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

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

Document Number: TR-01-01-SMT-2023-01

EAC Project Number: SMT-VSR1-21

Document Version: 06

Date: 09/04/2025

U.S. Election Assistance Commission
VSTL

EAC Lab Code 1501

NVLAP®

TESTING
NVLAP LAB CODE 200978-0

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) 1) all testing prescribed by the approved and published test plan or amended test plan was performed as identified or the divergence from the test plan was properly documented in this test report, 2) all identified voting system anomalies or failures were reported and resolved, and 3) this test report is accurate and complete. There are no opinions or interpretations included in this report, except as noted under Recommendations.

REVISIONS

Revision	Description	Date
00	Initial Release	07/25/2025
01	Updates per EAC comments	08/14/2025
02	Updates per EAC comments; Removed reference to hardware testing results as proprietary	08/21/2025
03	Update TDP document version	08/25/2025
04	Update TDP document versions	08/27/2025
05	Update TDP document version	08/28/2025
06	Update to reflect Test Plan changes	09/04/2025

TABLE OF CONTENTS

SECTION I: INTRODUCTION

The purpose of this Test Report is to document the procedures and test approach Pro V&V, Inc. followed 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 was performed to ensure the applicable requirements of VVSG 2.0 and the EAC Testing and Certification Program Manual, Version 3.0 were met. Additionally, all EAC Request for Interpretations (RFI) and Notices of Clarification (NOC) relevant to the system under test were 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.

The Smartmatic VSR1 2.1 EAC-approved test plan (TP-01-01-SMT-2023-01 Rev 02), as published on the EAC's website at www.eac.gov, was utilized as the guiding document during test performance. Since test plan approval, and as testing progressed, minor system modifications or revised system documentation were incorporated. This test report reflects all testing completed and details the final versions of all technical documentation and system components and supersedes the approved test plan.

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 is listed Table I-3 of this Test Report)*

SECTION I.2 TERMS AND ABBREVIATIONS

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

"ADA" – Americans with Disabilities Act 1990

"ATI" – Accessible-Tactile Interface

"BMD" – Ballot Marking Device

"CCOS" – Central Count Optical Scanner

"COTS" – Commercial Off-The-Shelf

"CVR" – Cast Vote Record

"EAC" – United States Election Assistance Commission

"FCA" – Functional Configuration Audit

"HAVA" – Help America Vote Act

"LAT" – Logic and Accuracy Test

"NIST" – National Institute of Standards and Technology

"NOC" – Notice of Clarification

"NVLAP" – National Voluntary Laboratory Accreditation Program

"PCA" – Physical Configuration Audit

"PCOS" – Precinct Count Optical Scanner

"QA" – Quality Assurance

"RFI" – Request for Interpretation

"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 SYSTEM IDENTIFICATION AND OVERVIEW

The hardware, software, and technical documentation of the Smartmatic Voting System VSR1 2.1 (Smartmatic VSR1 2.1) submitted for certification testing is listed in the relevant subsections below.

Tables I-1, I-2, and I-3 represent the final versions of the Smartmatic VSR1 2.1 System software/firmware, hardware, and technical data package considered for EAC accreditation.

SECTION I.3.1 SOFTWARE AND FIRMWARE

This subsection lists the Smartmatic VSR1 2.1 proprietary and COTS software provided by the manufacturer as part of the test campaign.

Smartmatic VSR1 2.1 is comprised of the proprietary and COTS software identified in Table I-1.

Table I-1 VSR1 2.1 Software

Configuration Item	Description	Source	COTS
EMP			
Application Version	8.9.51.4	Smartmatic	No
OS Version	Base OS: Ubuntu 20.04.6 LTS AMD64	Canonical	Yes
Platform	Linux	Linux	Yes
OS-level virtualization	Docker 27.5.1	Docker	Yes
Audit log data visualization tool	Auditd, Apparmor, rsyslog	Ubuntu	Yes
	Kibana/Elastic-Search	Elastic	Yes
Database	Oracle Database 18.4-xe	Oracle	Yes
CCOS			
Application Version	1.40.0	Smartmatic	No
OS version	7.3.0 en_US.UTF-8 (default language) Base OS: Ubuntu 24.04.2 LTS	Smartmatic	No
Platform	Linux	Linux	Yes
BMD			
Application Version	1.4.5	Smartmatic	No
OS Version	7.3.0 en_US.UTF-8 (default language) Base OS: Ubuntu 24.04.2 LTS	Smartmatic	No
Platform	Linux	Linux	Yes
PCOS			
Application Version	1.40.0	Smartmatic	No
OS version	7.3.0 en_US.UTF-8 (default language) Base OS: Ubuntu 24.04.2 LTS	Smartmatic	No
Platform	Linux	Linux	Yes

SECTION I.3.2 HARDWARE/EQUIPMENT

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

Smartmatic VSR1 2.1 is comprised of the proprietary and COTS hardware identified in Table I-1.

Table I-2 VSR1 2.1 Hardware/Equipment

Configuration Item	Description	Source	COTS
EMP			
EMP Server	PowerEdge T550 Parallax Security Bezel, Two Layer Door	Dell	Yes
EMP Election Official Laptop	Latitude 5520	Dell	Yes
Firewall Appliance	FortiGate 40F	Fortinet	Yes
Network switch	CBS350-8P-E-2G	Cisco	Yes
UPS	Smart-UPS (SMT1500C)	APC	Yes
External Hard Drive	2TB Extreme Portable SSD	SanDisk	Yes
Smartcard reader	ACR39U	ACS	Yes
Monitor	24 E2422H	Dell	Yes
Keyboard	Business Multimedia Keyboard - KB522	Dell	Yes
Mouse	Optical Mouse- MS116	Dell	Yes
Printer	LaserJet Pro 4001n	HP	Yes
VGA Cable	Generic VGA to VGA Cable 6 Feet	Dell	Yes
USB Locks with key	40452 Blue	Lindy	Yes
RJ45 Port blocker with key	40470	Lindy	Yes
CCOS			
Scanner	imageFORMULA DR-G2140 Imprinter Unit 3601C001	Canon	Yes
Device	OptiPlex 3000 micro	Dell	Yes
Display	M-Series 1502L 15-inch	Elo	Yes
Printer	Laser Jet Pro 4001n	HP	Yes
Smart card Reader	ACR39U	ACS	Yes
UPS	Smart-UPS (SMT1500C)	APC	Yes
USB hub	Hub	Anker	Yes
BMD			
BMD Main Unit	BMD-155 (RC5)	Smartmatic	No
Ballot Box	BBX-151	Smartmatic	No
Leg Stand	BLS-155	Smartmatic	No
Privacy Flap	BPF-155	Smartmatic	No
Power Adapter & Cable	24DC V @ 6.25 Amp	Smartmatic	No
UPS	APC UPS (BR1500MS2)	APC	Yes
Accessibility Devices	Sip-and-Puff AC-0304-V2	Origin instrument	Yes
Accessibility Devices	Buddy Buttons SWP1	Origin instrument	Yes

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

Configuration Item	Description	Source	COTS
Accessibility Devices	CD-46 Over-Ear Stereo Headphones	Yoga Electronics	Yes
Accessibility Devices	Stylus – B07WRQYQFF	Zerone	Yes
Accessibility Devices	Audio Tactile Interface (ATI) device KPB200	Smartmatic	No
PCOS			
PCOS	A4-800	Smartmatic	No
Ballot Box	BBX-800	Smartmatic	No
Power adapter and cable	100-240 V AC 50/60Hz	Smartmatic	No
Privacy flaps	PPF-800	Smartmatic	No
Accessibility Devices	Sip-and-Puff AC-0304-V2	Origin instrument	Yes
Accessibility Devices	Buddy Buttons SWP1	Origin instrument	Yes
Accessibility Devices	CD-46 Over-Ear Stereo Headphones	Yoga Electronics	Yes
Accessibility Devices	Stylus - B07WRQYQFF	Zerone	Yes
Accessibility Devices	Audio Tactile Interface (ATI) device KPB200	Smartmatic	No

SECTION I.3.3 TECHNICAL DATA PACKAGE (TDP) DOCUMENTS

This subsection lists the Smartmatic VSR1 2.1 end-user TDP documentation. For a complete listing of all TDP documents submitted to support this test campaign, please refer to the published test plan.

A listing of all documents contained in the Smartmatic VSR1 2.1 end-user TDP is provided in Table I-3.

Table I-3 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
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

Table I-3 VSR1 2.1 TDP Documents *(continued)*

Document ID	Description	Version
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
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

Table I-3 VSR1 2.1 TDP Documents *(continued)*

Document ID	Description	Version
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

SECTION I.3.4 TEST 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 I-4 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

Table I-4 VSR1 2.1 Materials/Consumables *(continued)*

Configuration Item	Description	Source
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
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		

Table I-4 VSR1 2.1 Materials/Consumables *(continued)*

Configuration Item	Description	Source
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 inches with 0.63" notched corner	Mitsubishi
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 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

Table I-4 VSR1 2.1 Materials/Consumables *(continued)*

Configuration Item	Description	Source
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
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 I.4 SYSTEM OVERVIEW

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 VSR1 2.1 comprises the following key 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 imageFORMULA DR-G2140

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 following sub-components that encompass task lists according to the voting stage: Election Configuration System (ECS) and Results Management System (RMS). The EMP is located at the election data center.

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.

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.

Central Count Optical Scanner (CCOS) - Scanner Model: Canon imageFORMULA 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.4.1 BLOCK DIAGRAMS

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 the hardware platforms and software components and a minimum data interchange as well as all network communications.

