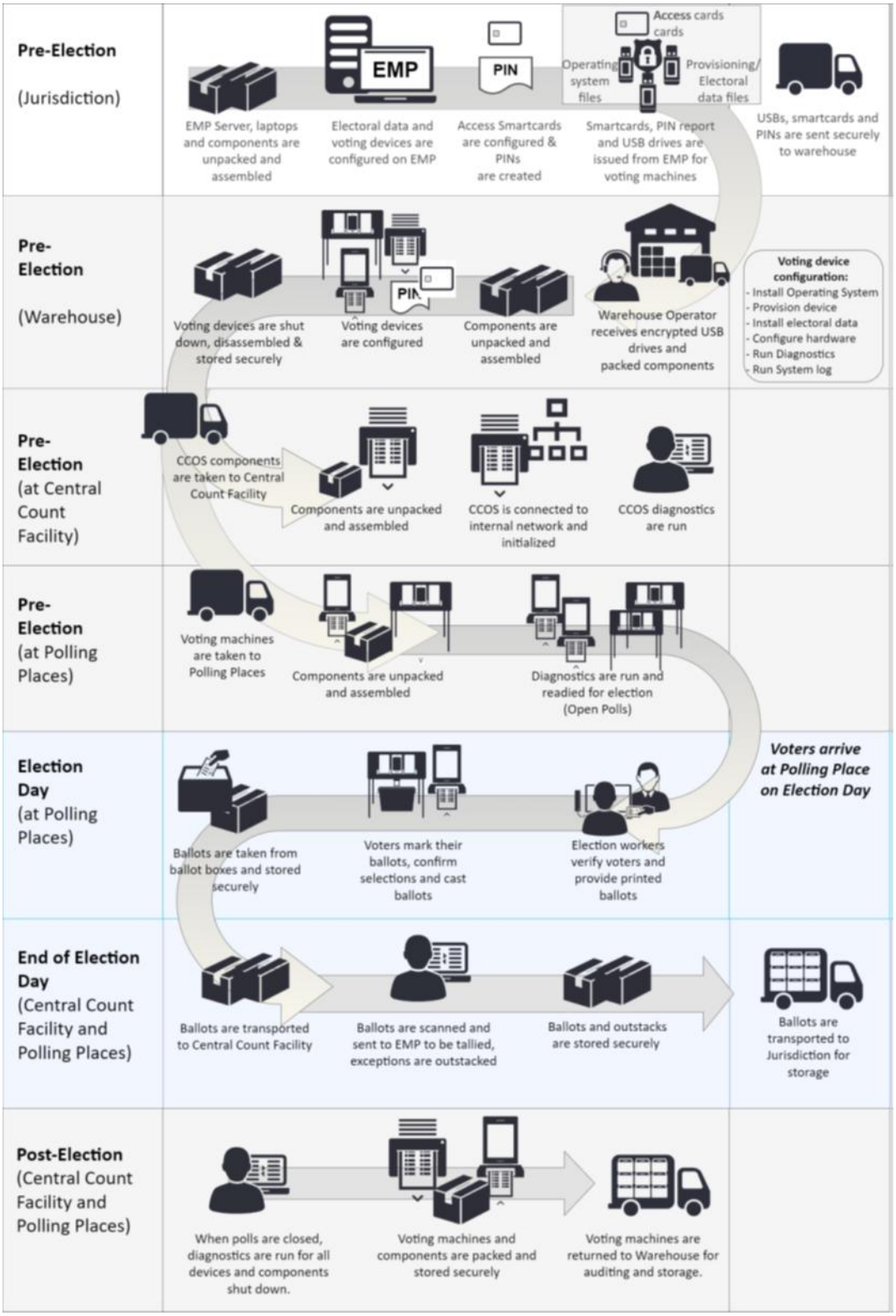

Figure I-2 Operational Process of the Smartmatic VSR1 2.1

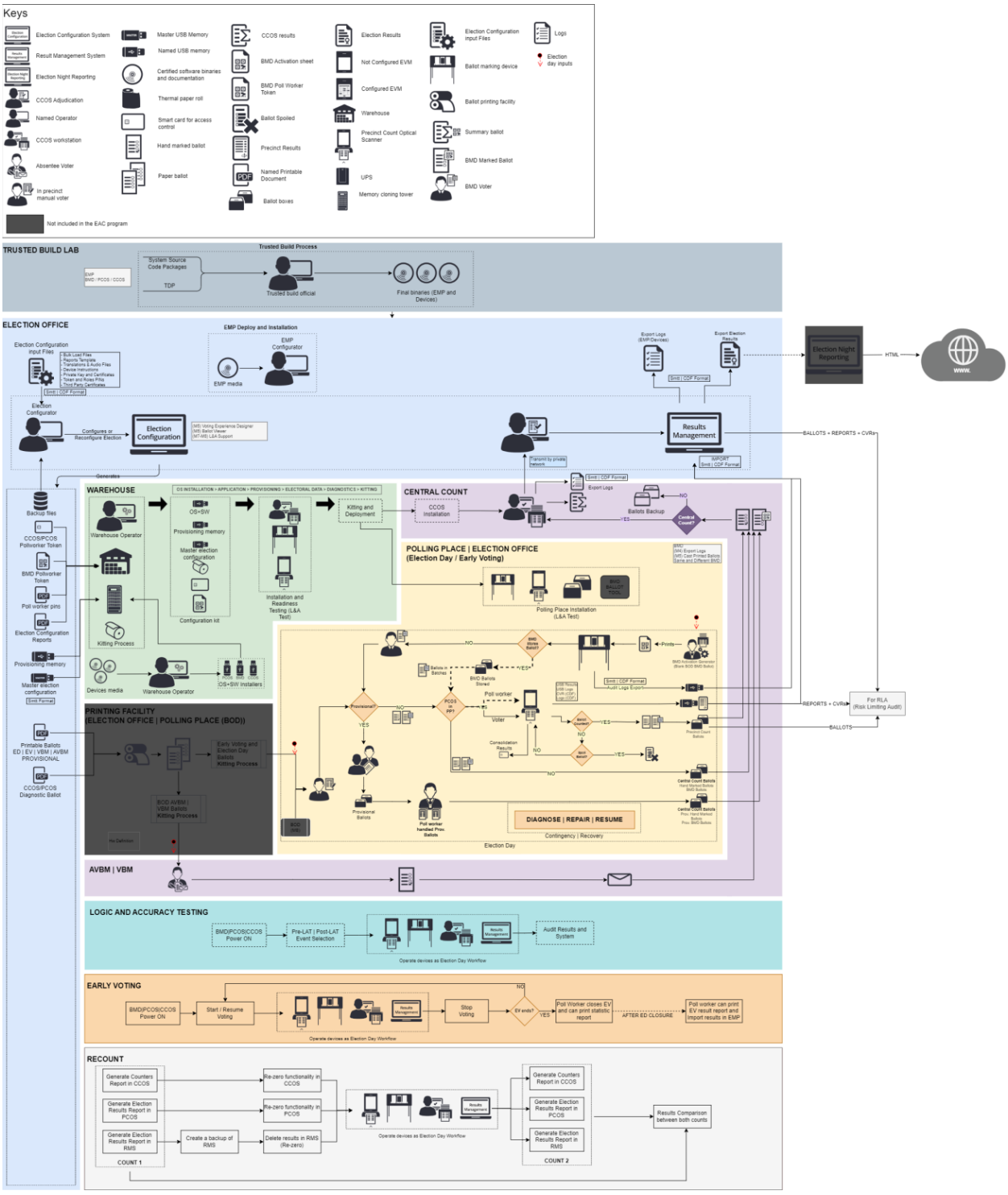

Figure I-3 Solution Deployment Diagram of the Smartmatic VSR1 2.1

SECTION I.3.1.2 SYSTEM LIMITS

Smartmatic has defined the following system performance characteristic limits for the Smartmatic VSR1 2.1 under a specific configuration:

