

Hart InterCivic Verity Vanguard 1.0 EAC Certification Test Plan

v3.0

HIN-23003-TP-03

Prepared for:

Vendor Name	<i>Hart InterCivic</i>
Vendor System	<i>Verity Vanguard 1.0</i>
EAC Application No.	<i>HRT-VV-1.0</i>

Prepared by:



**4720 Independence Street
Wheat Ridge, CO 80033
(303) 422-1566
<https://slicompliance.com/>**



***Accredited by the
Election Assistance Commission (EAC)
for selected Voting System
Test Methods or Services***



Revision History

Date	Version	Author	Revision Summary
5/22/2024	1.0	M. Santos	Initial Release
6/5/2024	2.0	M. Santos	Address EAC comments
6/13/2024	3.0	M. Santos	Address EAC comments

Disclaimer

The information reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government.

Trademarks

All products and company names are used for identification purposes only and may be trademarks of their respective owners.

Copyright © 2024 by SLI Compliance[®], a Division of Gaming Laboratories International LLC



Table of Contents

1. Introduction.....	6
1.1 References.....	6
1.2 Attachments.....	6
1.3 Terms and Abbreviations	7
1.4 Testing Responsibilities.....	9
1.4.1 Project Schedule	9
1.4.1.1 Owner Assignments.....	9
1.4.1.2 Test Case (Module) Development	9
1.4.1.3 Test Procedure Development and Validation	10
1.4.1.4 Third Party Hardware Testing.....	10
1.4.1.5 EAC & Manufacturer Dependencies.....	11
1.4.1.6 Formal Test Execution	11
1.5 Target of Evaluation Description.....	11
1.5.1 System Overview.....	11
1.5.2 Block Diagram	15
1.5.3 Supported Languages.....	15
1.5.4 Verify Vanguard 1.0 System Limits	16
1.5.5 Supported Functionality.....	17
1.5.5.1 Standard VVSG Functionality.....	17
1.5.5.2 Manufacturer Extensions	17
2. Pre-Certification Testing and Issues	17
2.1 Evaluation of prior VSTL Testing	17
2.2 Evaluation of Prior Non-VSTL Testing	17
2.3 Known Field Issues	17
3. Materials Required for Testing.....	18
3.1 Software/Firmware	18
3.1.1 Manufacturer Software/Firmware.....	18
3.1.2 COTS Software/Firmware	19



3.1.3	Additional Supporting Test Software.....	20
3.2	Verity Vanguard Equipment.....	21
3.2.1	Verity Vanguard Custom Equipment	21
3.2.2	COTS Equipment	21
3.2.3	Supporting Hardware Test Equipment	24
3.3	Test Materials.....	24
4.	Test Specifications	25
4.1	Requirements.....	25
4.1.1	Mapping of requirements to equipment type and features	25
4.1.2	Rationale for why some requirements are not applicable for this campaign	25
4.2	Verity Vanguard Hardware Configuration and Design.....	25
4.3	Software System Functions.....	26
4.3.1	Election Definition Creation – Vanguard Define.....	26
4.3.2	Election Media Creation – Vanguard Deploy.....	26
4.3.3	Pre-voting Aspects – Vanguard (Vault, Flex, Adapt, Boost, Capture)	26
4.3.4	Voting Aspects – Polling Place – Vanguard (Vault, Flex, Adapt, Boost)	26
4.3.5	Voting Aspects – Central Count – Vanguard Capture	26
4.3.6	Post Voting – Vanguard Results	27
4.3.7	Error Messaging and Recovery – Vanguard (All Components)	27
4.3.8	Auditing – Vanguard (All Components)	27
4.3.9	Security – Vanguard (All Components)	27
4.4	Test Case (Suite) Design	27
4.4.1	Software and Hardware Qualitative Examination Design	27
4.4.2	Hardware Test Case Design.....	28
4.4.3	Software Module Test Case Design and Data.....	29
4.4.4	Software Functional Test Case Design and Data.....	29
4.4.4.1	Component-level Test Suite Design.....	29
4.4.4.2	VVSG 2.0 Verification Test Suite Design	30
4.4.5	System-level Test Suite Design	32
4.5	Security Functions.....	34