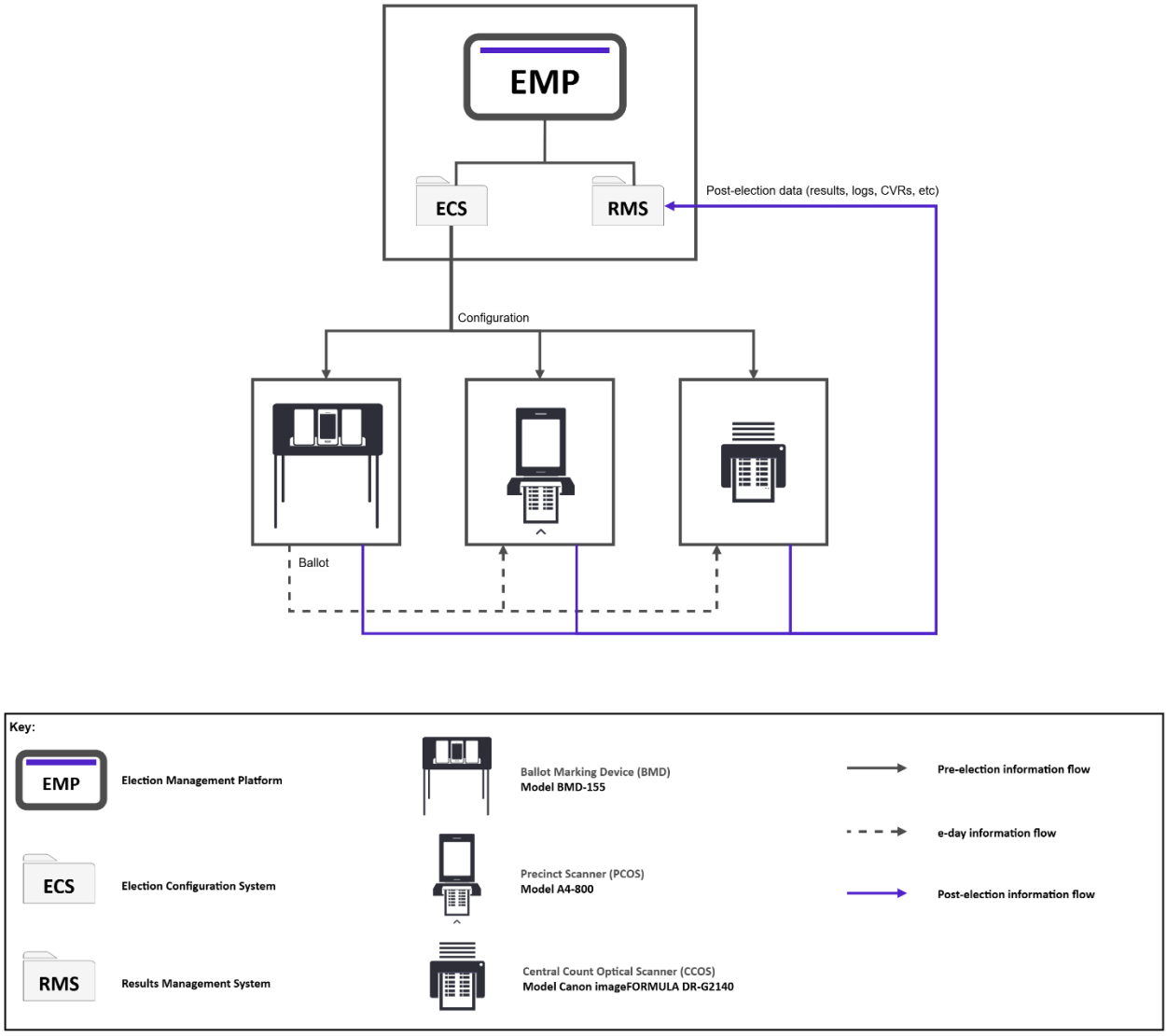

Figure I-1 Components of the Smartmatic VSR1 2.1

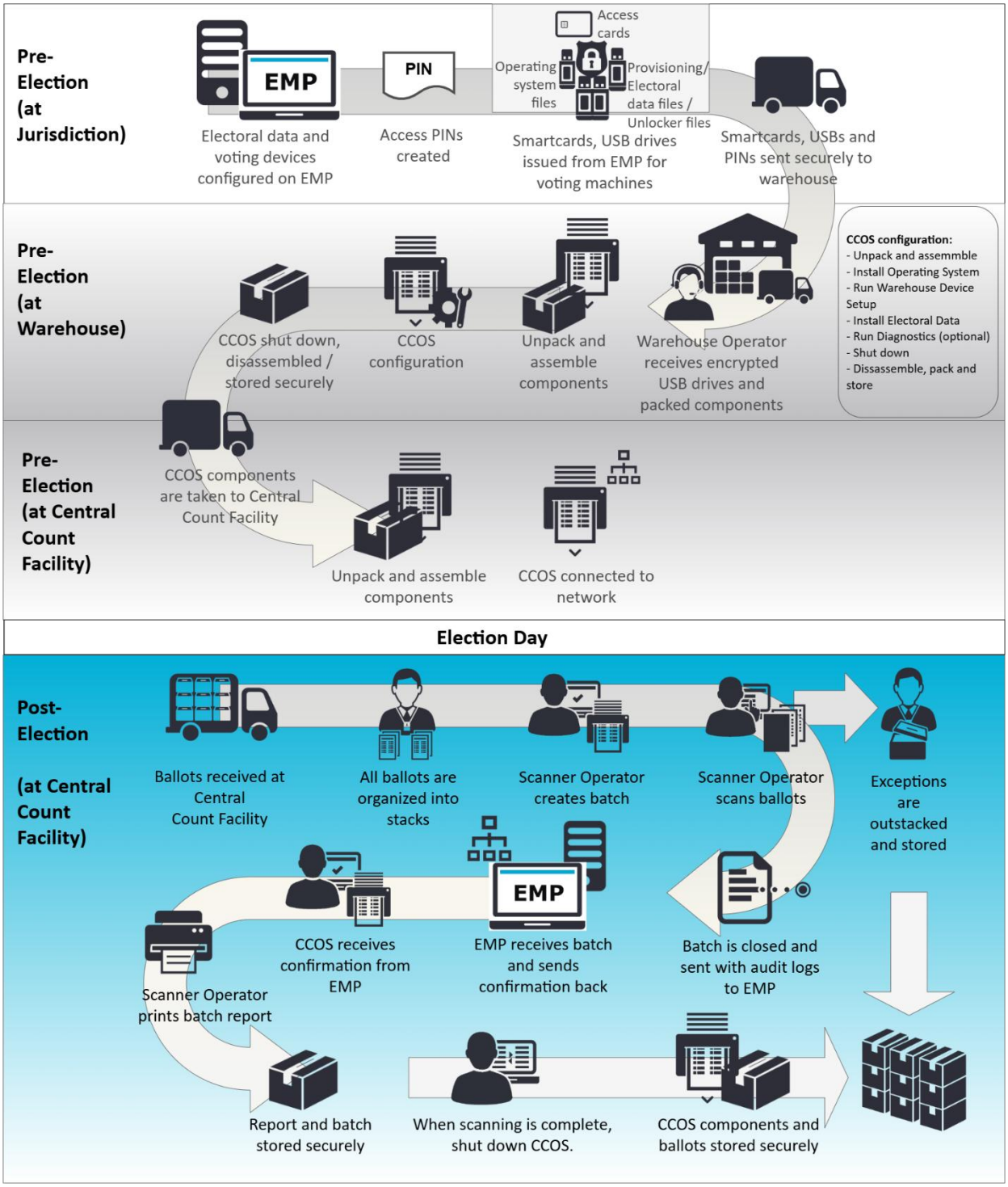

Figure I-2 Operational Process of the Smartmatic VSR1 2.1

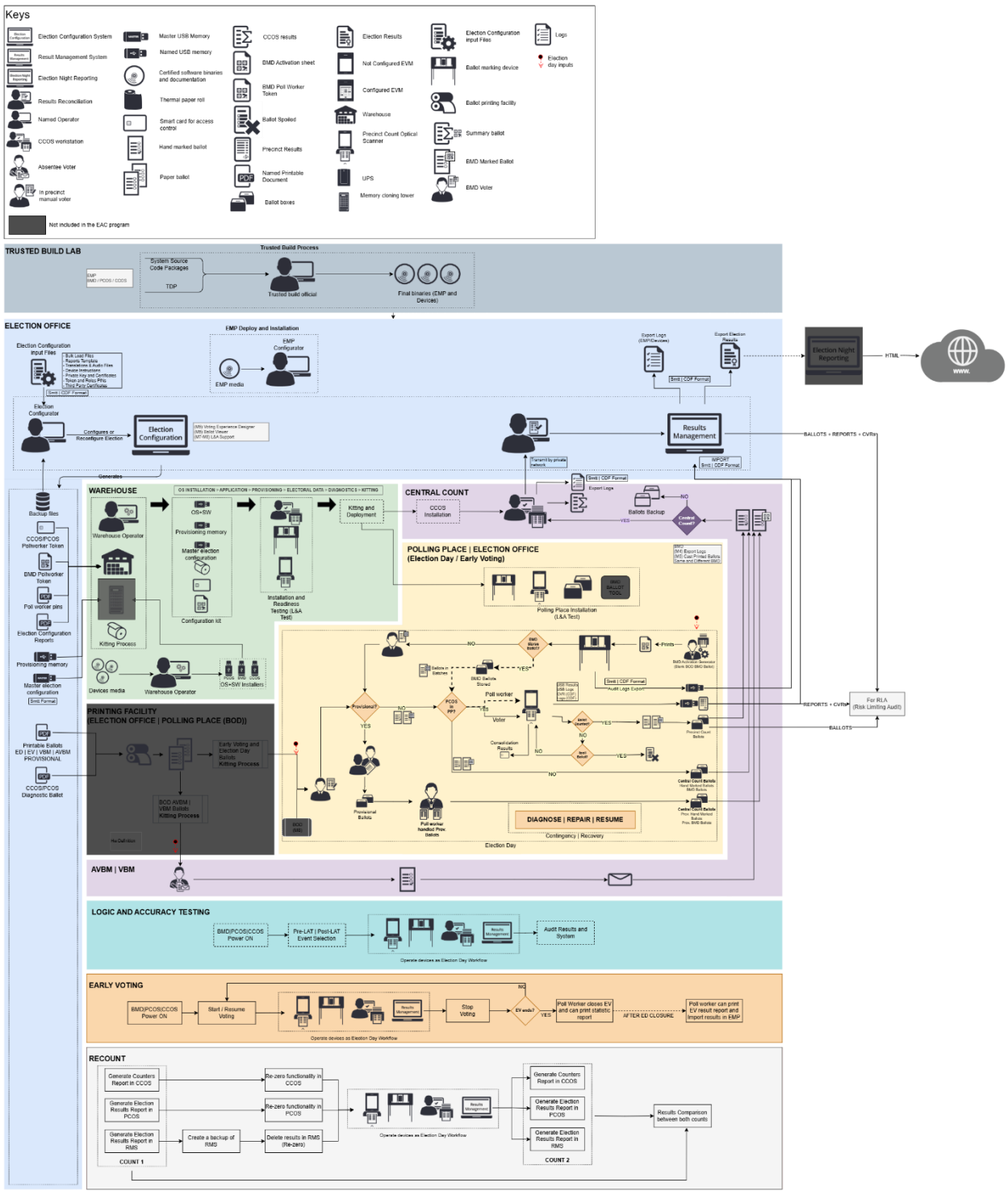

Figure I-3 Solution Deployment Diagram of the Smartmatic VSR1 2.1

SECTION I.4.2 SYSTEM LIMITS

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

Table I-5 System Limits

#	Parameter	Definition	Component Affected	System Limit
1	Max. Subdivisions levels	The subdivisions represent the jurisdiction configuration of the system as State, county, etc.	EMP	47
2	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
3	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
4	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
5	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
6	Max. Parties (General Election)	Number of parties defined for a General Election	Ballot size EMP Performance Reports Voting experience	20
7	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

Table I-5 System Limits *(continued)*

#	Parameter	Definition	Component Affected	System Limit
8	Max. Choices (candidates + yes/no) per contest	Number of candidates defined for a single contest	Ballot size EMP Performance Reports Voting experience	2140
9	Max Offices per election	A position established by law with certain associated rights and duties.	Ballot size EMP Performance Reports Voting experience	200
10	Max. Devices per election	Number of devices associated in a polling place	---	821
11	Max. Devices per election Election day	Number of devices associated in a polling place	---	PCOS: 400 BMD: 400
12	Max. Devices per election Early Voting/Voting Center	Number of devices associated in a polling place	---	PCOS: 8 BMD: 8
13	Max. Devices per election Absentee	Number of devices associated in a polling place	---	CCOS: 4
14	Max. Write-ins per contest	Number of write-ins options defined for a single contest	Ballot Reports	22 certified write-ins
15	Min. "Vote for" per contest	Definition of N - M values for a specific contest	Ballot	1
16	Max. "Vote for" per contest	Definition of N - M values for a specific contest	Ballot	22
17	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
18	Max. Events per election (Pre-LAT, Official)	Events supported in a specific election.	---	2
19	Central Count max cards per batch	Ballots scan per batch	---	1700 ballots
20	Ballot width	Ballot width that can be used in the election	---	8.5”

Table I-5 System Limits *(continued)*

#	Parameter	Definition	Component Affected	System Limit
21	Ballot lengths	Ballot lengths that can be used in the election.	-	PCOS and CCOS: • Minimum: 11” • Maximum: 21” BMD: • Minimum: 11” • Maximum: 13”
22	Scanner Document Feeder Maximum Capacity	Maximum number of ballots that should be stacked on the scanner document feeder	---	11" ballots: 200 ballots. 14" and 17" ballots: 120 ballots. 19" and 21" ballots: 100 ballots
23	Max choices per contest	Number of choices available per contest	Hand-marked ballots BMD reports Voter experience	208
24	Max contests in a ballot	Number of contests in a ballot	Ballots Reports	56
25	Max Ballot Styles supported by EMP	Ballot styles managed by the EMP	---	1000

Note: The EMP does not support the tilde character "~". The tilde "~" must be replaced with a dash "-".