Table I-1 System Limits

Parameter	Definition	Component Affected	System Limit
Max. Subdivisions levels	The subdivisions represent the jurisdiction configuration of the system as State, county, etc.	EMP	47
Max. Precincts per election	Subdivision of an electoral district, typically a contiguous area within which all electors go to a single polling place to cast their ballots.	Performance* Reports (EMP)	1000
Max. Splits Precincts per election	A subdivision of a precinct which arises when a precinct is split by two or more election districts that may require different ballot styles. Synonyms: split, split precinct, sub-precinct	Performance* Reports (EMP)	400
Max. Districts per election	A territorial subdivision for electing members to a legislative body. Generally, only voters (constituents) who reside within the district are permitted to vote in an election held there.	Reports (EMP)	1500
Max. Polling places per election	Location at which voters may cast in-person ballots under the supervision of election workers during one or more specific time periods. Synonyms: poll, polling station 22	Reports (EMP)	220
Max. Parties (General Election)	Number of parties defined for a General Election	Ballot size EMP Performance Reports Voting experience	20
Max. Contests per election	Number of contests in the election. The contests depend on the voting variations.	Ballot size EMP Performance Reports Voting experience	200
Max. Choices (candidates+yes/no) per contest	Number of candidates defined for a single contest	Ballot size EMP Performance Reports Voting experience	2140

Table I-1 System Limits *(continued)*

Parameter	Definition	Component Affected	System Limit
Max Offices per election	A position established by law with certain associated rights and duties.	Ballot size EMP Performance Reports Voting experience	200
Max. Devices per election	Number of devices associated in a polling place	-	821
Max. Devices per election Election day	Number of devices associated in a polling place	-	PCOS: 400 BMD: 400
Max. Devices per election Early Voting/Voting Center	Number of devices associated in a polling place	-	PCOS: 8 BMD: 8
Max. Devices per election Absentee	Number of devices associated in a polling place	-	CCOS: 4
Max. Write-ins per contest	Number of write-ins options defined for a single contest	Ballot Reports	1 1 contest with write in (30 certified write-ins)
Min. "Vote for" per contest	Definition of N - M values for a specific contest	Ballot	1
Max. "Vote for" per contest	Definition of N - M values for a specific contest	Ballot	99
Max. Languages per election	Languages that can be used in the election, including text and audio	Performance (EMP) Ballot Device Idle Screen (BMD, PCOS)	4
Max. Events per election (Pre-LAT, Official)	Events supported in a specific election.	-	2
Central Count max cards per batch	Ballots scan per batch	-	400 ballots

Table I-1 System Limits *(continued)*

Parameter	Definition	Component Affected	System Limit
Ballot lengths	Ballot lengths that can be used in the election.	-	PCOS and CCOS: • 8.5 X 11" • 8.5 X 14" • 8.5 X 17" • 8.5 X 19" • 8.5 X 21" BMD: • 8.5 X 11" • 8.5 X 13.25”

SECTION I.3.1.3 SUPPORTED LANGUAGES

The Smartmatic VSR1 2.1 supports the following languages:

- English
- Spanish
- Chinese
- Russian

Per Smartmatic Voting Systems, the Smartmatic VSR1 2.1 is capable of displaying and printing the ballot, contest options, review screens, ballots, and voting instructions in all supported languages, in both visual and audio formats, where applicable. The Smartmatic VSR1 2.1 does not support non-written languages. Additionally, EMP's base language is English; however ballots and election configuration files can be generated in the supported languages.

During testing, support for all stated languages will be verified; however, only English and Spanish language ballots will be cast during the performance of functional testing. One character based language (Chinese) will be tested during System Integration Testing. Additionally, Pro V&V will execute tests designed to verify the Smartmatic VSR1 2.1:

- Is capable of displaying and printing the ballot, contest options, review screens, voter verifiable paper records, and voting instructions in all languages the manufacturer has declared the system supports, in both visual and audio formats where applicable.
- Is capable of presenting all information that is presented to the voter in English in all other languages that are supported, whether the language is in visual or audio format.
- Visibly presents the controls to identify or change language on the screen at all times, not hidden within a help or settings feature and includes the native version of each language name in the list of language options.

SECTION I.3.1.4 SUPPORTED FUNCTIONALITY

The Smartmatic VSR1 2.1 is designed to support the following voting variations:

- General Election
- Partisan Closed Primary Election
- N-of-M
- Issue Contest
- Precinct Splits
- Ballot Rotation
- Write-ins
- Party Affiliations

During the test campaign, Pro V&V will execute tests designed to verify the Smartmatic VSR1 2.1:

- Provides the capability to define and identify contests, contest options, candidates, and ballot questions using all voting variations identified by Smartmatic.
- 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.3.2 HARDWARE CONFIGURATION AND DESIGN

The Smartmatic VSR1 2.1 Voting System consists of the following major components: the Election Management Platform (EMP), a Ballot Marking Device (BMD), a Precinct Count Optical Scanner (PCOS), and a Central Count Optical Scanner (CCOS).

The following paragraphs provide an overview of the Smartmatic VSR1 2.1, as provided by Smartmatic:

The Election Management Platform is a software-based product running on COTS computing hardware and provides for the back-office management of election lifecycle functions such as ballot layout and results reporting. Data at rest and in motion in the client-server network is encrypted and all data exported from EMP, such as voting machine files is digitally signed. As mentioned below the CCOS scanners also connect to the EMP client-server network via switches and firewalls. The minimum specifications for the EMP Server are 16 GB dual rank RAM, 480 GB SSD HD capacity, and a 2 CPU configuration Xenon 4300 series processor (12c/24t). The minimum specifications for the EMP Client are 16 GB RAM, 512 GB HD capacity, and an Intel i7 processor with IPU.
The BMD accepts signed election configuration file packages from EMP that provide each unit with the election configuration including ballot audio as provisioned by the jurisdiction. It is important to note that the BMD marks but does not tabulate ballots. The BMD has a voter reachable 3.5mm audio jack and a

voter reachable 3.5mm two-channel device jack to allow for headphones and personal assistive devices such as sip and puff units.

The PCOS also accepts signed election configuration file packages from EMP. It scans and tabulates hand marked paper ballots.

Both in-person vote capture devices, the BMD and the PCOS, are provisioned via USB removable memory devices. Open and Close Poll reports are produced from printers integral to each unit. Both the BMD and PCOS are Smartmatic proprietary hardware devices produced from COTS electronic piece parts and custom metal and plastic enclosure parts.

The Central Count Optical Scan system (CCOS) uses COTS computing hardware and a COTS Canon brand scanner, model DR-G2140. A COTS computer is attached to each scanner via USB, and manages the scanner and resulting ballot image pairs. There is also an Ethernet connection from that computer to the EMP instance for upload of scanned image pairs for subsequent tabulation. Network switches and firewalls allow for both Ethernet traffic and a degree of protection from intrusion into the closed, isolated EMP network. Both EMP and CCOS can therefore be classified as "back office" system components, housed within jurisdiction facilities. This is in contrast to the BMD and PCOS which are deployed to polling places. The minimum specifications for the CCOS are 16 GB RAM, 256 GB SSD HD capacity, and an Intel i5 processor.

Election back-up and archive/restore utilize external hard drives to store those election artifacts.

Jurisdictions will always need to deploy EMP in their voting system, as well as the BMD to allow for accessible voting. One or both of the PCOS and CCOS are also needed since BMD units do not tabulate the ballot thus those ballots must be scanned in order to be tabulated. The only documented system configurations are: EMP+BMD+PCOS, EMP+BMD+CCOS, or EMP+BMD+PCOS+CCOS.

SECTION I.3.3 SOFTWARE SYSTEM FUNCTIONS

The Smartmatic VSR1 2.1 Voting System is a set of software written in Java, JavaScript, C++ and Typescript that runs on a Linux operating system, with customized Docker Containers installed onto the EMP Server. The Smartmatic VSR1 2.1 Voting System is designed for use in two distinct locals: Central Processing and In-Precinct Systems.

The functions of the voting system software and other relevant functionality, including items on pre-election, election, and post-election, are contained in Table I-2.