4.5.1	Security Test.....	34
4.6	TDP Evaluation	35
4.7	Source Code Review.....	36
4.8	Trusted Build	36
4.9	Standard VSTL Test Methods and Uncertainty of Test Data Measurement.....	37
4.10	EAC Interpretations.....	37
5.	Test Data.....	38
5.1	Data Recording.....	38
5.2	Test Data Criteria	38
5.3	Test Data Reduction.....	39
6.	Test Procedure and Conditions	39
6.1	Facility Requirements.....	39
6.2	Test Setup.....	39
6.3	Test Sequence	40
7.	Test Operations Procedures	40
8.	Approval Signatures	41

List of Tables

Table 1 – Terms and Abbreviations	7
Table 2 – Hardware Test Labs.....	10
Table 3 – Verify Vanguard 1.0 Software/Firmware.....	18
Table 4 – Verify Vanguard COTS Software/Firmware	19
Table 5 – Additional Supporting Test Software	20
Table 6 – Verify Vanguard Custom Equipment	21
Table 7 – Verify Vanguard COTS Equipment	21
Table 8 – Additional Supporting Hardware Test Equipment.....	24



1. INTRODUCTION

This Voting System Test Plan outlines the test approach SLI Compliance will follow when performing testing on the **Hart InterCivic Verity Vanguard 1.0 (Vanguard)** voting system, against the Election Assistance Commission's Voluntary Voting System Guidelines version 2.0 (EAC VVSG 2.0). The purpose of this document is to provide a clear understanding of the work SLI Compliance will conduct and a detailed plan outlining the test effort.

When the testing is complete, SLI Compliance will submit a test report that details all test results and findings from the test effort, as well as a recommendation to the EAC.

1.1 References

The following key documents were used in preparing this test plan:

1. Election Assistance Commission Voluntary Voting System Guidelines (EAC VVSG), Version 2.0, February 10, 2021
2. VVSG Version 2.0 Test Assertions Version 1.3
3. NIST Handbook 150: 2020
4. NIST Handbook 150-22: 2021
5. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 3.0
6. SLI Compliance VSTL Quality System Manual, Rev. 4.1 Aug. 14, 2023

1.2 Attachments

The following attachments apply to this Voting System Test Plan:

- Attachment A – Supported VVSG 2.0 Functionality
- Attachment B – Manufacturer Extensions
- Attachment C – Verity Vanguard 1.0 Test Matrix – **PROPRIETARY**
- Attachment D – Vanguard EAC Project Plan
- Attachment E – Technical Data Package Listing
- Attachment F – Accredited Hardware Test Lab Certification



1.3 Terms and Abbreviations

Table 1 defines terms and abbreviations used throughout this document.

Table 1 – Terms and Abbreviations

Term	Abbreviation	Description
American Association for Laboratory Accreditation	A2LA	A nonprofit, non-governmental, public service, membership society whose mission is to provide comprehensive services in laboratory accreditation and laboratory-related training.
Ballot Marking Device	BMD	An accessible computer-based voting system that produces a marked ballot (usually paper) that is the result of voter interaction with visual or audio prompts.
Central Count Scanner	CCS	A mark sense-based ballot and vote counting device typically located at a central count facility and is operated by an automated multi-sheet feeding capability.
Compact Flash card	CF	This is a type of flash memory card in a standardized enclosure often used in voting systems to store ballot and/or vote results data.
Commercial Off the Shelf	COTS	Term used to designate computer software, hardware or accessories that are ready-made and available for sale, lease, or license to the general public
Election Assistance Commission	EAC	An independent, bipartisan commission created by the Help America Vote Act (HAVA) of 2002 that operates the federal government's voting system certification program.
Election Management System	EMS	Typically a database management system used to enter jurisdiction information (district, precincts, languages, etc.) as well as election specific information (races, candidates, voter groups (parties), etc.). In addition, the EMS is also used to lay out the ballots, download the election data to the voting devices, upload the results and produce the final results reports.
Electromagnetic Compatibility	EMC	The goal of EMC is to validate the correct functioning of different equipment in the same environment and the avoidance of any interference effects between them.
Institute of Electrical and Electronics Engineers	IEEE	A non-profit professional association for the advancement of technology.