SECTION I.4.3 SUPPORTED LANGUAGES

Smartmatic VSR1 2.1 supports the following languages:

- English
- Spanish
- Chinese
- Russian

The Smartmatic VSR1 2.1 can display and print 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 was verified; however, only English and Spanish language ballots were cast during the performance of functional testing. One character-based language (Chinese) was tested during System Integration Testing. Additionally, Pro V&V executed tests designed to verify Smartmatic VSR1 2.1:

- Can display and print 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.
- Can present 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 always identify or change language on the screen, 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.4.4 SUPPORTED FUNCTIONALITY

Smartmatic VSR1 2.1 supports 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 executed tests designed to verify 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 II: CERTIFICATION TEST BACKGROUND

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 was performed on the system and a complete TDP review was 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 this 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). 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".

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). The report was reviewed and approved by the EAC prior to VVSG 2.0 evaluation.

SECTION II.1 REVISION HISTORY

The table below details the version history of the Smartmatic VSR1 2.1 System:

Table II-1. Smartmatic VSR1 2.1 System Revision History

System Version	Certification Type	Baseline System	Certification Number
VSR1 2.1	New System	--- (Original System) ---	SMT-VSR1-21

*Upon grant of certification by the EAC

The Smartmatic VSR1 2.1 was 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 for subsequent systems submitted for evaluation at a later date.

SECTION II.2 IMPLEMENTATION STATEMENT

The Smartmatic VSR1 2.1 System Implementation Statement (SMT-2022-TDP-01) detailing the System's capabilities, features, and optional functions as well as any implemented extensions is provided as *Attachment A: Implementation Statement*.

SECTION II.3 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, were utilized when developing VSTL Test Cases during the test campaign.

As a new system, the Smartmatic VSR1 2.1 was evaluated against all applicable requirements contained in the principles and guidelines. To accomplish this, Pro V&V defined multiple test areas relevant to each Principle. Tests were executed within each test area to evaluate the applicable Requirements. Additionally, a VVSG 2.0 Matrix specific to the Smartmatic VSR1 2.1 was utilized during the test campaign to ensure that all applicable VVSG 2.0 requirements were addressed. Table II-2 details the VVSG 2.0 Principles, Guidelines, and associated test areas.

Table II-2 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 Review
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. 2.6 - The voting system handles errors robustly and gracefully recovers from failure. 2.7 - The voting system performs reliably in anticipated physical environments.	Source Code Review, TDP Review, FCA, Security Review, Electrical Hardware Testing, Operational Environmental Hardware Testing, Non-Operational Environmental Hardware Testing, Vulnerability Testing

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

VVSG 2.0 Guideline	VSTL Test Areas
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
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. *(continued)*	Usability, Accessibility, FCA, TDP Review

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

VVSG 2.0 Guideline	VSTL Test Areas
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.	*(continued)*
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 Review, 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. 10.2 - The voting system does not contain nor produce records, notifications, information about the voter, or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.	FCA, Usability, Accessibility, TDP Review, Security Tests, Cryptographic Testing
Principle 11: Access Control *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. *(continued)*	Security Review, Vulnerability Testing, FCA

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

VVSG 2.0 Guideline	VSTL Test Areas
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	*(continued)*
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 Review, Vulnerability Testing, FCA, TDP Review
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. 13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.	Security Review, FCA, TDP Review, Cryptographic Testing
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. *(continued)*	Security Review, Penetration Testing, TDP Review, Source Code Review, Vulnerability Testing, Cryptographic Testing, FCA

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

VVSG 2.0 Guideline	VSTL Test Areas
14.4 - Voting system software updates are authorized by an administrator prior to installation.	*(continued)*
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 Review, FCA, Vulnerability Testing, TDP Review

SECTION II.3.1 NOT APPLICABLE REQUIREMENTS

Pro V&V determined the Requirements listed below are not applicable to the Smartmatic VSR1 2.1 System. *Requirements notated with an asterisk (*) have been added since the approval of the published test plan.*

1.1.4- F – Partisan open primary ballot*

1.1.4-K – Straight-party voting, Casting*

1.1.4-L – Cumulative voting contest. Casting*

1.1.4-M – Ranked choice voting contest, Casting

1.1.4-N – Party preference contest*

1.1.4-O – Top-2 primary contest (blanket primary contest)*

1.1.4-P – Presidential delegate contest, Casting*

1.1.4-Q – Proportional voting contest (equal-and-even cumulative voting contest), Casting*

1.1.4-R – Group voting contest, Casting*

1.1.4-S – Top-2 IRV contest (supplementary or contingent vote contest)*

1.1.8-B.2 – Tabulation of an open primary ballot*

1.1.8-B.3 – Open primary ballot with party preference contest*

1.1.8-E – Straight-party voting, Tabulation*

1.1.8-F – Cross-party endorsement with straight-party voting*

1.1.8-I – Cumulative voting contest, Tabulation*

1.1.8-J, 1.1.8-J.1, 1.1.8-J.2 – Ranked choice voting contest, Tabulation

1.1.8-K – Group voting contest, Tabulation*

1.1.8-L – Presidential delegate contest, Tabulation*

1.1.8-N – Proportional voting contest (equal-and-even cumulative voting contest), Tabulation*

1.1.9-I – Ranked choice voting, report results

2.1-B – COTS language extensions are acceptable*

7.2-F, 7.2-F.1, 7.2-F.2 – Voter Speech*

8.1-D – Secondary ID and biometrics*

8.1-G – Telephone style handset*

9.1.6 – Cryptographic E2E verifiable

9.1.6-A– Verified cryptographic protocol

9.1.6-B – Independent evaluation of E2E cryptographic protocol implementation

9.1.6-C, 9.1.6-C.1, 9.1.6-C.2 – Cryptographic ballot selection verification by voter

9.1.6-D – Methods for cryptographic ballot selection verification

9.1.6-E, 9.1.6-E.1, 9.1.6-E.2, 9.1.6-E.3, 9.1.6-E.4, 9.1.6-E.5 – Ballot receipt

9.1.6-F – Disputes involving ballot receipts

9.1.6-G, 9.1.6-G.1, 9.1.6-G.2 – Evidence export

9.1.6-H– Mandatory ballot availability

9.1.6-I, 9.1.6-I.1, 9.1.6-I.2 – Verification of encoded vote documentation

9.1.6-J, 9.1.6-J.1, 9.1.6-J.1.a, 9.1.6-J.1.b, 9.1.6-J.2 – Verifier reference implementation

9.1.6-K – Privacy preserving, universally verifiable ballot tabulation

10.2.1-B – Indirect voter associations*

10.2.1-C – Use of indirect voter associations*

10.2.1-D – Isolated storage location*

10.2.1-E – Removal of indirect voter associations*

10.2.1-F – Confidentiality for ballots with indirect voter associations*

10.2.4-A – Voting information in receipts*

12.1-F – Secure locking systems*

13.3-B – E2E cryptographic voting protocols*

SECTION II.4 TESTING RESPONSIBILITIES

Pro V&V conducted all core voting system tests (as defined by NIST handbook 150-22) on the Smartmatic VSR1 2.1 System. Testing was performed by personnel verified by Pro V&V to be qualified to perform the test.

SECTION II.5 THIRD PARTY TESTS

Pro V&V utilized third-party test facilities for performance of the electrical and environmental tests (non-core hardware testing). These tests were performed at the Element Materials Technology Denver-Longmont facility located in Longmont, Colorado. All testing was witnessed on-site by Pro V&V personnel, except for the Operational Environmental Hardware Testing (Continuous Operation – Varied Environmental Conditions) in which Pro V&V-qualified staff executed all testing.

SECTION III: TEST PROCESS AND SUMMARY FINDINGS

Smartmatic VSR1 2.1 was evaluated against all applicable requirements contained in the principles and guidelines. The results contained within this test report represent a summary of the outcomes of the testing activities; detailed information regarding test methods can be found in the corresponding approved test plan. The VVSG 2.0 Compliance Results Matrix associated with this test campaign (*Attachment H: VVSG 2.0 Compliance Results Matrix - PROPRIETARY*) maps the requirements to the executed test cases. This matrix is designated as proprietary and is not approved for publication; however, it was submitted to the EAC for review purposes. All additional findings, noted discrepancies, or deficiencies (if applicable) are detailed in *Attachment E: Additional Findings - PROPRIETARY*.

For each test area, Pro V&V utilized proprietary baseline test cases augmented with specially designed test cases tailored to the specific design of the Smartmatic VSR1 2.1. Test cases provided 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. Pro V&V mapped test cases to each applicable VVSG 2.0 requirement. Due to their proprietary nature, the test cases utilized during this campaign are not published within this test report; however, they were submitted to the EAC for review purposes (*Reference Attachment F: Test Cases*).

Descriptions of the test areas defined in Table II-2, including a listing of the VVSG 2.0 requirements encompassed within each test area and the associated Summary Findings, are detailed in the sections that follow. *Note: Some requirements are covered within multiple test areas; however, they may only be listed in the primary test area under which they were evaluated.*

SECTION III.1 SUMMARY FINDINGS

Summary findings include the number of test cases executed during evaluation of each test area, the VVSG 2.0 requirements being evaluated, and a summary of the results obtained. As of the date of this test report, test assertions have been developed for a select subset of VVSG 2.0 requirements. These test

assertions were utilized when developing VSTL Test Cases during the test campaign to determine conformance to specific requirements. These test assertions are not included in the VVSG 2.0 requirements listings.

SECTION III.1.1 PHYSICAL CONFIGURATION AUDIT (PCA)

The Physical Configuration Audit (PCA) compares the voting system components submitted for testing 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 was conducted in two phases: Initial (to baseline the system prior to test commencement) and Final (to verify final software and hardware configurations).

This test area encompasses the following VVSG 2.0 requirements:

4.3-A, 4.4, 4.4-A

Summary Findings

During execution of the PCA, the components of the Smartmatic VSR1 2.1 system were documented by component name, model, serial number, major component, and any other relevant information needed to identify the component. For COTS equipment, every effort was made to verify that the COTS equipment had not been modified for use. Additionally, each technical document submitted in the TDP was recorded by document name, description, document number, revision number, and date of release. At the conclusion of the test campaign, test personnel verified that any changes made to the software, hardware, or documentation during the test process were fully and properly documented.