Table I-2 Software System Functions

Component	Mode of Operation		
	pre-election	**election**	**post-election**
EMP	• import information in CDF • create and manage ballot layout • layer in ballot audio • allow for ballot proofing/editing • generate ballot pdf's • generate machine files	N/A	• aggregate results, images, logs report results • support post-election audits • back-up/archive elections
BMD	• intake election definition machine files • perform pre-election logic and accuracy • Preparation of devices including sealing of USB or other ports • Perform device diagnostics	• physical sealing of ports, and ballots boxes with tamper proof labels or with secured zip ties • capture in-person voting sessions (touchscreen) • allow for accessible voting • provide ballot accounting • open/close reports	• log extraction • device audits (logs, seals)
PCOS	• intake election definition machine files • perform pre-election logic and accuracy • Preparation of devices including sealing of USB or other ports • Perform device diagnostics	• physical sealing of ports, and ballots boxes with tamper proof labels or with secured zip ties • scan and tabulate in-person voting sessions (hand marked paper ballot) • allow for accessible ballot review (BMD and hand marked paper) • provide ballot accounting and results reports	• log extraction • device audits (logs, seals)
CCOS	• intake election definition machine files • perform pre-election logic and accuracy • Preparation of devices including sealing of USB or other ports • Perform device diagnostics	• scan and tabulate absentee ballots (hand marked paper ballot, and can also scan BMD generated ballots) • provide ballot accounting and results reports	• log extraction • device audits (logs, seals)
NOTE: PCOS and CCOS may be used for post-election audits and recounts, depending on State law			

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 Smartmatic VSR1 2.1 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-3 details the VVSG 2.0 Principles, Guidelines, and associated test areas.

Table I-3 VVSG 2.0 Test Areas

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

Table I-3 VVSG 2.0 Test Areas *(continued)*

VVSG 2.0 Guideline	VSTL Test Areas
(continued) 2.6 - The voting system handles errors robustly and gracefully recovers from failure. 2.7 - The voting system performs reliably in anticipated physical environments.	*(continued)*
Principle 3: Transparent *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. 3.2 - The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection. 3.3 - The public can understand and verify the operations of the voting system throughout the entirety of the election.	TDP Review, Usability, FCA, System Integration Testing
Principle 4: Interoperable *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. 4.2 - Standard, publicly available formats for other types of data are used, where available. 4.3 - Widely-used hardware interfaces and communications protocols are used. 4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.	Interoperability, TDP Review, FCA, System Integration Testing, PCA
Principle 5: Equivalent and Consistent Voter Access *All voters can access and use the voting system regardless of their abilities.*	
5.1 - Voters have a consistent experience throughout the voting process within any method of voting. 5.2 - Voters receive equivalent information and options in all modes of voting	Usability, Accessibility, FCA, TDP Review
Principle 6: Voter Privacy *Voters can mark, verify, and cast their ballot privately and independently.*	
6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections. 6.2 - Voters can mark, verify, and cast their ballot or other associated cast vote record, without assistance from others	Usability, Accessibility, FCA, TDP Review

Table I-3 VVSG 2.0 Test Areas *(continued)*

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

Table I-3 VVSG 2.0 Test Areas *(continued)*

VVSG 2.0 Guideline	VSTL Test Areas
(continued) 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.	*(continued)*
Principle 11: Access Control *The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.*	
11.1 - The voting system enables logging, monitoring, reviewing, and modifying of access privileges, accounts, activities, and authorizations. 11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access. 11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. 11.4 - The voting system's default access control policies enforce the principles of least privilege and separation of duties. 11.5 - Logical access to voting system assets are revoked when no longer required	Security Testing, Vulnerability Testing, FCA
Principle 12: Physical Security *The voting system prevents or detects attempts to tamper with voting system hardware.*	
12.1 - The voting system supports mechanisms to detect unauthorized physical access. 12.2 - 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 *The voting system protects data from unauthorized access, modification, or deletion.*	
13.1 –The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. 13.2 - The source and integrity of electronic tabulation reports are verifiable. 13.3 - All cryptographic algorithms are public, well-vetted, and standardized.	Security Tests, FCA, TDP Review, Cryptographic Testing

Table I-3 VVSG 2.0 Test Areas *(continued)*

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

Pro V&V has determined that Requirements associated with E2E Verifiable Voting Systems or Ranked Choice Voting (RCV) functionality are not applicable to the Smartmatic VSR1 2.1 System. These Requirements include the following:

1.1.4-M – Ranked choice voting contest, Casting

1.1.8-J – Ranked choice voting contest, Tabulation

1.1.9-I – Ranked choice voting, report results

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 – Cryptographic ballot selection verification by voter

9.1.6-D – Methods for cryptographic ballot selection verification

9.1.6-E – Ballot receipt

9.1.6-F – Disputes involving ballot receipts

9.1.6-G – Evidence export

9.1.6-H– Mandatory ballot availability

9.1.6-I – Verification of encoded vote documentation

9.1.6-J – Verifier reference implementation

9.1.6-K – Privacy preserving, universally verifiable ballot tabulation

Additionally, a *VVSG 2.0 Cross Reference Matrix* specific to the Smartmatic VSR1 2.1 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 names and titles of 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.

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 NTS Longmont facility located in Longmont, Colorado. All testing will be witnessed on-site by Pro V&V personnel, with the exception of 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

The Smartmatic VSR1 2.1 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 Smartmatic VSR1 2.1 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 testing was to assess the security posture of the Smartmatic VSR1 2.1 voting system 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 the Smartmatic VSR1 2.1 was considered for this test campaign.

SECTION II.3 KNOWN FIELD ISSUES

The Smartmatic VSR1 2.1 is being submitted for evaluation as a new system that has not been fielded; therefore, there are no fielded systems preceding this system. The Smartmatic VSR1 2.1 may serve as the baseline to subsequent systems submitted for evaluation at a later date. At that time, any known field issues on the baseline system or any subsequent certified versions derived from the Smartmatic VSR1 2.1 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 of the Smartmatic VSR1 2.1 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 to be provided by the manufacturer as part of the test campaign.

Table III-1 VSR1 2.1 Software

Configuration Item	Description	Source
EMP		
Application Version	8.9.51.4	Smartmatic
OS Version	Base OS: Ubuntu 20.04.6 LTS AMD64	Canonical

Table III-1 VSR1 2.1 Software *(continued)*

Configuration Item	Description	Source
Platform	Linux	Linux
OS-level virtualization	Docker 27.5.1	Docker
Audit log data visualization tool	Auditd, Apparmor, rsyslog	Ubuntu
	Kibana/Elastic-Search	Elastic
Database	Oracle Database 18.4-xe	Oracle
CCOS		
Application Version	1.40.0	Smartmatic
OS version	7.3.0 en_US.UTF-8 (default language) Base OS: Ubuntu 24.04.2 LTS	Smartmatic
Platform	Linux	Linux
BMD		
Application Version	1.4.5	Smartmatic
OS Version	7.3.0 en_US.UTF-8 (default language) Base OS: Ubuntu 24.04.2 LTS	Smartmatic
Platform	Linux	Linux
PCOS		
Application Version	1.40.0	Smartmatic
OS version	7.3.0 en_US.UTF-8 (default language) Base OS: Ubuntu 24.04.2 LTS	Linux
Platform	Linux	Linux

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.

Table III-2 VSR1 2.1 Hardware/Equipment

Configuration Item	Description	Source
EMP		
EMP Server	PowerEdge T550 Parallax Security Bezel, Two Layer Door	Dell
EMP Election Official Laptop	Dell Latitude 5520	Dell
Firewall Appliance	Fortinet FortiGate 40F	Fortinet
Network switch	Cisco CBS350-8P-E-2G	Cisco
UPS	APC Smart-UPS (SMT1500C)	APC
External Hard Drive	SanDisk 2TB Extreme Portable SSD	SanDisk
Smartcard reader	Model: ACR39U Part Number: ACR39U-U1	ACS
Monitor	Dell 24 E2422H	Dell
Keyboard	Dell Business Multimedia Keyboard - KB522	Dell
Mouse	Dell Optical Mouse- MS116	Dell
Printer	HP LaserJet Pro 4001n	HP
VGA cable	Generic VGA to VGA Cable 6 Feet	Dell
USB Locks with key	40452 Blue	Lindy
RJ45 Port blocker with key	40470	Lindy