Term	Abbreviation	Description
National Institute of Standards and Technology	NIST	A non-regulatory federal agency within the U.S. Dept. of Commerce. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.
National Voluntary Laboratory Accreditation Program	NVLAP	A division of NIST that provides third-party accreditation to testing and calibration laboratories.
Precinct Count Scanner	PCS	A precinct-count optical scanner is a mark sense-based ballot and vote counting device located at a precinct and is typically operated by scanning one ballot at a time.
Request For Interpretation	RFI	A means used by testing laboratories and manufacturers to request that the EAC provide an interpretation of a technical issue related to testing of voting systems.
Technical Data Package	TDP	The data package supplied by the vendor, which includes Functional Requirements, Specifications, End-user documentation, Procedures, System Overview, Configuration Management Plan, Quality Assurance Program, and manuals for each of the required hardware, software, firmware components of a voting system.
Voluntary Voting System Guidelines	VVSG	A set of specifications and requirements against which voting systems can be tested to determine if the systems provide all of the basic functionality, accessibility and security capabilities required for EAC certification.
Voting System Test Lab	VSTL	An independent testing organization accredited by NVLAP and the EAC to conduct voting system testing for EAC certification.
Voting System Under Test	VSUT	The designation for a voting system that is currently being tested.
Voting Test Engineer	VTE	An SLI Compliance employee who has been qualified to perform EAC voting system testing.



1.4 Testing Responsibilities

The following project schedule contains owner assignments and identifies test procedure (module) development, test case (suite) development, third party tests, and EAC and Manufacturer dependency.

1.4.1 Project Schedule

The subsections below describe the project schedule.

1.4.1.1 Owner Assignments

Test Manager, M. Santos, is responsible for oversight and approvals for this test campaign. Work is conducted by SLI Compliance's trained and authorized Voting Test Engineers.

- System analysis and review will be conducted by Source Code Review, Security and Voting Test Engineers, with oversight by the Test Manager.
- Source code review will be conducted by Voting Test Engineers (Source Code Review Specialists), with oversight by the Test Manager.
- The trusted build will be conducted by Voting Test Engineers trained in the trusted build process.
- Documentation review will be conducted by Security and Voting Test Engineers, with oversight by the Test Manager.
- Test module development will be conducted by Security and Voting Test Engineers, with oversight by the Test Manager.
- Test suite development will be conducted by Security and Voting Test Engineers utilizing SLI Compliance's formal test methods, with oversight by the Test Manager.
- Formal test execution will be conducted by Security and Voting Test Engineers, with oversight by the Test Manager.
- Third Party testing will be conducted by the subcontracting third party hardware laboratories, with oversight by the Hardware Test Engineer.

1.4.1.2 Test Case (Module) Development

Test modules will be developed to provide detailed, repeatable test steps. The modules are defined at a basic level in SLI Compliance's formal test methods and are designed for use in any suite that employs their functionality. This reusability reduces the development time associated with creating test procedures. The test modules will provide traceability to SLI Compliance's formal test methods as well as the VVSG requirements. This is done by identifying the test method name and listing each requirement addressed in the module.



1.4.1.3 Test Procedure Development and Validation

Test Procedures (Suites) will be developed to help group and focus testing around key areas of the voting system. The test suites will contain multiple test modules providing clear and traceable test scripts and key information. As needed for the system under test, various configurations will be identified within the suites. Variations of the same suite may be run multiple times to verify different configurations.

1.4.1.4 Third Party Hardware Testing

Hardware testing will be conducted by Third Party certified hardware test laboratories to verify the voting system devices are in compliance with the VVSG hardware requirements.

SLI Compliance is responsible for all core voting system tests as defined in the EAC Program Manuals. The labs listed below will perform non-core testing for this test campaign.