SECTION III.1.2 TECHNICAL DATA PACKAGE (TDP) REVIEW

To determine full compliance with the VVSG 2.0, three phases of TDP review were conducted. As part of the review process, Pro V&V utilized a TDP Review Checklist that contains TDP requirements specified in the VVSG 2.0. Results of the review of each document were entered on the TDP Review Checklist

and reported to the manufacturer for disposition of any discrepancies or noted deficiencies. This process was ongoing until all issues were resolved. The three phases are described below:

- Initial TDP Review

  The first review was performed to determine whether the TDP submitted was complete enough to perform TDP review. This was an abbreviated review. Each document was reviewed to determine the sufficiency of the provided description of the submitted voting system components and if the document generically addressed VVSG requirements. The results of the review were used in determining contractual requirements for the test campaign.

- Compliance Review

  This review was conducted to determine if each Federal, State, or manufacturer-stated requirement had been met based on the context of each requirement. This review did not address consistency or completeness of documents. The review is more complex than the initial TDP review. Results of the review of each document were entered on the TDP Review Checklist and reported to the manufacturer for disposition of any discrepancies. This process was ongoing until all noted issues were resolved.

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

- Consistency/Completeness Review

  The third TDP review was completed after the review for compliance had been performed. This review was to ensure the information included in the TDP documents was 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. As with the other TDP reviews, the TDP Review Checklist was utilized to report any discrepancies to the manufacturer for resolution, if required. The TDP review continued until all noted issues were satisfactorily resolved.

This test area encompasses the following VVSG 2.0 requirements:

1.3, 1.3-A, 1.3-A.1, 1.3-A.2, 1.3-A.3, 1.3-A.4, 1.3-A.5, 1.3-A.6, 1.3-A.7, 1.3-A.8, 1.3-A.9, 1.3-B, 2.1-D, 2.1.1, 2.1.1-A, 2.1.1-A.1, 2.1.1-A.2, 2.1.1-B, 2.1.1-B.1, 2.1.1-B.2, 2.1.1-B.3, 2.1.1-B.4, 2.1.1-B.5, 2.1.1-C, 2.1.1-D, 2.1.2-A, 2.1.2-A.1, 2.1.2-A.2, 2.1.2-A.3, 2.1.2-B, 2.1.2-B.1,2.1.2-B.2, 2.1.2-B.3, 2.1.2-B.4, 2.1.2-B.5, 2.2, 2.2-A, 2.2-A.1, 2.2-A.2, 2.2-A.3, 2.2-A.4, 2.5-B, 3, 3.1, 3.1.1, 3.1.1-A, 3.1.1-B, 3.1.1-C, 3.1.1-C.1, 3.1.1-C.2, 3.1.1-C.3, 3.1.1-C.4, 3.1.1-C.5, 3.1.1-C.6, 3.1.1-C.7, 3.1.1-C.8, 3.1.1-C.9, 3.1.1-D, 3.1.1-D.1, 3.1.1-D.2, 3.1.1-D.3, 3.1.1-E, 3.1.2-A, 3.1.2-A.1, 3.1.2-A.2, 3.1.2-A.3, 3.1.2-A.4, 3.1.2-A.5, 3.1.2-B, 3.1.2-C, 3.1.2-C.1, 3.1.2-C.2, 3.1.2-C.3, 3.1.2-D, 3.1.2-D.1, 3.1.2-D.2, 3.1.2-D.3, 3.1.2-D.4, 3.1.2-D.5, 3.1.3, 3.1.3-A, 3.1.3-B, 3.1.3-B.1, 3.1.3-B.2, 3.1.3-B.3, 3.1.3-B.4, 3.1.3-C, 3.1.3-D, 3.1.4, 3.1.4-A, 3.1.4-B, 3.1.4-B.1, 3.1.4-B.2, 3.1.4-B.3, 3.1.4-B.4, 3.1.4-B.5, 3.1.4-B.6, 3.1.4-B.7, 3.1.4-B.8, 3.1.4-C, 3.1.4-D, 3.1.4-E, 3.1.4-F, 3.1.4-G, 3.1.4-H, 3.1.4-I, 3.1.4-I.1, 3.1.4-I.2, 3.1.4-I.3, 3.1.4-I.4, 3.1.4-I.5, 3.1.4-I.6, 3.1.4-I.7, 3.1.4-I.8, 3.1.4-J, 3.1.4-K, 3.1.4-L, 3.1.4-M, 3.1.5, 3.1.5-A, 3.1.5-A.1, 3.1.5-A.2, 3.1.5-A.3, 3.1.5-A.4, 3.1.5-A.5, 3.1.5-A.6, 3.1.5-A.7, 3.1.5-A.8, 3.1.5-A.9, 3.1.5-B, 3.1.5-C, 3.1.5-D, 3.1.5-E, 3.1.5-F, 3.1.5-G, 3.1.5-G.1, 3.1.5-G.2, 3.1.5-G.3, 3.1.5-G.4, 3.1.5-G.5, 3.1.5-H, 3.1.5-I, 3.1.5-I.1, 3.1.5-I.2, 3.1.5-I.3, 3.1.5-I.4, 3.1.5-J, 3.1.5-J.1, 3.1.5-J.2, 3.1.5-K, 3.1.5-K.1, 3.1.5-K.2, 3.1.5-K.3, 3.1.6,

3.1.6-A, 3.1.6-B, 3.1.6-C, 3.1.6-D, 3.1.6-D.1, 3.1.6-D.2, 3.1.6-D.3, 3.1.6-D.4, 3.1.6-D.5, 3.1.6-D.6, 3.1.6-D.7, 3.1.6-D.8, 3.1.6-E, 3.1.6-F, 3.1.6-F.1, 3.1.6-F.2, 3.1.6-F.3, 3.1.6-F.4, 3.1.6-G, 3.1.6-G.1, 3.1.6-G.2, 3.1.6-G.3, 3.1.6-G.4, 3.1.6-G.5, 3.1.6-G.6, 3.1.6-H, 3.1.6-I, 3.1.6-J, 3.1.6-J.1, 3.1.6-J.2, 3.1.6-J.3, 3.1.6-J.4, 3.1.6-J.5, 3.1.6-J.6, 3.1.6-K, 3.1.6-L, 3.1.6-M, 3.1.6-M.1, 3.1.6-M.2, 3.1.6-N, 3.1.6-O, 3.1.6-P, 3.1.6-Q, 3.1.6-Q.1, 3.1.6-Q.2, 3.1.6-Q.3, 3.1.7, 3.1.7-A, 3.1.7-B, 3.1.7-B.1, 3.1.7-B.2, 3.1.7-B.3, 3.1.7-B.4, 3.1.7-B.5, 3.1.7-B.6, 3.1.7-B.7, 3.1.7-C, 3.1.7-D, 3.2, 3.2-A, 3.2-B, 3.2-B.1, 3.2-B.2, 3.2-B.3, 3.2-B.4, 3.2-C, 3.2-D, 3.2-E, 3.2-F, 3.2-G, 3.2-H, 3.2-I, 3.2-J, 3.2-K, 3.2-L, 3.2-M, 3.2-N, 3.2-O, 3.2-P, 3.2-P.1, 3.2-P.2, 3.2-P.3, 3.2-P.4, 3.2-Q, 3.2-Q.1, 3.2-Q.2, 3.2-Q.3, 3.2-Q.4, 3.2-Q.5, 3.2-Q.6, 3.2-Q.7, 3.2-Q.8, 3.3, 3.3-A, 3.3-A.1, 3.3-A.2, 3.3-B, 3.3-B.1, 3.3-B.2, 3.3-B.3, 3.3-C, 3.3-D, 4.1-E, 4.1-F, 5.1-F, 5.1-F.1, 5.1-F.2, 7.3-O, 7.3-P, 9.1.1-A.2, 9.1.3-C, 9.1.4-B, 9.2-A, 9.4-B, 11.4-B, 12.1-A, 13.3-E, 14.1-A, 14.1-B, 14.1-C, 14.1-C.1, 14.1-C.2, 14.1-C.3, 14.1-C.4, 14.1-D, 14.2-F, 14.2-J, 14.2-J.1, 14.2-J.2, 14.2-J.3, 14.2-J.4, 14.3-A, 14.3-A.1, 14.3-A.2, 14.3-A.3, 14.3-A.4, 14.3-A.5, 14.3-B, 14.3-C, 14.3-C.1, 14.3-C.2, 14.3-C.3, 14.3-C.4, 15.2-B, 15.3-C, 15.4-A, 15.4-B, 15.4-C

Summary Findings

All noted issues were successfully resolved by the conclusion of the test campaign. Pro V&V concluded the documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood. Additionally, Pro V&V concluded that the documentation was sufficient for end-users to understand and verify the operations of the voting system throughout the entirety of the election.

SECTION III.1.3 SOURCE CODE REVIEW

Pro V&V performed a compliance inspection of the submitted source code of the Smartmatic VSR1 2.1 software of the EMP, CCOS, PCOS and BMD. Pro V&V reviewed the submitted source code to VVSG 2.0 and the manufacturer-submitted coding standards. Prior to initiating the software review, Pro V&V verified the submitted documentation was 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 were met.

The submitted source code was subjected to a compliance review to ensure the submitted source code was stable enough to proceed with testing. The source code and all additional packages were then compiled into a Compliance Build. Following successful completion of the FCA, a Trusted Build was performed. The trusted build consisted 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 included the build documentation review.

A combination of automated source code review and manual source code review methods were used to review the submitted source code. The complete source code was reviewed utilizing the automated source code tools described in the Smartmatic TDP document *SMT-2022-TDP-10 Software Design and Specification*. These tools included 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 allowed 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 were manually reviewed to ensure that all source code was VVSG 2.0 compliant.

The manual source code review consisted 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.

Any additional code drops submitted by Smartmatic, were examined using ExamDiffPro, version 15.0, to do a manual comparison review against the previously submitted code. Any findings that were discovered were sent to Smartmatic for resolution. All issues were successfully resolved before the Trusted Build was completed.

This test area encompasses the following VVSG 2.0 requirements:

2.1, 2.1-A, 2.1-A.1, 2.1-A.2, 2.1-A.3, 2.1-A.4, 2.1-A.5, 2.1-B, 2.1-C, 2.3, 2.3-A, 2.3-B, 2.3-C, 2.3-D, 2.3-D.1, 2.3-D.2, 2.3.1, 2.3.1-A, 2.3.1-B, 2.3.1-C, 2.3.1-D, 2.4, 2.4-A, 2.4-A.1, 2.4-A.2, 2.4-A.3, 2.4-A.3.a, 2.4-A.3.b, 2.4-A.4, 2.4-A.5, 2.4-A.6, 2.4-B, 2.4-C, 2.4-C.1, 2.4-C.2, 2.4-C.3, 2.4-D, 2.5, 2.5-A, 2.5-B, 2.5.1, 2.5.1-A, 2.5.1-B, 2.5.1-C, 2.5.1-D, 2.5.2, 2.2.5-A, 2.5.2-A.1, 2.5.2-A.2, 2.5.2-A.3, 2.5.2-A.4, 2.5.3, 2.5.3-A, 2.5.3-B, 2.5.3-C, 2.5.4, 2.5.4-A, 2.5.4-A.1, 2.5.4-A.2, 2.5.4-A.3, 2.5.4-A.4, 2.5.4-A.5, 2.5.4-A.6, 2.5.4-A.7, 2.5.4-B, 2.5.4-C, 2.5.4-D, 2.5.4-E, 2.5.4-F, 2.5.4-G, 2.5.4-H, 2.5.4-H.1, 2.5.4-H.2, 2.5.4-I, 2.5.4-J, 2.5.4-K, 2.5.4-L, 2.5.4-L.1, 2.5.4-L.2, 2.5.4-M, 2.5.4-N, 2.5.4-O, 9.1.1, 9.1.1-A, 9.1.1-A.1, 14.2-G, 14.2-H, 14.2-I, 14.2-K

Summary Findings

All issues discovered were identified to Smartmatic for resolution. All issues were successfully resolved by the conclusion of the test campaign. Pro V&V concluded that the source code for each application in the Smartmatic VRS1 2.1 System complies with VVSG 2.0 and the Smartmatic-submitted coding standards. Pro V&V determined the voting system, and its software, were implemented using trustworthy materials and best practices in software development that support system processes and data with integrity. The voting system logic was determined to be clear and well-structured. The voting system structure was found to be modular, scalable, and robust. Additionally, based on system design capabilities and functionality supported, Pro V&V determined Requirement 2.1-B is not applicable to the Smartmatic VSR1 2.1 System.