Table III-2 VSR1 2.1 Hardware/Equipment *(continued)*

Configuration Item	Description	Source
CCOS		
Scanner	imageFORMULA DR-G2140 Imprinter Unit 3601C001	Canon
Device	Dell OptiPlex 3000 micro	Dell
File storage	Dell M.2 256GB PCIe NVMe Class 35 Solid State Drive	Dell
Display	Elo M-Series 1502L 15-inch	Elo
Printer	HP Laser Jet Pro 4001n	HP
Smart card Reader	Model: ACR39U	ACS
UPS	APC Smart-UPS (SMT1500C)	APC
USB hub	Hub	Anker
BMD		
BMD Main Unit	BMD-155 (RC5)	Smartmatic
Ballot Box	BBX-151	Smartmatic
Leg Stand	BLS-155	Smartmatic
Privacy Flap	BPF-155	Smartmatic
Power Adapter & Cable	24DC V @ 6.25 Amp	Smartmatic
UPS	APC UPS (BR1500MS2)	APC
Accessibility Devices	Sip-and-Puff AC-0304-V2	Origin instrument
Accessibility Devices	Buddy Buttons SWP1	Origin instrument
Accessibility Devices	CD-46 Over-Ear Stereo Headphones	Yoga Electronics
Accessibility Devices	Stylus – B07WRQYQFF	Zerone
Accessibility Devices	Audio Tactile Interface (ATI) device KPB200	Smartmatic
PCOS		
PCOS	A4-800	Smartmatic
Ballot Box	BBX-800	Smartmatic
Power adapter and cable	• 100-240 V AC • 50/60Hz	Smartmatic
Privacy flaps	PPF-800	Smartmatic
Accessibility Devices	Sip-and-Puff AC-0304-V2	Origin instrument
Accessibility Devices	Buddy Buttons SWP1	Origin instrument
Accessibility Devices	CD-46 Over-Ear Stereo Headphones	Yoga Electronics
Accessibility Devices	Stylus - B07WRQYQFF	Zerone
Accessibility Devices	Audio Tactile Interface (ATI) device KPB200	Smartmatic

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 VSR1 2.1 Materials/Consumables

Configuration Item	Description	Source
EMP		
Materials		
Smartcards	ACOS3 (Contact) Series	ACS
USB memory drives	8GB capacity USB drives for installing operating system	SanDisk or similar
USB memory drives for voting devices	USB drives for the provisioning of voting machines and for encrypted election data for each voting device, Minimum 8GB capacity in EXT3 format	Smartmatic
Passwords and PINs	Key passwords and PINs (in electronic or physical format).	Smartmatic
Security Lock	N17 Laptop T-bar – Keyed • Super-strong, steel composite cable with carbon-tempered steel core • Patented T-bar lock provides theft protection	Kensington
Manuals	• *EMP Installation Manual* • *EMP Maintenance Manual* • *EMP User Manuals* • *EMP Hardware Manuals* • *EMP Troubleshooting Manual*	Smartmatic
Consumables		
Serialized Tamper-evident security seals	• USB Port Blockers #40462	Lindy
	• RJ45 Port Blockers #40471	Lindy
	• UltraGuard™ #XUG6-K222-60SN Tamper Evident Security Labels	NovaVision
Paper	• Ream of 8.5 x 11" white bond paper	Generic
Printer consumables	• Toner cartridges: o HP 148A (page yield ~2,900 pages) o HP 148X (page yield ~9.500 pages)	HP
Local Area Network		
Cables	LAN connection cables • Red Cat 5 Ethernet Cable • White Cat 5 Ethernet Cable • Blue Cat 5 Ethernet Cable USB Cables	Amazon basics
CCOS		
Smart cards	Smart card ACOS3 Microprocessor Card • election worker card	ACS
USB memory drive	• 8GB in EXT3 format • Unlocker files • Operating system files • Provisioning files • Electoral data files	Smartmatic

Table III-3 VSR1 2.1 Materials/Consumables *(continued)*

Configuration Item	Description	Source
Manuals	• *CCOS Installation Manual* • *CCOS User Manual* • *CCOS Troubleshooting Manual* • *Canon imageFORMULA DR-G2140 User Manual* • *Printer HP LaserJet Pro 4001 User Guide* • *ACR39-Series-1.05* • *APC SMT 1500 Operation Manual*	Smartmatic Canon ACS HP APC
Ethernet patch cable	CAT6 (with colors)	Amazon basics
Consumables		
Serialized tamper evident security labels	• USB Port Blockers #40462	Lindy
Serialized tamper evident security labels	• RJ45 Port Blockers #40471	Lindy
Serialized tamper evident security labels	• UltraGuard #XUG6-K222-60SN • Tamper Evident Security Labels	NovaVision
Ink cartridges for scanner (imprinter)	Ink Black cartridge C6602A Ink Blue cartridge C6602B Ink Green cartridge C6602G	HP
Roller replacement Kit for scanner	3601C002	Canon
Toner cartridges for printer	148A Black Original LaserJet Toner Cartridge	HP
Diagnostic ballots or paper	Ballot paper for absentee ballots and provisional ballots	Smartmatic
Printer paper	Ream of 8.5 x 11"	Generic
BMD		
Materials		
User Authentication Token	QR Code	Smartmatic
USB Memory Drive	• Unlocker • Operating system files • Electoral data files	Smartmatic
Manuals	• *BMD Installation Manual* • *BMD Setup Inspection* • *BMD User Manual* • *BMD Maintenance Manual* • *BMD Troubleshooting Manual*	Smartmatic
Paper	Paper Ballots • Mitsubishi TF 1467 Thermal paper 8.5 x 13.25 inches with 0.63" notched corner	Mitsubishi

Table III-3 VSR1 2.1 Materials/Consumables *(continued)*

Configuration Item	Description	Source
Consumables		
Serialized tamper-evident security seals	• Plastic Numbered Disposable Self-Locking Security Seals • Handilok HL-8 Padlock Seal - TydenBrooks	TydenBrooks
Serialized tamper-evident security seals	• Plastic zip ties #625-40095-RD • Security zip ties - red color: 250	BankSupplies
Serialized tamper-evident security seals	• Labels • SW-90031 - Tamper Evident Security Labels	Solitary Walker
Paper Ballots	• Mitsubishi TF 1467 Thermal paper 8.5 x 13.25 inches with 0.63" notched corner	Mitsubishi
Accessibility	Set of Sanitized Headphone Covers, 60mm, BBTO-Earpads-e1083 or similar	Scansound
PCOS		
Materials		
Smartcard	Smart card ACOS3 • election worker card	ACS
USB Memory Drive	• Unlocker files • Operating system files • Provisioning files • Electoral data files	Smartmatic
Manuals	• *PCOS Installation Manual* • *PCOS User Manual* • *PCOS Troubleshooting Manual*	Smartmatic
Consumables		
Serialized tamper-evident security seals	• Plastic Numbered Disposable Self-Locking Security Seals • Handilok HL-8 Padlock Seal - TydenBrooks	TydenBrooks
Serialized tamper-evident security seals	• Plastic zip ties #625-40095-RD • Security zip ties - red color: 250	BankSupplies
Paper	Calibration ballot (blank paper A4/Letter/Legal size)	Mitsubishi
Paper	Paper ballots	• Rolland Hi-tech • Accent Opaque (100# text) • Domtar Lynx (100# text)
Paper	Diagnostic ballots	Smartmatic
Paper	Thermal paper (printer)	• Alpestech Co., Ltd. 台北. Model: A4-800 • Koelher Thermal paper Model: K T 75 FA

Table III-3 VSR1 2.1 Materials/Consumables *(continued)*

Configuration Item	Description	Source
Markers	Medium point (1mm) • Quick dry (no smudge) • Not bleed trough (test with paper to be used)	Recommended: • Smartmatic marker Brand: Smartmatic Model: PCOS Marker • Lumocolor Non-Permanent M Brand: Staedtler Model Lumocolor non-permanent. Medium Point. Black SKU: 315-9 • Stabilo Pen 68 • Stabilo PointMax
Accessibility	Set of Sanitized Headphone Covers 60mm, BBTO-Earpads-e1083 or similar	Scansound

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 Smartmatic VSR1 2.1 submitted for evaluation will be performed to ensure the applicable requirements of the VVSG 2.0, the VVSG 2.0 Test Assertions, Version 1.3 (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 Smartmatic VSR1 2.1 test requirements, each Principle of the VVSG 2.0 will be analyzed in conjunction with a preliminary TDP review to determine the applicable Requirements. The preliminary TDP is performed to gather information concerning the system under test and its capabilities or design intentions. Additionally, a TDP review will be performed throughout the test campaign. The TDP Review includes the Initial Review, the Regulatory/Compliance Review, and the Final Review. This review is conducted to determine if the submitted technical documentation meets the regulatory, customer-stated, or end-user requirements and includes reviewing the documents for stated functionality review and verification. The Pro V&V-designated Test Areas utilized to evaluate the Smartmatic VSR1 2.1 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 Smartmatic VSR1 2.1. 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. Test cases shall be based on the following aspects of the voting system: Hardware qualitative examination design, Hardware environmental test case design, Software module test case design and data, Software functional test case design, and System level test case design. Test cases shall provide information regarding the sequence of actions to be performed for the execution of a test, the requirements being met, the test objective, test configuration, equipment needed, special requirements, assumptions, and pass/fail criteria.