Table 2 – Hardware Test Labs

Laboratory	Address	Test(s)
Element Materials Technology Denver-Longmont (A2LA certified for Electromagnetic Compatibility/ Interference (EMC/EMI), Lightning, Transient, and Surge tests)	1736 Vista View Drive Longmont, CO 80504	<u>EMC / EMI Tests:</u> <ul style="list-style-type: none"> • Radiated Emissions • Conducted Emissions • ESD • Electromagnetic Susceptibility • Electrical Fast Transient • Lightning Surge • Conducted RF Immunity • Electrical Power Disturbance (Voltage Dips)
Element Materials Technology Denver-Longmont (A2LA certified for mechanical including MIL STD 810)	1601 Dry Creek Drive Longmont, CO 80503	<u>MIL-STD-810H Tests:</u> <ul style="list-style-type: none"> • Bench Handling, Vibration • Low Temperature • High Temperature • Continuous Operation – Varied Envir. Conditions Low / High Temp / Humidity • Reliability



1.4.1.5 EAC & Manufacturer Dependencies

The Test Plan will require EAC approval prior to finalization.

Hart InterCivic (Hart) will be required to provide all source code, documentation, equipment and supporting materials identified as part of the voting system.

The source code must have all discrepancies resolved, be successfully built and the outputs installed, and the components must pass operational status checks prior to formal test execution.

In addition, **Hart** is required to provide training on the voting system and support throughout the life of the project.

Please see the “Attachment D - Vanguard EAC Project Plan” for a listing of activities within the scope of this test campaign.

1.4.1.6 Formal Test Execution

Formal execution of the approved test suites and modules will be conducted to verify the system’s compliance with the VVSG 2.0 requirements.

1.5 Target of Evaluation Description

1.5.1 System Overview

The **Hart InterCivic Verity Vanguard 1.0** voting system is a paper-based voting system comprised of both precinct and central count tabulators along with a Ballot Marking Device (BMD) and a hybrid BMD/Precinct Tabulator. All polling place devices are able to utilize Americans with Disabilities Act (ADA) components.

The **Verity Vanguard 1.0** voting system’s major components include Vanguard **Workspace**, Vanguard **Define**, Vanguard **Deploy**, Vanguard **Capture**, Vanguard **Results**, Vanguard **Boost**, Vanguard **Flex**, Vanguard **Adapt** and Vanguard **Vault**.

The Vanguard Workspace (EMS)

Vanguard Workspace is the Vanguard workstation home screen. The Vanguard workspace displays tiles for each of the installed Vanguard components. The components displayed are based on the roles and permissions assigned to the current user by the System Administrator.

The Manage application is used to create new elections, archive and restore elections, and export signed elections.

The Users application is used to create and manage Vanguard users and write security tokens.

The Settings application is used to perform additional workstation functions such as setting the clock and exporting file hashes.



Additionally, unlockable applications may be displayed on the lower right of the Home screen. These applications provide additional functionality when working with elections in Vanguard.

Vanguard Define (Pre-Election EMS)

Vanguard Define is a component of the Verity Vanguard voting system used by election officials to enter election data for contests, candidates, proposition text, translations, and audio. Vanguard Define also provides the user with controls for proofing of data and layout and performs validation prior to locking the data to ensure its readiness for use in Vanguard Deploy, the election definition software.

Vanguard Deploy (Pre-Election EMS)

Vanguard Deploy is used by officials to complete pre-voting tasks for creating and generating an election definition and ballots. Vanguard Deploy provides a ballot layout proofing process. The process establishes relationships between election data, jurisdiction, and polling place data, for the shared election definition. Vanguard Deploy will create the portable media, vDrives, to provide a method of transferring the shared election definition to Verity Vanguard voting devices and workstations.

Note that Vanguard Define and Vanguard Deploy share the same environment, so are fielded on the same workstation.

Vanguard Define/Deploy can include a stand-alone workstation or multiple Vanguard Capture workstations that are networked on a closed LAN in a server/client configuration. The closed LAN cannot connect to other LANs or systems, ensuring the air gap remains for security of data.

Vanguard Capture (Central Scan)

Vanguard Capture is used by officials for paper ballot scanning, contest resolution, and conversion of voter selection marks to electronic Cast Vote Records (CVRs). Once the CVRs are written to vDrive(s) they can be transferred into Vanguard Results for vote tabulation and reporting of election results. Vanguard Capture records cast vote records only; it does not tabulate.