The source code review report is included as *Attachment G: Source Code Review Report – PROPRIETARY.* Records related to the generation of the Trusted Build are included in *Attachment C: Trusted Build*.

SECTION III.1.4 FUNCTIONAL CONFIGURATION AUDIT (FCA)

The Functional Configuration Audit (FCA) encompassed an examination of manufacturer tests, and the conduct of additional tests, to verify that the system hardware and software performed 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 included a test of system operations in the sequence in which they would normally be performed. These system operations and functional capabilities were 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 included an assessment of the submitted system capabilities and inputs of both normal and abnormal data during test performance. This evaluation utilized baseline test cases as well as specifically designed test cases and included predefined election definitions for the input data. As part of the FCA, primary and general elections were executed to verify successful system operation. During the performance of the FCA, qualified personnel:

- Reviewed the manufacturer's test procedures and test results to determine if the manufacturer's specified functional requirements have been adequately tested. This examination included an assessment of the adequacy of the manufacturer's test cases and input data to exercise all system functions, and to detect program logic and data processing errors, if such are present.
- Performed or supervised the performance of additional tests to verify nominal system performance in all operating modes and verified on a sampling basis the manufacturer's data reports. If manufacturer developmental test data was incomplete, qualified personnel designed and conducted all appropriate module and integrated functional tests.

This test area encompasses the following VVSG 2.0 requirements:

1, 1.1, 1.1.1, 1.1.1-A, 1.1.1-A.1, 1.1.1-A.2, 1.1.1-A.3, 1.1.1-A.4, 1.1.1-B, 1.1.1-B.1, 1.1.1-B.2, 1.1.1-C, 1.1.1-C.1, 1.1.1-C.2, 1.1.1-C.3, 1.1.1-D, 1.1.1-D.1, 1.1.1-D.2, 1.1.1-D.3, 1.1.1-E, 1.1.1-F, 1.1.1-G, 1.1.1-H, 1.1.1-I, 1.1.1-J, 1.1.1-K, 1.1.1-L, 1.1.1-M, 1.1.1-N, 1.1.2-A, 1.1.2-B, 1.1.2-C, 1.1.2-D, 1.1.2-E, 1.1.2-F, 1.1.2-G, 1.1.2-H, 1.1.2-H.1, 1.1.2-H.2, 1.1.2-H.3, 1.1.2-H.4, 1.1.2-H.5, 1.1.2-I, 1.1.2-I.1, 1.1.2-I.2,

1.1.2-I.3, 1.1.2-I.4, 1.1.2-J, 1.1.2-J.1, 1.1.2-J.2, 1.1.2-J.3, 1.1.2-J.4, 1.1.2-K, 1.1.2-K.1, 1.1.2-K.2, 1.1.2-K.3, 1.1.2-L, 1.1.2-L.1, 1.1.2-L.2, 1.1.2-L.3, 1.1.2-L.4, 1.1.2-L.5, 1.1.2-L.6, 1.1.2-L.7, 1.1.3, 1.1.3-A, 1.1.3-B, 1.1.3-B.1, 1.1.3-B.2, 1.1.5, 1.1.5-A, 1.1.5-B, 1.1.5-B.1, 1.1.5-B.2, 1.1.5-C, 1.1.5-C.1, 1.1.5-C.2, 1.1.5-D, 1.1.5-D.1, 1.1.5-D.2, 1.1.5-D.3, 1.1.5-D.4, 1.1.5-E, 1.1.5-E.1, 1.1.5-E.2, 1.1.5-E.3, 1.1.5-E.4, 1.1.5-F, 1.1.5-F.1, 1.1.5-F.2, 1.1.5-F.3, 1.1.5-G, 1.1.5-G.1, 1.1.5-G.2, 1.1.5-G.3, 1.1.5-G.4, 1.1.5-G.5, 1.1.5-G.6, 1.1.5-G.7, 1.1.5-H, 1.1.6, 1.1.6-A, 1.1.6-B, 1.1.6-B.1, 1.1.6-B.2, 1.1.6-C, 1.1.6-C.1, 1.1.6-C.2, 1.1.6-C.3, 1.1.6-C.4, 1.1.6-D, 1.1.6-D.1, 1.1.6-D.2, 1.1.6-D.3, 1.1.6-D.4, 1.1.6-E, 1.1.6-E.1, 1.1.6-E.2, 1.1.6-F, 1.1.6-F.1, 1.1.6-F.2, 1.1.6-G, 1.1.6-H, 1.1.6-H.1, 1.1.6-H.2, 1.1.6-H.3, 1.1.6-I, 1.1.6-J, 1.1.6-K, 1.1.7, 1.1.7-A, 1.1.7-B, 1.1.7-C, 1.1.7-D, 1.1.7-E, 1.1.8, 1.1.8-A, 1.1.8-A.1, 1.1.8-A.2, 1.1.8-A.3, 1.1.8-B, 1.1.8-B.1, 1.1.8-B.2, 1.1.8-B.3, 1.1.8-C, 1.1.8.C.1, 1.1.8.C.2, 1.1.8-D, 1.1.8-E, 1.1.8-F, 1.1.8-G, 1.1.8-H, 1.1.8-I, 1.1.8-J, 1.1.8-J.1, 1.1.8-J.2, 1.1.8-J.3, 1.1.8-K, 1.1.8-L, 1.1.8-M, 1.1.8-N, 1.1.9, 1.1.9-A, 1.1.9-B, 1.1.9-B.1, 1.1.9-B.2, 1.1.9-B.3, 1.1.9-B.4, 1.1.9-B.5, 1.1.9-C, 1.1.9-C.1, 1.1.9-C.2, 1.1.9-C.3, 1.1.9-C.4, 1.1.9-C.5, 1.1.9-D, 1.1.9-E, 1.1.9-F, 1.1.9-G, 1.1.9-H, 1.1.9-I, 1.1.9-J, 1.1.9-K, 1.1.9-L, 1.1.9-M, 2.1.2-C.1, 2.1.2-C.2, 2.1.2-C.3, 2.6, 2.6-A, 2.6-A.1, 2.6-A.2, 2.6-A.3, 2.6-B, 2.6-C, 9.1.2-B, 9.1.3-A, 9.1.4-A, 9.1.3-B, 9.1.5-A, 9.1.5-B, 9.1.5-C, 9.1.5-D, 9.1.5-F, 9.1.5-G, 9.4-C, 9.4-D, 10.1, 15.1-D.1, 15.1-D.1.a, 15.1-D.1.b, 15.1-D.1.c, 15.1-D.1.d, 15.1-D.1.e, 15.1-D.1.f, 15.1-D.1.g, 15.1-D.1.h, 15.1-D.1.i, 15.1-D.1.j, 15.1-D.1.k, 15.1-D.2, 15.1-D.2.a, 15.1-D.2.b, 15.1-D.2.c, 15.1-D.3, 15.1-D.3.a, 15.1-D.4, 15.1-D.4.a, 15.1-D.4.b, 15.1-D.4.c, 15.1-D.4.d, 15.1-D.4.e, 15.1-D.5, 15.1-D.5.a, 15.1-D.5.b, 15.2-C, 15.2-D

Summary Findings

All functional tests were successfully executed. Regression testing was performed as needed to verify all noted deficiencies were successfully addressed.

Based on system design capabilities and functionality supported, Pro V&V determined the following requirements in this test area were not applicable to the Smartmatic VSR1 2.1 System: 1.1.8-B.2, 1.1.8-B.3, 1.1.8-E, 1.1.8-F, 1.1.8-I, 1.1.8-J.1, 1.1.8-J.2, 1.1.8-J.3, 1.1.8-K, 1.1.8-L, 1.1.8-N, and 1.1.9-I.

SECTION III.1.5 SECURITY REVIEW

The purpose of the Security Review was 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.

The test methods for performing the Security Testing were execution and review. Prior to performance of Security testing, the examiner verified that security hardening scripts had been properly applied to system components per the system documentation. The examiner reviewed the submitted TDP to verify that documented access and physical controls were in place. Following the documented procedures, the system was configured for use and functionality to verify that the documented controls were in place and adequate and met the stated requirements. The Security Review consisted of an Administrative Review, Technical Review, and Physical Review, described as follows:

Administrative Evaluation

The Administrative Security Evaluation began with reviewing the TDP package for assessor orientation to the system while evaluating the breadth and depth of security topics covered. The documentation was assessed for coverage, clarity, correctness, consistency, and effectiveness of the documented security controls. The assessment evaluated the security controls' effectiveness in protecting confidentiality, integrity, availability, and accountability within the system. The evaluation also assessed that ample and appropriate controls were implemented within the system to provide adequate protection to the system. This evaluation spanned security defenses and phases mentioned above. The assessment extended beyond the TDP Review to evaluate the compliance in fulfilling the requirements outlined in the VVSG and/or related requirements. The assessment included a review of the vendor's submitted threat matrix (*VSR1 Security Dashboard*) provided in the TDP to evaluate security controls for effectiveness in protecting against threats.

During the Administrative Security Evaluation specific experiential tests were derived from the controls specified in the documentation. These tests were executed during the technical / logical evaluation phases through hands-on applied assessment. Tasks performed on each component during the Administrative Security Evaluation included, but were 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 consisted 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 included an assessment of preventative and detective controls against physical breach to a component. Physical Security Evaluation tasks included, but were not limited to, altering the physical components to allow for unauthorized access to the system, and real word threat actor scenarios. For each component possible tasks included:

- 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:

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

Detection & Prevention - While attempting to gain physical access to the system, Pro V&V monitored time lapsed and if the attempt was noticeable.

Technical/Logical Evaluation

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

To perform the Security Review, qualified test personnel developed and executed specifically designed test cases aimed at defeating the access controls and security measures documented in the system TDP. The test cases were developed utilizing the requirements found in Principles 11-15 to verify that each identified security feature and procedure met requirements and functions as expected and documented. Qualified personnel also performed 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 was accomplished by utilizing a combination of functional testing and source code review. All findings were reported to the EAC and Smartmatic.

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

- 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:

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 - Attempt to manipulate the system to perform actions that they system was not intended to do

Additionally, network analysis tools were 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 was utilized across all devices.