Once the test cases are finalized, they will be validated and published for use in the test campaign. The validation of the test case will be accomplished by technical review and approval. This validation will include the following: confirmation of adequate test coverage of all requirements; confirmation that test case results are not ambiguous and gave objective pass/fail criteria; and confirmation that any automated test suites will produce valid results. All Smartmatic-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 Smartmatic VSR1 2.1. 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 shall 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 shall design additional test cases to as needed to satisfy all specified coverage criteria. Component Level Testing will be implemented during the FCA for each component and subcomponent. During the source code review, compliance builds, and security testing, Pro V&V will utilize limited structural-based techniques (white-box testing). Additionally, specification-based techniques (black-box testing) will be utilized for the individual software components.

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

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

SECTION IV.2.3 SOFTWARE FUNCTIONAL TEST CASE DESIGN AND DATA

Pro V&V shall review the manufacturer-submitted test plans and data to verify that the individual performance requirements specified in the VVSG 2.0 and the TDP are reflected in the software. As part of this process, Pro V&V shall review the manufacturer's test case design and prepare a detailed matrix of system functions and the test cases that exercise them. Following analysis and validation of the Smartmatic-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 performed to determine the cause. The test will be repeated in an attempt to reproduce the results. If the failure can be reproduced and the expected results are not met, the system will have failed the test. If the results cannot be reproduced, the test will continue. All errors encountered will be documented and tracked through resolution.

SECTION IV.2.4 SYSTEM-LEVEL TEST CASE DESIGN

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

SECTION IV.3 TEST PROCEDURE DEVELOPMENT AND VALIDATION

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

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

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

SECTION V: TEST PROCEDURES

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

SECTION V.1 PHYSICAL CONFIGURATION AUDIT (PCA)

The Physical Configuration Audit (PCA) compares the voting system components submitted for qualification 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

In order 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 the Smartmatic VSR1 2.1 TDP is provided in Table V-1.

Table V-1 VSR1 2.1 TDP Documents

Document ID	Description	Version
1 – EMP Manuals		
SMT-2022-EMP-INM-01	EMP Installation Manual	12
SMT-2022-EMP-INM-02	EMP Workstation Getting Started Guide	3

Table V-1 VSR1 2.1 TDP Documents (continued)

Document ID	Description	Version
SMT-2022-EMP-MNM	EMP Maintenance Manual	9
SMT-2022-EMP-STP	EMP Setup Inspection	9
SMT-2022-EMP-SYS-01	EMP Data Bulk Load Specifications	7
SMT-2022-EMP-TSM	EMP Troubleshooting Manual	10
SMT-2022-EMP-USM-00	EMP Getting Started Guide	1
SMT-2022-EMP-USM-01	EMP User Manual - System Administration	9
SMT-2022-EMP-USM-02	EMP User Manual - Election Management	10
SMT-2022-EMP-USM-03	EMP User Manual – Results Management	8
SMT-2022-EMP-USM-04	EMP User Manual – Jurisdiction Dashboard	3
2 – BMD Manuals		
SMT-2022-BMD-INM	BMD Installation Manual	12
SMT-2022-BMD-MNM	BMD Maintenance Manual	11
SMT-2022-BMD-STP	BMD Setup Inspection	9
SMT-2022-BMD-TSM	BMD Troubleshooting Manual	9
SMT-2022-BMD-USM	BMD User Manual	15
3 – PCOS Manuals		
SMT-2022-PCOS TSM	PCOS Troubleshooting Manual	8
SMT-2022-PCOS-INM	PCOS Installation Manual	13
SMT-2022-PCOS-MNM	PCOS Maintenance Manual	11
SMT-2022-PCOS-STP	PCOS Setup Inspection	10
SMT-2022-PCOS-USM	PCOS User Manual	13
4 – CCOS Manuals		
SMT-2022-CCOS-INM	CCOS Installation Manual	10
SMT-2022-CCOS-MNM	CCOS Maintenance Manual	9
SMT-2022-CCOS-STP	CCOS Setup Inspection	9
SMT-2022-CCOS-TSM	CCOS Troubleshooting Manual	9
SMT-2022-CCOS-USM	CCOS User Manual	11
5 – TDP		
SMT-2022-EMP-TBP	EMP Trusted Build Procedures	11
SMT-2022-EVM-TBP	EVM Trusted Build Procedures	8
SMT-2022-QPL	Master QA Plan	7
SMT-2022-TDP-01	Implementation Statement	12
SMT-2022-TDP-02	System Overview	16
SMT-2022-TDP-03	System Performance	11
SMT-2022-TDP-04	System Operations	8
SMT-2022-TDP-05	System Security Specification	9
SMT-2022-TDP-05-01	Security Architecture	6
SMT-2022-TDP-05-02	Security Policy (Secure Operations)	8
SMT-2022-TDP-05-03	Key Management	11
SMT-2022-TDP-05-04	Smartmatic Protection Model	8
SMT-2022-TDP-05-05	Supply Chain Risk Management	6
SMT-2022-TDP-05-06	Criticality Analysis	3
SMT-2022-TDP-05-07	Vulnerability Management Plan	7

Table V-1 VSR1 2.1 TDP Documents (continued)

Document ID	Description	Version
SMT-2022-TDP-06	Personnel Deployment & Training	6
SMT-2022-TDP-07	Paper & Ballot Specifications	9
SMT-2022-TDP-08	System Functionality Description	11
SMT-2022-TDP-09-01	EMP Hardware Specification	10
SMT-2022-TDP-09-02	BMD Hardware Specification	10
SMT-2022-TDP-09-03	PCOS Hardware Specification	10
SMT-2022-TDP-09-04	CCOS Hardware Specification	8
SMT-2022-TDP-10	Software Design and Specification	9
SMT-2022-TDP-10-01	EMP Programming Specifications	8
SMT-2022-TDP-10-02	EMP Database Specification	v8.9.51.4
SMT-2022-TDP-10-03	PCOS and CCOS Programming Specifications	7
SMT-2022-TDP-10-04	BMD Programming Specifications	7
SMT-2022-TDP-10-05	Design and Interface Specification	10
SMT-2022-TDP-10-06	Smartmatic Coding Conventions and Guidelines	6
SMT-2022-TDP-ATM	Logic and Accuracy Testing Manual	6
SMT-2022-TDP-ATS	System Audit Type Specifications	7
SMT-2022-TDP-AUP	System Audit Procedures	7
SMT-2022-TDP-BCS	System Barcode Specifications	8
SMT-2022-TDP-BCS (PUB)	System Barcode Specifications	2
SMT-2022-TDP-CDS	System Common Data Format Specifications	7
SMT-2022-TDP-CDS (PUB)	System Common Data Format Specifications	1
SMT-2022-TDP-SLS	System Log Event Code Specifications	10
SMT-2022-TDP-SLS (PUB)	System Log Event Code Specifications	2
SMT-2022-CPL	Configuration Management Plan	8
5 – TDP BOM		
A4-800-A0.1	Bill of Material A4-800 Rev. A01.1-BOM	A
BMD-155 RC5	e-BOM (Engineering Bill of Materials)	A
CCS BOM	CCOS Bill of Materials	Rev.2024.11.07
EMP BOM	EMP Bill of Materials	Rev.2023 0412
VSR1-SBoM	VSR1-System Bill of Materials	20230203
5 – TDP Benchmark Directory Listings		
---	usa-vvsg-2022-evapplication_h-bmd155-installed-file	2/6/2023
---	usa-vvsg-2023-ccapplication_l-ccos-installed-files	2/6/2023
---	usa-vvsg-2023-emp-server-docker-lv-installed-files230201	2/6/2023
---	usa-vvsg-2023-emp-server-root-lv-instaled-files-20230201	2/6/2023
---	usa-vvsg-2023-emp-workstation-installed-files-20230201	2/6/2023
---	usa-vvsg-2023-pcapplication_l-pcos-installed-files	2/6/2023