Vanguard Capture can include a stand-alone workstation or multiple Vanguard Capture workstations that are networked on a closed LAN in a server/client configuration. The closed LAN cannot connect to other LANs or systems, ensuring the air gap remains for security of data.

Vanguard Results (Post-Election EMS)

Vanguard Results is used by officials to complete post-voting functionality to tabulate election results and generate reports. Vanguard Results receives the CVRs from portable media devices (vDrives) used to record CVRs from Vanguard Vault devices or Vanguard Capture workstations. Vanguard Results can be used by officials to resolve Vault or Vanguard Capture write-in votes for paper ballots that were manually marked.



Vanguard Results can also be used to collect and store all election logs from every Verity Vanguard device used in the election, allowing for complete election audit log reviews.

Vanguard Results can include a stand-alone workstation or multiple Vanguard Results workstations that are networked on a closed LAN in a server/client configuration. The closed LAN cannot connect to other LANs or systems, ensuring the air gap remains for security of data.

Vanguard Manage (EMS)

Vanguard Manage is available only within server and standalone workstation software applications. This software enables authorized users to add, copy, import, export, archive, restore, and manage elections. Once an election is added or imported in the Election Management application, the election can be opened and handled per the features available within the Vanguard software installed on that workstation.

Vanguard Boost (Polling Place Ballot Issuance)

Vanguard Boost is a poll worker facing device designed to improve voter service by optimizing ballot issuance in the polling place. Vanguard Boost can be utilized by poll workers in two ways. Boost may be used to print blank paper ballots on demand, using an attached ballot printer. Boost may also be used to issue VotePasses, which allow voters to access, mark, and print a printed vote record using Vanguard Flex or Adapt. Vanguard Boost does not store vote data.

Vanguard Flex (Polling Place BMD)

Vanguard Flex is a universal ballot marking device that produces an auditable summary ballot of a voter's choices. Voters can mark their ballots using the touchscreen interface or a wide variety of accessible controls. Printed summary ballots are then scanned in Verity Vault for tabulation.

Vanguard Vault (Polling Place Precinct Scanner)

Vanguard Vault is a polling place scanning device that captures voter choices whether using ballots marked by hand or machine, including summary ballots (printed vote records (PVRs)).

Vanguard Adapt (Polling Place Limited Dexterity Mark, Verify and Cast device)

Vanguard Adapt is an all-in-one voting device that produces an auditable summary ballot of a voter's choices. Voters can mark their ballots using the touchscreen interface or a wide variety of accessible controls. Vanguard Adapt enables voters to mark, verify, and cast their ballot all without touching a piece of paper.

Vanguard Libraries (EMS)

Vanguard Libraries is an application that can be unlocked on any Vanguard Define/Deploy workstation. Libraries allows users to save translations and audio from any Vanguard election and use them in future elections. Translations and audio in



Vanguard Libraries can be imported into any election in the Vanguard Define application on the same workstation.

Vanguard Test Decks (EMS)

Vanguard Test Decks is an application that can be unlocked on any Vanguard Define/Deploy workstation. Test Decks allows users to generate a pre-marked set of ballots (a “Test Deck”) that can be used for Logic and Accuracy Testing of the Vanguard voting system. Test Decks allows users to select a marking pattern and generate a test deck which is then available to print and/or export within the Vanguard Deploy software application.

Vanguard Ranked Choice (EMS)

Vanguard Ranked Choice is an application that can be unlocked on any Vanguard Results workstation. Ranked Choice allows users to perform tabulation of ranked choice contest results that have been read into Vanguard Results.

Auxiliary System Components

Verity Access (Polling Place)

Verity Access is an Audio-Tactile Interface (ATI) module that is optionally connected to Vanguard Flex and is optional for all other devices as well. Access has three tactile buttons, one audio port, and one port for external tactile buttons or sip and puff devices. Jacks for headphones and adaptive devices are located on the top edge of the device, and the device has grip surfaces on either side.