This test area encompasses the following VVSG 2.0 requirements:

9.1.2-A, 9.1.2-A.1, 9.1.2-A.2, 9.3, 9.3-A, 9.4-A, 10.1-A, 10.2, 10.2.1, 10.2.1-A, 10.2.1-B, 10.2.1-C, 10.2.1-D, 10.2.1-E, 10.2.1-F, 10.2.2, 10.2.2-A, 10.2.2-B, 10.2.2-C, 10.2.2-D, 10.2.2-D.1, 10.2.2-D.2,

10.2.2-E, 10.2.3, 10.2.3-A, 10.2.3-B, 10.2.4-A, 10.2.4-B, 12.1-E, 12.1-F, 12.1-G, 12.1-G.1, 12.1-G.2, 12.1-G.3, 12.2, 12.2-A, 12.2-B, 12.2-C, 12.2-D, 12.2-E, 13.1, 13.1.1, 13.1.1-A, 13.1.1-B, 13.1.1-C, 13.1.2, 13.1.2-A, 13.2, 13.2-A, 13.2-B, 13.2-B.1, 13.2-B.2, 13.2-B.3, 13.2-B.4, 14.2-A, 14.2-B, 14.2-C, 14.2-D, 14.2-E, 14.2-E.1, 14.2-E.2, 14.3.1-B, 14.3.1-C, 14.3.2-A, 14.3.2-C, 14.3.2-D, 14.4, 14.4-A, 14.4-B, 14.4-C, 15.1, 15.1-A, 15.1-B, 15.1-C, 15.1-C.1, 15.1-C.2, 15.1-D, 15.1-D.1, 15.1-D.1.a, 15.1-D.1.b, 15.1-D.1.c, 15.1-D.1.d, 15.1-D.1.e, 15.1-D.1.f, 15.1-D.1.g, 15.1-D.1.h, 15.1-D.1.i, 15.1-D.1.j, 15.1-D.1.k, 15.1-D.2, 15.1-D.2.a, 15.1-D.2.b, 15.1-D.2.c, 15.1-D.3, 15.1-D.3.a, 15.1-D.4, 15.1-D.4.a, 15.1-D.4.b, 15.1-D.4.c, 15.1-D.4.d, 15.1-D.4.e, 15.1-D.5, 15.1-D.5.a, 15.1-D.5.b, 15.1-E, 15.2-A, 15.2-C, 15.2-D, 15.3-A, 15.3-B, 15.4-D

Summary Findings

Pro V&V successfully completed the Security Review of the Smartmatic VRS1 2.1 System. Any issues discovered during testing were promptly reported to Smartmatic for resolution, and all were successfully resolved by the end of the test campaign. Pro V&V concluded that each application within the Smartmatic VRS1 2.1 System complied with applicable VVSG 2.0 requirements. Furthermore, Pro V&V determined that the voting system and its security policies adhere to security best practices in software development.

Based on system design capabilities and functionality supported, Pro V&V determined Requirements 10.2.1-B, 10.2.1-C, 10.2.1-D, 10.2.1-E, 10.2.1-F, 10.2.4-A, and 12.1F in the list above were not applicable to the Smartmatic VSR1 2.1 System.

SECTION III.1.6 VULNERABILITY TESTING

System vulnerability was assessed during performance of the Security Review. 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 evaluated the system by executing test cases developed to specific requirements focused on high quality best practices implementation and system integrity.

This test area encompasses the following VVSG 2.0 requirements:

2.5.4-B, 2.5.4-N, 10.2.4-C, 11.1, 11.1-A.1, 11.1-A.2, 11.1-A.3, 11.1-B, 11.1-C, 11.1-C.1, 11.1-C.2, 11.1-C.3, 11.1-D, 11.2, 11.2.1, 11.2.1-A, 11.2.1-B, 11.2.1-C, 11.2.1-C.1, 11.2.1-C.2, 11.2.1-C.3, 11.2.1-C.4, 11.2.1-D, 11.2.1-E, 11.2.1-F, 11.2.2, 11.2.2-A, 11.2.2-B, 11.2.2-B.1, 11.2.2-B.2, 11.2.2-B.3, 11.2.2-C, 11.2.2-C.1, 11.2.2-C.1.a, 11.2.2-C.1.b, 11.2.2-C.1.c, 11.2.2-C.2, 11.2.2-C.2.a, 11.2.2-C.2.b, 11.2.2-C.2.c, 11.2.2-C.3, 11.2.2-C.3.a, 11.2.2-C.3.b, 11.2.2-C.3.c, 11.2.2-D, 11.3, 11.3.1, 11.3.1-A, 11.3.1-B, 11.3.1-B.1, 11.3.1-B.2, 11.3.1-B.3, 11.3.1-B.4, 11.3.1-B.5, 11.3.1-B.6, 11.3.1-C, 11.3.2, 11.3.2-A, 11.3.2-B, 11.3.2-C, 11.3.2-D, 11.3.2-E, 11.4-A, 11.5, 11.5-A, 11.5-A.1, 11.5-A.2, 11.5-B, 11.5-C, 11.5-D, 12.1-A, 12.1-B, 12.1-C, 12.1-D, 15.3-D, 15.3-E, 15.3-F, 15.3-G

Summary Findings

Vulnerability testing was successfully completed. During the testing, qualified personnel performed administrative, physical, and technical/logical reviews on the Smartmatic VSR1 2.1 system. During the evaluation, the EMP server was connected directly to the Fortigate 40F firewall. The Fortigate 40F Firewall was connected to the Cisco CBS350-8P-E-2G network switch. Connected to the network switch

were the EMP Workstation, CCOS Workstation and an HP LaserJet Printer. Automated Vulnerability scans were taken of all networked machines to expose any vulnerabilities or unauthorized open network ports. Any vulnerabilities discovered were scrutinized utilizing security techniques to assess the severity. Any noted discrepancies were successfully resolved by the conclusion of the test campaign.

SECTION III.1.7 CRYPTOGRAPHIC TESTING

Cryptographic testing was performed to assess the Smartmatic VSR1 2.1 System to the requirements for cryptographic algorithms contained in VVSG 2.0. To assess conformance to these requirements, qualified personnel evaluated the system by executing test cases developed to specific requirements focused on verifying that all cryptographic algorithms are public, well-vetted, and standardized.

This test area encompasses the following VVSG 2.0 requirements:

9.1.6, 9.1.6-A, 9.1.6-B, 9.1.6-C, 9.1.6-C.1, 9.1.6-C.2, 9.1.6-D.1, 9.1.6-D.2, 9.1.6-E, 9.1.6-E.1, 9.1.6-E.2, 9.1.6-E.3, 9.1.6-E.4, 9.1.6-E.5, 9.1.6-F, 9.1.6-G, 9.1.6-G.1, 9.1.6-G.2, 9.1.6-H, 9.1.6-I, 9.1.6-I.1, 9.1.6-I.2, 9.1.6-J, 9.1.6-J.1, 9.1.6-J.1.a, 9.1.6-J.1.b, 9.1.6-J.2, 9.1.6-K, 10.2.2-E, 10.2.4-A, 13.3-A, 13.3-A.1, 13.3-A.2, 13.3-B, 13.3-C, 13.3-D, 13.3-E, 13.4, 13.4-A, 13.4-A.1, 13.4-A.2, 13.4-A.3, 14.3.1-A, 14.3.2-B

Summary Findings

Cryptographic testing was successfully completed. Any noted discrepancies were successfully resolved by the conclusion of the test campaign. Based on system design capabilities and functionality supported, Pro V&V determined Requirements associated with E2E Verifiable Voting Systems (Requirements 9.1.6 through 9.1.6-K and Requirement 13.3-B in the list above) were not applicable to the Smartmatic VSR1 2.1 System.

SECTION III.1.8 USABILITY REVIEW

A Usability Review was 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 consisted of tasks that address voter confidentiality (privacy and independence), integrity (accuracy), and availability (usability).

This test area encompasses the following VVSG 2.0 requirements:

1.1.6-B.1, 1.1.6-B-2, 6, 6.1, 6.1-A, 6.1-B, 6.1-C, 6.1-D, 6.2, 6.2-A, 6.2-A.1, 7.1-B, 7.1-C, 7.1-C.1, 7.1-C.2, 7.1-D, 7.1-D.1, 7.1-D.2, 7.1-D.2.a, 7.1-D.2-b, 7.1-D.2-c, 7.1-D.3, 7.1-E, 7.1-E.1, 7.1-E.2, 7.1-E.3, 7.1-F, 7.1-G, 7.1-G.1, 7.1-G.2, 7.1-G.2.a, 7.1-G.2.b, 7.1-G.2.c, 7.1-G.2.d, 7.1-H, 7.1-H.1, 7.1-H.2, 7.1-I, 7.1-J, 7.1-K, 7.1-K.1, 7.1-K.2, 7.1-K.3, 7.1-K.4, 7.1-K.5, 7.1-K.6, 7.1-K.7, 7.1-L, 7.2-B, 7.2-C, 7.2-C.1-3, 7.2-C.4, 7.2-C.5, 7.2-D, 7.2-D.1.a, 7.2-D.1.b, 7.2-D.1, 7.2-D.2, 7.2-D.2.a, 7.2-D.2.b, 7.2-D.2.c, 7.2-D.3, 7.2-D.3.a, 7.2-D.3.b, 7.2-D.3.c, 7.2-D.3.d, 7.2-D.3.e, 7.2-E, 7.2-E.1, 7.2-E.2, 7.2-E.3, 7.2-E.4, 7.2-E.5,

7.2-E.6, 7.2-H, 7.2-I, 7.2-I.1, 7.2-I.2, 7.2-I.3, 7.2-J, 7.2-K, 7.2-L, 7.2-M, 7.2-N, 7.2-N.1.a, 7.2-N.1.b, 7.2-N.1, 7.2-N.2, 7.2-N.3, 7.2-O, 7.2-O.1, 7.2-O.2, 7.2-O.3, 7.2-O.4, 7.2-R.1, 7.3, 7.3-A, 7.3-B, 7.3-B.1, 7.3-B.2, 7.3-C, 7.3-C, 7.3-C.1, 7.3-C.2, 7.3-C.3, 7.3-C.4, 7.3-C.5, 7.3-C.6, 7.3-D, 7.3-E, 7.3-F, 7.3-F.1, 7.3-F.2, 7.3-F.3, 7.3-G, 7.3-G.1.a, 7.3-G.1.b, 7.3-G.1.c, 7.3-G.2, 7.3-G.3, 7.3-G.2, 7.3-G.3, 7.3-H. 7.3-H.1, 7.3-H.2, 7.3-I, 7.3-I.1, 7.3-I.2, 7.3-J.1, 7.3-J.2, 7.3-K, 7.3-K.1, 7.3-K.1.a, 7.3-K.1.b, 7.3-K.1.c, 7.3-K.2, 7.3-K.2.a, 7.3-K.2.b, 7.3-L, 7.3-M, 7.3-M.1, 7.3-M.2, 7.3-N, 7.3-N.1, 7.3-N.2, 7.3-N.3, 7.3-O.1, 7.3-O.1.a, 7.3-O.1.b, 7.3-O.2, 7.3-O.2.a, 7.3-O.2.b, 7.3-O.2.c, 8.1, 8.1-A, 8.1-A.1.a, 8.1-A.1.b, 8.1-A.1, 8.1-A.2, 8.1-A.3, 8.1-A.2.a, 8.1-A.2.b, 8.1-A.3.a, 8.1-A.3.b, 8.1-B, 8.1-D, 8.1-J, 8.1-J.1, 8.1-J.2, 8.3, 8.3-A, 8.3-A.1.a, 8.3-A.1.b, 8.3-A.1.c, 8.3-A.1.d, 8.3-A.1, 8.3-A.2, 8.4, 8.4-A, 8.4-A.1.a, 8.4-A.1.b, 8.4-A.1.c, 8.4-A.1.d, 8.4-A.1.e, 8.4-A.1.f, 8.4-A.1.g, 8.4-A.1, 8.4-A.2, 8.4-A.3

Summary Findings

Pro V&V reviewed the following Smartmatic-submitted usability test reports detailing successful usability testing of the Smartmatic VSR1 2.1 system:

- *Smartmatic Voting System Usability Test Report, Election Worker Test Report: Smartmatic Voting System, Perkins Access, Perkins School for the Blind, dated March 16, 2023*
- *Smartmatic Voting System Usability Test Report, Usability Test Report: Smartmatic Voting System, Perkins Access, Perkins School for the Blind, dated March 16, 2023*

The Usability review was successfully completed. Any noted discrepancies were successfully resolved by the conclusion of the test campaign. Based on system design capabilities and functionality supported, Pro V&V determined Requirement 8.1-D is not applicable to the Smartmatic VSR1 2.1 System.