Table V-1 VSR1 2.1 TDP Documents *(continued)*

Document ID	Description	Version
5 – TDP Compliance Matrix		
---	BMD Compliance Matrix	2/14/2025
---	EMP Compliance Matrix	2/14/2025
---	PCOS-CCOS Compliance Matrix	2/14/2025
---	Documentation Compliance Matrix	2/14/2025
5 – TDP FMEA		
---	BMD FMEA VSR1	2.1
---	PCOS FMEA VSR1	0.1
5 – TDP General Build Quality		
---	Factory Quality Control Standard	9/4/2014
---	Mass Production Process	---
---	Quality Control and Manufacture	2012 05 (R1)
5 – TDP Provider Technical Documentation (COTS) CCOS Hardware Manuals		
---	Reference Guide HP LaserJet Pro 4001n/dn/dw series	2022
---	HP LaserJet Pro 4001, 4002, 4003, 4004, 4101, 4102, 4103, 4104 - Certificate of Volatility	Date Prepared: 2022
PUB. 6T3-0034-E2.00	Canon DR-G2140 User Manual	2018
---	HP LaserJet Pro 4001, 4002 - User Guide	Edition 1, 04/2022
---	HP Business PC & Print Devices Cleaning Guidance	2022
W1A52-90920	LaserJet Pro M304-M305, M404-M405 Getting Started Guide	2018
ACR39 Series – Reference Manual	ACR39 Series PC-linked Smart Card Readers Reference Manual	V1.05
ACR39U-U	ACR39U Specifications	May 2020
---	APC Smart-UPS SMT-1500C Product Data Sheet	3/2013
990-5458D	Installation Guide Smart-UPS SMT750/1000/1500/2200/3000C	02/2022
5 – TDP Provider Technical Documentation (COTS) EMP Hardware Manuals		
---	SanDisk Extreme Portable SSD data sheet	2021
---	Dell E2422H User's Guide	A02
---	Dell EMC PowerEdge T550 Technical Guide	A01
ENVPEP1612028_V1	Smart-UPS 1500 VA Product Environmental Profile	01/2017
FGFWF-40F-DAT-R24	Fortinet FortiGate FortiWiFi 40F Series Data Sheet	20220512
---	Fortinet FortiGate-40F_Regulatory Notices	---
---	Dell Latitude 5520 Setup and Specifications	A02
C78-743894-03	Cisco Business 250 Series Smart Switches Data Sheet	2021
ACR39 Series – Reference Manual	ACR39 Series PC-linked Smart Card Readers Reference Manual	1.05
---	Smart-UPS SMT1500C Product data sheet	3/2013
990-5458D	APC Installation Guide Smart-UPS SMT750/1000/1500/2200/3000C	02-2022

Table V-1 VSR1 2.1 TDP Documents *(continued)*

Document ID	Description	Version
ACR39U-U	PC-Linked Smart Card Reader ACR39U Specifications	Jan 2023
5 – TDP System Security Specifications, Key Management and Risk Assessment		
VSr1 Security Dashboard - Deliverable	Risk Assessment	20231218
5 – TDP Test Cases Catalogue		
---	BMD Test Cases Catalogue	20250221
---	CCOS Test Cases Catalogue	20250221
---	EMP Test Cases Catalogue	20250221
---	Integration Test Cases Catalogue	20250221
---	PCOS Test Cases Catalogue	20250221
5 – TDP Test Plan and Reports		
---	BMD Test Plans and Results	1
---	BMD Test Executions	20250530
---	CCOS Test Plans and Results	1.2
---	CCOS Test Executions	20250530
---	EMP Test Plans and Results	1.4
---	EMP Test Executions	20250530
---	PCOS Test Plans and Results	1.4
---	PCOS Test Executions	20250530
---	System Integration Test Plan and Results	20250530
---	System Integration Test Executions	20250530
5 – TDP UCD Reports		
---	SMT-2022 BMD UCD Reports	20231218
---	SMT-2022 CCOS UCD Reports	20231218
---	SMT-2022 EMP UCD Reports	20231218
---	SMT-2022 PCOS UCD Reports	20231218
---	SMT-2022-TDP-UCD User-Centered Design Report	20231218
5 – TDP Usability Reports		
---	Election Worker Test Report: Smartmatic Voting System	March 16, 2023
---	Usability Test Report: Smartmatic Voting System	March 16, 2023

SECTION V.3 SOURCE CODE REVIEW

Pro V&V will review the submitted source code to the 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 described in the Smartmatic TDP document *SMT-2022-TDP-10 Software Design and Specification*. These tools include Yarn Lint version 1.22.19, SonarSource SA SonarQube platform with Java plugin, version 8.9.16, and Parasoft C/C++test, both of which are listed on the Mitre Common Weakness Enumeration (CWE) Compatibility Product and Services List. To validate the tools, Pro V&V utilized Samate Software Assurance Reference Dataset (SARD). This dataset provides 'Pristine vs. Dirty' sample test data, in this case source code, and a 'Flawed and Fixed' dataset. These samples allow for the tool to be validated. Pro V&V then followed the Smartmatic TDP to install the automatic source code review tools. Once the tools were installed, validated, and the review executed, Pro V&V verified the results obtained matched the expected results. No modifications to the tools are required, only importing of the Smartmatic rule set. Findings from the automated review tool will be manually reviewed to ensure that all source code is VVSG 2.0 compliant.

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

SECTION V.4 FUNCTIONAL CONFIGURATION AUDIT (FCA)

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

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

- Post-voting Capabilities: These functional capabilities apply after all votes have been cast. They include closing the polling place; obtaining reports by voting machine, polling place, and precinct; obtaining consolidated reports; and obtaining reports of audit trails.
- Maintenance, Transportation and Storage Capabilities: These capabilities are necessary to maintain, transport, and store voting system equipment.

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

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

SECTION V.5 SECURITY REVIEW

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

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

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

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

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

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

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

The test methods for performing the Security Testing are execution and review. Prior to performance of Security testing, the examiner will verify that security hardening scripts have been properly applied to system components per the system documentation. The examiner will review the submitted TDP to verify that documented access and physical controls are in place. Following the documented procedures, the examiner will configure the voting system for use and functionality to verify that the documented controls are in place and adequate and meet the stated requirements. The Security Review consists of an Administrative Review, Technical Review, and Physical Review, described as follows:

Administrative Evaluation

The Administrative Security Evaluation begins with reviewing the TDP package for assessor orientation to the system while evaluating the breadth and depth of security topics covered. The documentation will be assessed for coverage, clarity, correctness, consistency, and effectiveness of the documented security controls. The assessment evaluates the security controls' effectiveness in protecting confidentiality, integrity, availability, and accountability within the system. The evaluation also assesses that ample and appropriate controls are implemented within the system to provide adequate protection to the system. This evaluation spans all security defenses and phases mentioned above. The assessment extends beyond the TDP Review to evaluate the compliance in fulfilling the requirements outlined in the VVSG and/or related requirements. The assessment includes a review of the vendor's submitted threat matrix (*VSR1 Security Dashboard*) provided in the TDP to evaluate security controls for effectiveness in protecting again 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:

- EMP: Privilege Escalation, Permissions & Roles, Access Controls
- BMD: Permissions & Roles, Access Controls
- PCOS: Permissions & Roles, Access Controls
- CCOS: Permissions & Roles, Access Controls

Examples of these attacks are provided below:

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

Physical Evaluation

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

- EMP: Removing Protective Measures, Detection & Prevention

- BMD: Removing Protective Measures, Detection & Prevention
- PCOS: Removing Protective Measures, Detection & Prevention
- CCOS: Removing Protective Measures, Detection & Prevention

Examples of these attacks are provided below:

Packet Capture – 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 take 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 Smartmatic VSR1 2.1 system.

Additionally, the Smartmatic VSR1 2.1 submitted threat matrix (*VSR1 Security Dashboard*) 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 Smartmatic.