Verity AutoBallot (Polling Place)

AutoBallot is an optional barcode scanner kit for all instances of ballot activation, including Vanguard Flex, Boost, and Adapt. AutoBallot allows air-gapped integration between an e-pollbook check-in process and the task of selecting the proper ballot style for the voting system. AutoBallot simplifies and automates the ballot style selection process in Vote Centers by allowing poll workers to scan a barcode output from an electronic poll book and activate the correct ballot style with the click of a button, thereby reducing human error. Once the ballot style has been input with the barcode scanner, the poll worker confirms the ballot style on the device display.

vDrive – Electronic Media

Verity vDrive is a required Vanguard component, used as a portable media device generated by Vanguard Deploy. The vDrive allows election definitions to be moved from Deploy to other device and workstation software. vDrive supports the transfer of Cast Vote Records (CVRs) from Vanguard Vault and Vanguard Capture.

Verity Key

Verity Key is an electronic media that is created by Verity Deploy for a specific election. Verity Key is the electronic media that provides user authentication and configures election security throughout the Verity Vanguard system.

Security Token

The Vanguard Security Token is a physical software security token for Multifactor Authentication. The Security Token is assigned to a workstation user and is used in conjunction with user credentials to allow secure access to Vanguard voting system components.

1.5.2 Block Diagram

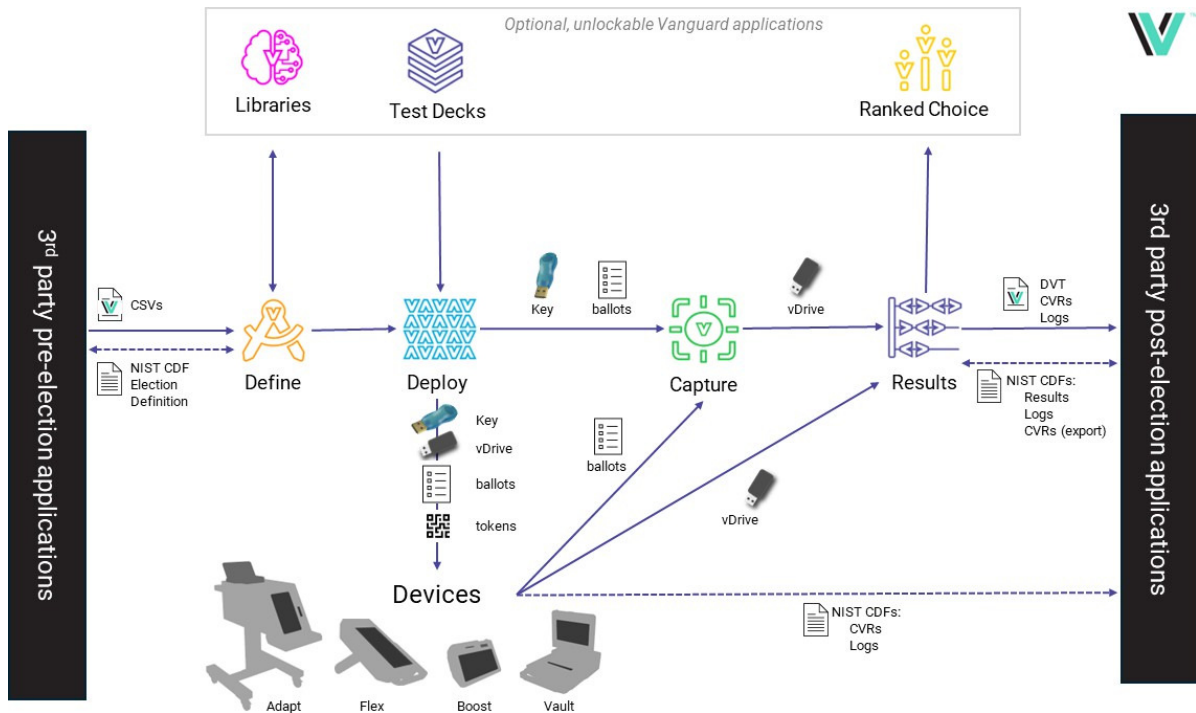


Figure 1 – Verity Vanguard 1.0 System Diagram

1.5.3 Supported Languages

Verity Vanguard 1.0 supports the following 19 languages: • English • Spanish • Mandarin Chinese • Japanese • Korean • Khmer • Thai • Vietnamese • Tagalog • Ilocano • Hindi • Haitian Creole • Gujarati • Hmong • Lao • Hawaiian • Cantonese Chinese • Punjabi • Bengali