SECTION III.1.9 ACCESSIBILITY REVIEW

An Accessibility Review was performed to 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. 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).

This test area encompasses the following VVSG 2.0 requirements:

5, 5.1, 5.1-A, 5.1-B, 5.1-C, 5.1-D, 5.1-E, 5.1-F, 5.1-F.1, 5.1-F.2, 5.2, 5.2-A, 5.2-B , 5.2-C, 5.2-D, 5.2-E, 5.2-E.1, 5.2-E.2, 5.2-F, 7.1-A, 7.1-M, 7.1-M.1, 7.1-M.2, 7.1-M.3, 7.1-N, 7.1-N.1, 7.1-N.2, 7.1-N.3, 7.1-O, 7.1-P, 7.2-A, 7.2-A.1, 7.2-A.2, 7.2-A.3, 7.2-A.4, 7.2-A.5, 7.2-F, 7.2-F.1, 7.2-F.2, 7.2-G, 7.2-G.1, 7.2-G.2, 7.2-G.3, 7.2-G.4, 7.2-P, 7.2-P.1, 7.2-P.2, 7.2-Q, 7.2-R.2, 8.1-C, 8.1-E, 8.1-F, 8.1-G, 8.1-H, 8.1-I, 8.1-I.1, 8.1-I.2, 8.1-I.3, 8.2, 8.2-A

Summary Findings

The Accessibility review was successfully completed. Any noted discrepancies were successfully resolved by the conclusion of the test campaign. Based on system design capabilities and functionality

supported, Pro V&V determined Requirements 7.2-F, 7.2-F.1, 7.2-F.2, and 8.1-G are not applicable to the Smartmatic VSR1 2.1 System.

SECTION III.1.10 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, was determined through functional tests integrating the voting system software with the remainder of the system. During system testing, the system was configured exactly as it would for normal field use per the procedures detailed in the Smartmatic VSR1 2.1 technical documentation. This included 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 two Primary Elections were exercised on the voting system, as described below. Each election is designed to test different voting variations. The descriptions included in this section are high level descriptions designed to provide an overview. The specific information will be included in the election definitions, which will be designed to accommodate system functionality, limitations, or specific functionality being tested.

Three general elections with the following breakdowns:

- General Election GEN-01: A General Election held in four precincts, one of which is a split precinct. This election contains nineteen contests compiled into four ballot styles. Five of the contests are in all four ballot styles. The other fourteen contests are split between at least two of the precincts with a maximum of four different contests spread across the four precincts.
- General Election GEN-02: A basic election held in three precincts. This election contains fifteen contests compiled into three ballot styles. Ten of the contests are in all three ballot styles with the other five split across the 3 precincts. This election also includes ballot rotation, if supported by the system under test.
- General Election GEN-03: A General Election held in two precincts. This election contains eight contests compiled into two ballot styles. Four of the contests are in both ballot styles. The other four contests are split between the two precincts. This election is designed to functionally test the handling of multiple ballot styles, support for at least three languages including a character-based language, support for common voting variations, and audio support for at least three languages and an ADA binary input device.

Two primary elections with the following breakdowns:

- Primary Election PRIM-01: This election is designed to functionally test a Closed Primary Election with multiple ballots and support for common voting variations. This election contains thirty-one contests and six parties compiled into eighteen ballot styles, each ballot containing six contests.
- Primary Election PRIM-03: A Closed Primary Election held in two precincts. This election contains ten contests and is compiled into two ballot styles. Two of the contests are in both ballot

styles. The other eight contests are split between the two parties' ballots. This election is designed to functionally test the handling of multiple ballot styles, support for at least three languages including a character-based language, support for common voting variations, and audio support for at least three languages and an ADA binary input device.

This test area encompasses the following VVSG 2.0 requirements:

1.1.1, 1.1.1-A, 1.1.1-A.1, 1.1.1-A.2, 1.1.1-A.3, 1.1.1-A.4, 1.1.1-B, 1.1.1-B.1, 1.1.1-B.2, 1.1.1-C, 1.1.1-C.1, 1.1.1-C.2, 1.1.1-C.3, 1.1.1-D, 1.1.1-D.1, 1.1.1-D.2, 1.1.1-D.3, 1.1.1-E, 1.1.1-F, 1.1.1-G, 1.1.1-H, 1.1.1-I, 1.1.1-J, 1.1.1-K, 1.1.1-L, 1.1.1-M, 1.1.1-N, 1.1.2-A, 1.1.2-B, 1.1.2-C, 1.1.2-H, 1.1.2-H.1, 1.1.2-H.2, 1.1.2-H.3, 1.1.2-H.4, 1.1.2-H.5, 1.1.2-J, 1.1.2-J.1, 1.1.2-J.2, 1.1.2-J.3, 1.1.2-J.4, 1.1.2-K, 1.1.2-K.1, 1.1.2-K.2, 1.1.2-K.3, 1.1.2-L, 1.1.2-L.1, 1.1.2-L.2, 1.1.2-L.3, 1.1.2-L.4, 1.1.2-L.5, 1.1.2-L.6, 1.1.2-L.7, 1.1.3, 1.1.3-A, 1.1.3-B, 1.1.3-B.1, 1.1.3-B.2, 1.1.4, 1.1.4-A, 1.1.4-B, 1.1.4-B.1, 1.1.4-B.2, 1.1.4-B.3, 1.1.4-C,1.1.4-D, 1.1.4-E, 1.1.4-F, 1.1.4-G, 1.1.4-G.1, 1.1.4-G.2, 1.1.4-H, 1.1.4-I, 1.1.4-J, 1.1.4-K, 1.1.4-L, 1.1.4-M, 1.1.4-N, 1.1.4-O, 1.1.4-P, 1.1.4-Q, 1.1.4-R, 1.1.4-S, 1.1.5, 1.1.5-A, 1.1.5-B, 1.1.5-B.1, 1.1.5-B.2, 1.1.5-C, 1.1.5-C.1, 1.1.5-C.2, 1.1.5-D, 1.1.5-D.1, 1.1.5-D.2, 1.1.5-D.3, 1.1.5-D.4, 1.1.5-E, 1.1.5-E.1, 1.1.5-E.2, 1.1.5-E.3, 1.1.5-E.4, 1.1.5-F, 1.1.5-F.1, 1.1.5-F.2, 1.1.5-F.3, 1.1.5-G, 1.1.5-G.1, 1.1.5-G.2, 1.1.5-G.3, 1.1.5-G.4, 1.1.5-G.5, 1.1.5-G.6, 1.1.5-G.7, 1.1.5-H, 1.1.6, 1.1.6-A, 1.1.6-B, 1.1.6-B.1, 1.1.6-B.2, 1.1.6-C, 1.1.6-C.1, 1.1.6-C.2, 1.1.6-C.3, 1.1.6-C.4, 1.1.6-D, 1.1.6-D.1, 1.1.6-D.2, 1.1.6-D.3, 1.1.6-D.4, 1.1.6-E, 1.1.6-E.1, 1.1.6-E.2, 1.1.6-F, 1.1.6-F.1, 1.1.6-F.2, 1.1.6-G, 1.1.6-H, 1.1.6-H.1, 1.1.6-H.2, 1.1.6-H.3, 1.1.6-I, 1.1.6-J, 1.1.6-K, 1.1.7, 1.1.7-A, 1.1.7-B, 1.1.7-C, 1.1.7-D, 1.1.7-E, 1.1.8, 1.1.8-A, 1.1.8-A.1, 1.1.8-A.2, 1.1.8-A.3, 1.1.8-B, 1.1.8-B.1, 1.1.8-B.2, 1.1.8-B.3, 1.1.8-C, 1.1.8.C.1, 1.1.8.C.2, 1.1.8-D, 1.1.8-E, 1.1.8-F, 1.1.8-G, 1.1.8-H, 1.1.8-I, 1.1.8-J, 1.1.8-J.1, 1.1.8-J.2, 1.1.8-J.3, 1.1.8-K, 1.1.8-L, 1.1.8-M, 1.1.8-N, 1.1.9, 1.1.9-A, 1.1.9-B, 1.1.9-B.1, 1.1.9-B.2, 1.1.9-B.3, 1.1.9-B.4, 1.1.9-B.5, 1.1.9-C, 1.1.9-C.1, 1.1.9-C.2, 1.1.9-C.3, 1.1.9-C.4, 1.1.9-C.5, 1.1.9-D, 1.1.9-E, 1.1.9-F, 1.1.9-G, 1.1.9-H, 1.1.9-I, 1.1.9-J, 1.1.9-K, 1.1.9-L, 1.1.9-M

Summary Findings

System Integration testing was successfully completed with all actual results obtained during test execution matching the expected results. Any noted discrepancies were successfully resolved by the conclusion of the test campaign.

Based on system design capabilities and functionality supported, Pro V&V determined the following requirements in this test area were not applicable to the Smartmatic VSR1 2.1 System: 1.1.4-F, 1.1.4-K, 1.1.4-L, 1.1.4-M, 1.1.4-N, 1.1.4-O, 1.1.4-P, 1.1.4-Q, 1.1.4-R, 1.1.4-S, 1.1.8-B.2, 1.1.8-B.3, 1.1.8-E, 1.1.8-F, 1.1.8-I, 1.1.8-J.1, 1.1.8-J.2, 1.1.8-J.3, 1.1.8-K, 1.1.8-L, 1.1.8-N, and 1.1.9-I.

SECTION III.1.11ACCURACY TEST

Accuracy testing was 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 voting system must function correctly under real-world operating conditions that address the need to satisfy integrity constraints for accuracy, achieving the required end-to-end accuracy benchmark, and the system's ability to reliably detect marks on the ballot.

This test area encompasses the following VVSG 2.0 requirements:

1.2-A, 1.2-A.1, 1.2-A.2, 1.2-A.3, 1.2-B, 1.2-C, 1.2-G, 3.1.6-K

Summary Findings

Accuracy testing was successfully completed with all actual results obtained during test execution matching the expected results. During testing, Pro V&V verified a minimum of 10,000,000 ballot positions could be read by the voting system and tabulated accurately. Any noted discrepancies were successfully resolved by the conclusion of the test campaign.