Pro V&V will use multiple security techniques to examine various security measures of the Smartmatic VSR1 2.1 Voting System. Examples of possible attack vectors may include but are not limited to SQL Injection Attacks, Network Scans, Packet Captures, and Brute Force Attacks. For each component the following tasks may include:

- EMP: SQL Injection Attacks, Network Scans
- BMD: Brute Force Attack
- PCOS: Brute Force Attack
- CCOS: Packet Capture, Brute Force Attack

Examples of these attacks are provided below:

Packet Capture – Using a packet squirrel hardware device, will plug in between the CCOS and EMP Server to examine the packets being sent from one component to the other. Verifying that the packets sent are encrypted

SQL Injection — Using SQL Injection on the EMP Web Application Login screen to try to modify the database

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

Brute Force Attack -Using a rubber ducky to manipulate the system to perform actions that they system was not intended to do

Additionally, network analysis tools will be used to obtain network packet captures to examine communication and authentication attempts between all Smartmatic VSR1 2.1 devices, and to assess that appropriate encryption is utilized across all devices

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 Smartmatic VSR1 2.1 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 Smartmatic VSR1 2.1 system.

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

SECTION V.7 CRYPTOGRAPHIC TESTING

Cryptographic testing will be performed to assess the Smartmatic VSR1 2.1 System to the following Principle:

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

To perform the Cryptographic Testing, qualified personnel will evaluate the system by executing test cases developed to the specified requirements contained within the Principle to verify the system meets the requirements and functions as expected and documented. Qualified personnel will also perform each type of identified evaluation (Administrative, Physical, and Technical/Logical) on the Smartmatic VSR1 2.1 system.

SECTION V.8 USABILITY REVIEW

A Usability Review will be performed to examine how users interact with the system. The purpose of the Usability Review is to assess the usability of the Smartmatic VSR1 2.1 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 of 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 that they also support voters with disabilities throughout the process of voting from activation through casting.

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

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

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

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

SECTION V.10 SYSTEM INTEGRATION TESTING

The System Integration area of testing is a system level test that evaluates the integrated operation of both hardware and software. Compatibility of the voting system software components or subsystems with one another, and with other components of the voting system environment, shall be determined through functional tests integrating the voting system software with the remainder of the system. Additionally, the system shall be configured exactly as it would for normal field use per the procedures detailed in the Smartmatic VSR1 2.1 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 contest 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: Open Primary Election held in two precincts. This election contains thirteen contests compiled into three ballot styles. One contest is in all three ballot styles; all other contests are independent.
- 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 VSR1 2.1 system under test must read a minimum of 10,000,000 ballot positions and tabulate accurately. The requirement shall be broken down by component using the following minimum ballot positions read and tabulated accurately:

BMD – 1,670,000 – Printed and tabulated on a scanner

PCOS – 3,340,000

CCOS – 5,010,000

Total – 10,020,000

Prior to test initiation, a Test Case and Election Definition specific to the Accuracy Test will be developed. The accuracy requirements for the Smartmatic VSR1 2.1 will be met by executing the Test Case utilizing a test deck composed of pre-marked and hand-marked ballots of each ballot length supported by the system. This test deck will be processed until the required minimum number of ballot positions to be tabulated is met.

SECTION V.12 VOLUME TEST

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

SECTION V.13 INTEROPERABILITY

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

Principle 4: Interoperable

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

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

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

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

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

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

1. Review the manufacturer's documentation for import and export features and data format.
2. Use the designated method to produce an export as a flat file.
3. Compare the exported flat file to the common data format specified in the manufacturer's documentation.
4. Note any discrepancies.
5. Alter a value for any entity in the data export.
6. Use the altered data export file to now import the changed data.
7. Use the designated method to import the data.
8. Compare the imported data and ensure the changes made to the exported flat file are now in the appropriate data structure (EMS/ tabulator data structure for a cast vote record/ event logs in the specified common data format).
9. When applicable, verify the election results for export are in the common data format for election night results reporting.

SECTION V.14 HARDWARE TESTING

The Smartmatic VSR1 2.1 is a new system submitted for testing to the VVSG 2.0; therefore, the full suite of Hardware Testing will be required for all components. VVSG 2.0 Hardware Testing consists of electrical hardware testing, an operational environmental test, and various non-operational environmental tests, as described below:

Electrical Hardware Tests

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

Non-Operational Environmental Hardware Tests

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

Operational Environmental Hardware Test

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

Table V-2 VSR1 2.1 Hardware Testing Overview

Hardware Test	VVSG 2.0 Requirement	Applicable Component		
		PCOS	CCOS	BMD
Radiated Emissions	1.2-I	Yes[1]	No	Yes
Conducted Emissions	1.2-I	Yes[1]	No	Yes
Radiated Immunity	2.7-G	Yes[1]	No	Yes
Conducted RF Immunity	2.7-J	Yes	No	Yes
Lightning Surge	2.7-I	Yes	No	Yes
Electrical Fast Transient	2.7-I	Yes	No	Yes
Electrostatic Disruption	2.7-K	Yes	No	Yes
Electrical Power Disturbance	2.7-I	Yes	No	Yes
Low Temperature	2.7-F	Yes	No	Yes
High Temperature	2.7-F	Yes	No	Yes
Bench Handling	2.7-D	Yes	No	Yes
Transportation Vibration	2.7-E	Yes	No	Yes
Continuous Operation – Varied Environmental Conditions	2.7-C	Yes[1,2]	Yes	Yes
Electrical Supply (Battery Backup)	2.7-H	Yes	Yes	Yes

1. *This test will be performed on the PCOS units in two configurations: one standard configuration without the Unique ID enabled and one configuration with the Unique ID enabled.*
2. *Tabulators with the Unique ID enabled will have 20% throughput as the total amount of ballots scanned each hour.*

SECTION V.14.1 ELECTRICAL HARDWARE TESTING

The Smartmatic VSR1 2.1 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:

- **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 contacts 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.

Note: The CCOS, the Central Count Component of the Smartmatic VSR1 2.1, will not be evaluated against the 2-hour battery backup requirement. The CCOS will be evaluated to verify it provides for a graceful shutdown to allow switching to an alternate power source.

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

  Requirement 2.7-I (Withstand conducted electrical disturbances)

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

  - Surges of 30% dip @10 ms;
  - Surges of 60% dip @100 ms & 1 sec;
  - Surges of >95% interrupt @ 5 sec;
  - Surges of ±15% line variations of nominal line voltage
  - Electric power increases of 7.5% and reductions of 12.5% of nominal specified power supply for a period of up to four hours at each power level

  The test for Electrical Power Disturbance shall be conducted in compliance with the test specified in IEC 61000-4-11 (2020).

- **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. Electrical fast transients of:

  - +2 kV and -2kV on External Power lines (both AC and DC)
  - +1 kV and -1 kV on Input/Output lines (signal, data, and control lines) longer than 3 meters
  - Repetition Rate for all transient pulses will be 100 kHz

  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, surges of:

  - ±2 kV AC line to line
  - ±2 kV AC line to earth
  - ±.5 kV DC line to line >10m
  - ±.5 kV DC line to earth >10m

- ±1 kV I/O signal/control >30m

The test for Lightning Surge shall be conducted in compliance with the test specified in IEC 61000-4-5 (2014).

- **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, ±15 kV air discharge and ±8 kV contact discharge. *Note: The equipment may reset or have momentary interruption so long as normal operation is resumed with 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).

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

  Requirement 2.7-J (Emissions from other connected equipment)

  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, an electromagnetic field of 10 V/m modulated by a 1 kHz 80% AM modulation over the frequency range of 80 MHz to 1000 MHz

  The test for Electromagnetic Susceptibility shall be conducted in compliance with the test specified in IEC 61000-4-3 (2020).

- **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, conducted RF Immunity of:

  - 10V rms over the frequency range 150 kHz to 80 MHz with an 80% amplitude modulation with a 1 kHz sine wave AC & DC power
  - 10V sig/control>3 m over the frequency range 150 kHz to 80 MHz with an 80% amplitude modulation with a 1 kHz sine wave

  The test for Conducted RF Immunity shall be conducted in compliance with the test specified in IEC 61000-4-6 (2013).