1.5.4 Verify Vanguard 1.0 System Limits

Item	Upper Limit
Languages in a single election	19 (including English)
Precincts in an Election	3,000
Splits per Precinct	20
Total Precincts and Splits in an Election	3,000
Districts in an Election	400
Polling Places in an Election	3,050
Parties in a General Election	24
Parties in a Primary Election	10
Contests (incl. Propositions) in an Election	2,000
Contest Choices (voting positions) in a Contest	300
Total number of Contest Choices in an Election (independent from ballot size)	5,000
Unique write-in values per contest (Results)	500
Unique write-in values per task (Results)	40,000
Voting Types in an Election	10
Tasks per Election (Capture, Results)	15
Registered Voters per Precinct (Results)	99,999
Maximum Sheets per ballot	4
Ballot Stubs per ballot	2
Scan rate (Capture)	8.5"x11": 60 PPM 8.5"x14": 60 PPM 8.5"x17": 50 PPM 8.5"x20": 50 PPM 8.5"x22": 50 PPM 11"x17": 40 PPM
Scan rate (Vault)	PVRs: Up to 6 PPM for PVRs (any size) Standard Ballots: Up to 8 PPM for 8.5"x11", decreases linearly to 4 PPM for 8.5"x22
Ballots per vDrive: Vault (1 sheet ballot)	25,000*
Ballots per vDrive: Capture	20,000
Ballots per election: Capture & Results	1,750,000
vDrives per election: Results	3,050
Ballot Sizes - Deploy, Capture, Boost, Vault	8.5"x11", 8.5"x14", 8.5"x17", 8.5"x20", 8.5"x22"
Ballot Sizes - Deploy, Capture (also includes)	11"x17"
Printed Vote Record page size - Flex	8.5"x11", 8.5"x14",
Printed Vote Record page size - Adapt	8.5"x11"



**The ballot limit for Verity Vault is a recommended limit for the number of single-sheet ballots scanned on an individual Verity Vault during a single election. For a two-sheet ballot, divided this number by 2; for a 4-sheet ballot divide this number by 4.*

1.5.5 Supported Functionality

The following standard VVSG functionality and manufacturer extensions are included in the voting system.

1.5.5.1 Standard VVSG Functionality

Please see “Attachment A – Supported VVSG 2.0 Functionality” for a listing of Verity Vanguard 1.0 supported VVSG 2.0 functionality.

1.5.5.2 Manufacturer Extensions

Please see “Attachment B – Manufacturer Extensions” for a listing of Verity Vanguard 1.0 manufacturer extensions.

2. PRE-CERTIFICATION TESTING AND ISSUES

For this initial certification testing of Verity Vanguard 1.0 to VVSG 2.0, no previous testing is being leveraged. All pertinent VVSG 2.0 requirements will be applied to relevant portions of Verity Vanguard 1.0 during this test campaign.

2.1 Evaluation of prior VSTL Testing

For this initial certification of Verity Vanguard 1.0 to VVSG 2.0, no previous VSTL testing is being evaluated.

2.2 Evaluation of Prior Non-VSTL Testing

As this is the initial certification test of Verity Vanguard 1.0, the system has not been fielded anywhere, nor been evaluated, so no previous Non-VSTL testing is being evaluated.

2.3 Known Field Issues

Verity Vanguard 1.0 has not been fielded anywhere, so has no known field issues in Verity Vanguard.

Verity Voting had an anomaly in Verity Count where only the first one hundred write-ins for a contest were being shown.

Verity Voting had an anomaly in Verity Data where Party Selection contest for Straight Party elections may not appear on printed ballots when certain conditions are met

Verity Voting had anomalies in Verity Data with text translation issues in Chinese and Vietnamese where inserting a sheet correctly in Touch Writer Duo, instead of indicating a successful insertion, the device displayed Chinese text that indicated



“Sheet inserted incorrectly”. Additionally, in Vietnamese, a button used to scroll and see additional choices read “More choices”, where the English equivalent was “More Choices... touch here”.