SECTION III.1.12 VOLUME & STRESS TEST

The Volume & Stress test investigated the system's response to conditions that tend to overload the system's capacity to process, store, and report data. The test parameters focused 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 was utilized to ensure the system could achieve the manufacturer's TDP claims of what the system can support. Testing was performed by exercising multiple election definitions developed specifically to test the volume and stress conditions of the system being tested.

This test area encompasses the following VVSG 2.0 requirements:

1.2-D, 1.2-E, 1.2-G

Summary Findings

Testing was successfully completed with all actual results obtained during test execution matching the expected results. During testing, Pro V&V verified voting system misfeed rate did not exceed the misfeed rate benchmark of Requirement 1.2-G. Any noted discrepancies were successfully resolved by the conclusion of the test campaign.

SECTION III.1.13 INTEROPERABILITY

Interoperability is defined by VVSG 2.0 as the extent to which systems from different manufacturers and devices with different system configurations can communicate with each other. Interoperability testing was performed to ensure the voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals. Conformance and interoperability testing of common data format import and export implementations was the focus of the review.

This test area encompasses the following VVSG 2.0 requirements:

1.1.2-E, 3.3-A.1, 3.3-A.2, 3.3-B.1, 3.3-B.2, 3.3-B.3, 3.3-C, 3.3-D, 4.1, 4.1-A, 4.1-A.1, 4.1-A.2, 4.1-B, 4.1-C, 4.1-D, 4.1-E, 4.1-F, 4.2, 4.2-A, 4.2-B, 4.3, 4.3-A, 4.4, 4.4-A, 9.1.5-E

Summary Findings

Testing was successfully completed with all actual results obtained during test execution matching the expected results. Any noted discrepancies were successfully resolved by the conclusion of the test campaign.

SECTION III.1.14 HARDWARE TESTING

Hardware Testing consisted of electrical hardware testing, a continuous operational environmental test, and various non-operational environmental tests. Hardware testing was performed on the equipment listed in Table I-2 of this report. All non-COTS hardware listed were tested to the full suite of electrical and environmental test requirements contained within the VVSG 2.0. Equipment that was deemed COTS was exempt from the environmental non-operational testing. Equipment that was deemed COTS was utilized during electrical testing for the PCOS and BMD as necessary to ensure proper functionality of the system under test during exposure. The COTS and non-COTS equipment was utilized during the 104-hour Continuous Operation – varied environmental conditions test. During the 104-hour Continuous Operation – varied environmental conditions Smartmatic, with Pro V&V oversight, performed maintenance on the CCOS as prescribed within the TDP. No unscheduled maintenance was required during hardware testing

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 was 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 had 20% throughput as the total amount of ballots scanned each hour.*

Electrical Supply (Battery Backup) testing was performed at the Pro V&V facility located in Huntsville, AL. All other listed hardware tests were performed at the Element Materials Technology Denver-Longmont facility located in Longmont, Colorado. All testing at the Element Materials Technology facility was witnessed on-site by Pro V&V personnel, except for the Operational Environmental Test (Continuous Operation – Varied Environmental Conditions) in which Pro V&V qualified staff conducted all operational testing. All pre-test and post-test operational status checks were conducted by Pro V&V personnel.

SECTION III.1.14.1 ELECTRICAL HARDWARE TESTING

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.

This test area encompasses the following VVSG 2.0 requirements:

1.2-I, 1.2-I.1, 1.2-I.2, 1.2-K, 1.2-L, 2.1.2-A, 2.1.2-B, 2.7-A, 2.7-A.3, 2.7-F, 2.7-G, 2.7-H, 2.7-I, 2.7-J, 2.7-K, 8.1-J.1, 8.1-J.2

Summary Findings

Testing was successfully completed with all actual results obtained during test execution matching the expected results. Any noted discrepancies were successfully resolved by the conclusion of the test campaign. The associated test parameters are described in the approved test plan for this test campaign. The Element Materials Technology test reports detailing the test methods and results of this testing are presented in *Attachments D.2, D.3, D.5, D.6, D.8, and D.9* contained in *"Attachment D: Hardware Test Results"*.

SECTION III.1.14.2 OPERATIONAL HARDWARE TESTING

Operational Hardware Testing consists of a Continuous Operation Test intended to simulate stresses faced during operation of voting machines, BMDs, and ballot counters. The test consists of continuous operation in varied environmental conditions.

This test area encompasses the following VVSG 2.0 requirements:

1.2-J, 2.7-B, 2.7-A, 2.7-A.1, 2.7-A.2, 2.4-B, 2.7-B, 2.7-C, 8.1-J.1, 8.1-J.2

Summary Findings

Testing was successfully completed with all actual results obtained during test execution matching the expected results. Any noted discrepancies were successfully resolved by the conclusion of the test campaign. The associated test parameters are described in the approved test plan for this test campaign. The Element Materials Technology test reports detailing the test methods and results of this testing are presented in *Attachment D.7* contained in *"Attachment D: Hardware Test Results*".

SECTION III.1.14.3 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.

This test area encompasses the following VVSG 2.0 requirements:

2.7-D, 2.7-E, 2.7-F

Summary Findings

Testing was successfully completed with all actual results obtained during test execution matching the expected results. Any noted discrepancies were successfully resolved by the conclusion of the test campaign. The associated test parameters are described in the approved test plan for this test campaign. The Element Materials Technology test reports detailing the test methods and results of this testing are presented in *Attachment D.1* contained in *"Attachment D: Hardware Test Results"*.

SECTION III.1.15 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. During this test area, the system was evaluated to ensure it meets specific VVSG 2.0 product marking and workmanship requirements.

This test area encompasses the following VVSG 2.0 requirements:

2.1.1, 2.1.1-A, 2.1.1-B, 2.1.1-C, 2.1.1-D, 2.1.2-C, 8.1-J.1, 8.1-J.2, 8.1-K

Summary Findings

Pro V&V reviewed the following Smartmatic-submitted product safety test report detailing successful completion of the product safety review of the Smartmatic VSR1 2.1 system:

- *Smartmatic USA Corporation Test Report, Safety testing of Smartmatic voting system models A4-800 and BMD-155, Intertek Report No. 150314051ATL-001, dated May 15, 2023*

Testing was successfully completed with all actual results obtained during test execution matching the expected results. Any noted discrepancies were successfully resolved by the conclusion of the test campaign.

SECTION IV: EVALUATION SUMMARY AND FINAL RECOMMENDATION

The following subsections contain an evaluation summary of the tests conducted, descriptions of anomalies or deficiencies encountered during testing, and a final recommendation for or against the grant of certification.

SECTION IV.1 EVALUATION SUMMARY

Pro V&V conducted a comprehensive evaluation of the Smartmatic VSR1 2.1 System to the applicable requirements set forth for voting systems in the U.S. Election Assistance Commission (EAC) Voluntary Voting System Guidelines (VVSG), Version 2.0. Based on the results obtained during the evaluation, Pro V&V concluded:

- The voting system is designed to accurately and completely carry out election processes, provide transparency, and can be accessed and used by voters regardless of their abilities.

- The source code for each application in the Smartmatic VRS1 2.1 System complies with VVSG 2.0 and the Smartmatic-submitted coding standards.
- The voting system is implemented using high quality best practices with clear and well-structured voting system logic and a modular and robust structure.
- The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.
- The documentation was sufficient to allow end-users to understand and verify the operations of the voting system throughout the entirety of the election.
- The results obtained during performance of the Functional Configuration Audit (FCA) verified that the system hardware and software performed all the functions described in the manufacturer's documentation submitted in the TDP (such as system operations, voter manual, maintenance, and diagnostic testing manuals).
- The voting system successfully met the pass/fail criteria for each of the required (operating and non-operating) hardware tests with no unscheduled system maintenance necessary and all documented discrepancies were resolved prior to the test campaign conclusion.

Specific Summary Findings for each test area are presented in Section III of this report.

SECTION IV.1.1 ANOMALIES

An anomaly occurs when a result is encountered during test performance that deviates from what is standard or expected. Pro V&V considers anomalies to be recordable events if the cause cannot be determined and/or if the anomalous condition cannot be reproduced. If the cause of the anomaly can be determined and/or the anomalous condition can be reproduced, this is considered a deficiency. No anomalies occurred during the testing of the Smartmatic VSR1 2.1 System.

SECTION IV.1.2 CORRECTION OF DEFICIENCIES

A deficiency is considered a non-conformity to the voting standard to which the voting system is being certified. Throughout the test campaign, any deficiencies encountered were logged in the Pro V&V tracking system (Mantis) for disposition and resolution. Each deficiency was designated either 'Significant' or 'Insignificant' based on its severity. In each instance, if applicable, the resolution was verified to be resolved through all required means of testing (regression testing, source code review, and TDP update) as needed. For all Significant deficiencies, Smartmatic conducted a root cause analysis (RCA) to determine the resolution. All RCAs were submitted to the VSTL and the EAC for review.

All deficiencies identified were successfully resolved prior to the test campaign completion. All additional findings, noted discrepancies, or deficiencies (if applicable) are detailed in *Attachment E: Additional Findings - PROPRIETARY*.

SECTION IV.1.3 FINAL RECOMMENDATION

The Smartmatic VSR1 2.1 System, as presented for testing, successfully met the required acceptance criteria of each applicable requirements set forth for voting systems in the U.S. Election Assistance Commission (EAC) Voluntary Voting System Guidelines (VVSG), Version 2.0. During the test campaign, Pro V&V conducted sufficient testing to determine the voting system meets the guidelines of each Principle described in VVSG 2.0.

Additionally, Pro V&V, Inc. has determined the Smartmatic VSR1 2.1 System functioned as a complete system during System Integration Testing and provides all the basic functionality, accessibility, and security capabilities required of voting systems. Based on the test findings, Pro V&V recommends the EAC grant the Smartmatic VSR1 2.1 System identified in this report certification to the EAC VVSG 2.0.

ATTACHMENT A: IMPLEMENTATION STATEMENT

This attachment is provided under separate cover.

ATTACHMENT B: WARRANT OF ACCEPTING CHANGE CONTROL RESPONSIBILITY

This attachment is provided under separate cover.

ATTACHMENT C: TRUSTED BUILD

This attachment is provided under separate cover.

ATTACHMENT D: HARDWARE TEST RESULTS

This Attachment is comprised of the Element Materials Technology test reports (Attachments D.1 through D.9) detailing the test methods and results of hardware testing.

ATTACHMENT E: ADDITIONAL FINDINGS - *PROPRIETARY*

Additional findings, noted discrepancies, or deficiencies (if applicable) resulting from this test campaign are presented in this attachment. This attachment is designated as proprietary and is not approved for publication; however, it was submitted to the EAC for review purposes.

ATTACHMENT F: TEST CASES - *PROPRIETARY*

Due to their proprietary nature, the test cases utilized during this campaign are not published within this test report; however, they were submitted to the EAC for review purposes.

ATTACHMENT G: SOURCE CODE REVIEW REPORT - *PROPRIETARY*

Due to its proprietary nature, the source code review report associated with this campaign is not published within this test report; however, it was submitted to the EAC for review purposes.

ATTACHMENT H: COMPLIANCE RESULTS MATRIX - *PROPRIETARY*

The VVSG 2.0 Compliance Results Matrix mapping the test cases to each requirement associated with this test campaign is designated as proprietary and is not approved for publication; however, it was submitted to the EAC for review purposes.