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, with the exception of Electrical Supply. Testing will be performed at the NTS Longmont facility located in Longmont, Colorado. All testing at the NTS 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 stresses faced during operation of voting machines, BMD's, and ballot counters. 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 is similar to the low and high temperature tests of MIL-STD-810H, Methods 502.7 and 501.7, with test conditions that correspond to the requirements of the performance standards. This procedure tests system operation under various environmental conditions for at least 104 hours. During 72 hours of the operating time, the equipment shall be in a test chamber under imposed test conditions for both temperature and humidity. For the remaining 32 hours, the equipment shall be operated at room temperature or ambient conditions. The system shall be powered for the entire period of this test; the power may be disconnected if necessary for removal of the system from the test chamber. 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, 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**

  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**

  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**

  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 degrees F. Relative humidity ranges of 25% to 55% shall be tested.

- **High Temperature Test**

  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 degrees F. Relative humidity ranges of 25% to 55% shall be tested.

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, Smartmatic 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 NTS Longmont facility located in Longmont, Colorado. Testing at the NTS Longmont facility will be witnessed on-site by Pro V&V personnel, with the exception of the Operational Environmental Test (Continuous Operation – Varied Environmental Conditions) in which Pro V&V qualified staff will execute all testing. All pre-test and post-test operational status checks shall be conducted by Pro V&V personnel.

SECTION V.15 PRODUCT SAFETY REVIEW

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

- **Principle 8, 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 defect that could make them unsatisfactory for their intended purpose; and
  2. Ensuring that components provided by external suppliers are free from damage or defect that could make them unsatisfactory or hazardous when used for their intended purpose.

  2.1.1-B – Durability estimation
  A manufacturer must submit a warranty model to the EAC, testing labs, and customers, 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 for data analysis. For source code and TDP reviews, results shall be compiled in reports and submitted to Smartmatic for resolution.

SECTION VI.2 TEST DATA CRITERIA

The Smartmatic VSR1 2.1 shall be evaluated against all applicable requirements contained in the VVSG 2.0. A *VVSG 2.0 Cross Reference Matrix* specific to the Smartmatic VSR1 2.1 will be utilized during the test campaign to ensure that all applicable VVSG 2.0 requirements are addressed. The matrix will contain the requirement number, title, and text for each VVSG 2.0 requirement, a listing of applicable system components, Artifact and Result Artifact IDs (Test Case IDs, Test Result IDs, Test Reports, etc.), and any applicable notes.

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

SECTION VI.3 TEST DATA REDUCTION

Test data shall be processed and recorded in the Engineering Notebook on the VSR1 2.1 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 Smartmatic Representative. Additionally, a comparison shall be made between the recorded serial numbers/part numbers and those listed on shipper's manifest and any discrepancies shall be reported to the Smartmatic 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

The Smartmatic VSR1 2.1 will be evaluated against all applicable requirements in the VVSG 2.0. There is no required sequence for test performance; however, there may be prerequisite tasks for some testing. If so, the predecessor task will be identified within the test case.

SECTION VIII: TEST OPERATIONS PROCEDURES

Pro V&V will identify PASS/FAIL criteria for each executed test case. The PASS/FAIL criteria will be based on the specific expected results of the system. In the case of an unexpected result that deviates from what is considered standard, normal, or expected, a root cause analysis will be performed. Pro V&V will evaluate every VVSG 2.0 requirement applicable to the Smartmatic VSR1 2.1 voting system. Any deficiencies noted will be reported to the EAC and the manufacturer. If it is determined that there is insufficient data to determine compliance, this test plan will be altered, and additional testing will be performed.

APPENDIX A: PROJECT SCHEDULE

Task #	Task Name	Start Date	End Date	Assigned To	Title	Predecessors
2	**EAC Application & TRR**	**02/06/23**	**03/31/23**			
3	Application Submitted to EAC	02/06/23	02/06/23	H. Medlock	Project Manager	
4	Pen Testing	02/21/23	03/16/23	H. Medlock	Project Manager	
5	TRR	02/21/23	03/16/23	H. Medlock	Project Manager	
6	Application Approval from EAC	03/17/23	03/31/23	H. Medlock	Project Manager	4
7	**TDP**	**04/03/23**	**02/27/25**			
8	Initial Review	04/03/23	04/14/23	S. Glover	QA Manager	5
9	Compliance Review	04/17/23	01/13/25	S. Glover	QA Manager	7
10	Final review	02/21/25	02/27/25	S. Glover	QA Manager	8
11	**Test Plan**	**04/03/23**	**10/30/23**			
12	Test Plan Creation	04/03/23	09/06/23	W. Owens	Program Director	5
13	Vendor Review & Comments	09/07/23	09/08/23	W. Owens	Program Director	11
14	EAC Submission and Review	09/11/23	10/06/23	W. Owens	Program Director	12
15	VSTL Comment Review & Update	10/09/23	10/12/23	W. Owens	Program Director	13
16	EAC Submission & Review of Revision	10/13/23	10/26/23	W. Owens	Program Director	14
17	EAC Approved Test Plan	10/27/23	10/30/23	W. Owens	Program Director	15
18	**Source Code**	**06/08/23**	**01/25/24**			
19	Automated Review	06/08/23	06/30/23	H. Medlock	Project Manager	
20	Source Code Review - Compliance Review 1	07/05/23	07/11/23	H. Medlock	Project Manager	18
21	Source Code Re-Review - Compliance Review 1	07/05/23	07/19/23	H. Medlock	Project Manager	18
22	Document Review	07/20/23	07/20/23	H. Medlock	Project Manager	20
23	Compliance Build 1	7/21/23	07/22/23	H. Medlock	Project Manager	
24	Automated Review – Code Drop 2	01/08/24	01/19/24	H. Medlock	Project Manager	
25	Document Review - Code Drop 2	01/22/24	01/22/24	H. Medlock	Project Manager	23
26	Compliance Build - Code Drop 2	01/23/24	01/25/24	H. Medlock	Project Manager	24
27	**System Delivery & Setup**	**02/21/23**	**09/11/23**			
28	PCA	02/21/23	02/22/23	H. Medlock	Project Manager	
29	System Setup	08/08/23	08/10/23	H. Medlock	Project Manager	
30	System Loads & Hardening	08/11/23	09/11/23	H. Medlock	Project Manager	25
31	**Hardware Testing**	**11/06/23**	**01/12/24**			
32	Electrical Testing	11/06/23	11/17/23	M. Walker	Program Manager	
33	Environmental Testing	11/06/23	11/10/23	M. Walker	Program Manager	
34	Continuous operation - varied enviro	12/04/23	12/08/23	M. Walker	Program Manager	

Task #	Task Name	Start Date	End Date	Assigned To	Title	Predecessors
35	Electrical Supply	12/11/23	12/12/23	H. Medlock	Project Manager	30
36	Maintainability	12/13/23	01/10/24	H. Medlock	Project Manager	31
37	Acoustic Testing	01/11/24	01/12/24	H. Medlock	Project Manager	32
38	**System Level Testing**	**09/12/23**	**01/09/25**			
39	FCA	09/12/23	07/11/24	H. Medlock	Project Manager	26
40	Security Testing – SCAP	07/12/24	07/25/24	H. Medlock	Project Manager	35
41	Security Testing – Physical Security	07/26/24	07/30/24	H. Medlock	Project Manager	36
42	Usability	07/31/24	08/05/24	H. Medlock	Project Manager	37
43	Accessibility	08/06/24	08/08/24	H. Medlock	Project Manager	38
44	Volume & Stress	08/09/24	09/05/24	H. Medlock	Project Manager	39
45	Accuracy	09/06/24	11/28/24	H. Medlock	Project Manager	40
46	Regression Testing	11/29/24	12/12/24	H. Medlock	Project Manager	41
47	Trusted Build	12/13/24	12/19/24	H. Medlock	Project Manager	42
48	System Loads & Hardening	12/20/24	12/26/24	H. Medlock	Project Manager	43
49	System Integration	12/27/24	01/09/25	H. Medlock	Project Manager	44
50	**Test Report**	**01/10/25**	**03/14/25**			
51	Test Report Creation	01/10/25	01/23/25	W. Owens	Program Director	45
52	Vendor Review & Comments	01/24/25	01/27/25	W. Owens	Program Director	47
53	EAC Submission & Review	01/28/25	02/24/25	W. Owens	Program Director	48
54	VSTL Comment Review & Update	02/25/25	02/27/25	W. Owens	Program Director	49
55	EAC Submission & Review of Revision	02/28/25	03/13/25	W. Owens	Program Director	50
56	EAC Approved Test Report	03/14/25	03/14/25	W. Owens	Program Director	51