Known issues will be verified to be resolved in Verity Vanguard 1.0.

3. MATERIALS REQUIRED FOR TESTING

Any materials used in an election cycle must be provided to SLI Compliance to facilitate testing of the voting system. This section outlines such materials.

3.1 Software/Firmware

All software and firmware used by the voting system, whether directly or indirectly, in a production environment must be validated during the testing process.

The following software/firmware is required for the execution of hardware, software, telecommunications, and security tests. This includes all supporting software such as operating systems, compilers, assemblers, application software, firmware, and any applications used for burning of media, transmission of data or creation/management of databases.

3.1.1 Manufacturer Software/Firmware

The table below lists the Verity Vanguard 1.0 system Software/Firmware.

Table 3 – Verity Vanguard 1.0 Software/Firmware

Component	Component Type	Software
Define (Pre-election EMS)	Workstation Software	1.0.0
Deploy (Pre-election EMS)	Workstation Software	1.0.0
Capture (Central Count)	Workstation Software	1.0.0
Results (Post-election EMS)	Workstation Software	1.0.0
Manage (EMS)	Workstation Software	1.0.0
Ranked Choice (EMS)	Workstation Software	1.0.0
Libraries (EMS)	Workstation Software	1.0.0
Test Decks (EMS)	Workstation Software	1.0.0
Boost (Polling Place Ballot Issue)	Polling Place Device	1.0.0
Flex (Polling Place BMD)	Polling Place Device	1.0.0
Vault (Polling Place Scanner)	Polling Place Device	1.0.0
Adapt (Polling Place All in one BMD)	Polling Place Device	1.0.0



3.1.2 COTS Software/Firmware

Table 4 – Verity Vanguard COTS Software/Firmware

Workstations (Define/Deploy, Capture, Results)		
Manufacturer	Application	Version
Microsoft	Windows 10 Enterprise 2019 LTSC Configured for Verity Kiosk Operations	10.0.19044
Canon	DR-G2000 Series Driver	1.0.6904
NVIDIA	NVIDIA Graphics Driver	531.41
NVIDIA	NVIDIA HD Audio Driver	1.3.40.14
Maxim	1-Wire Driver	4.1.0
McAfee	Application Control for Devices (“Solidifier”) Configured for Verity Kiosk	8.3.5.126
Microsoft	Help Viewer	2.3.28107
Microsoft	Microsoft SQL Server Standard 2019	15.04345.5
Microsoft	Visual Studio C++ 2013 Redistributable x64	12.0.30501.0
Microsoft	Visual Studio C++ 2013 Redistributable x86	12.0.40660.0
Microsoft	Visual Studio C++ 2015-2022 Redistributable x64	14.36.32532.0
Microsoft	Visual Studio C++ 2015-2022 Redistributable x86	14.36.32532.0
OKIDATA	OKI USBDevice	1.0.0.0
OKIDATA	OKI USBDevice	1.0.2.0
IntoPrint	SP1360(PCL6) Driver	1.0.0.0
Brother	HL-6400DWVS Driver	10.0.19041.1
HP	HP LaserJet Pro 4001 4002 4003 4004 PCL 6	10.0.19041.1
TWAIN Working Group	Twacker 32	2.5.0
TWAIN Working Group	Twacker 64	2.5.0
Open Source	Tesseract Open Source OCR Engine	4.5.411



Devices (Vault, Flex, Adapt, Boost)		
Manufacturer	Application	Version
Microsoft	Windows 10 Enterprise 2019 LTSC Configured for Verity Kiosk Operations	10.0.19044
Maxim	1-Wire Driver	4.1.0
McAfee	Application Control for Devices ("Solidifier") Configured for Verity Kiosk	8.3.5.126
SQLite	SQLite	3.45.3
Microsoft	Visual Studio C++ 2015-2022 Redistributable x86	14.34.31931
Microsoft	Visual Studio C++ 2015-2022 Redistributable x64	14.34.31931
Seiko Instruments	SII IFD50x Driver	2.5.0.0
Open Source	Tesseract Open Source OCR Engine	4.5.411
Brother	Brother Printer Setting Tool	1.6.0051
Brother	Brother HL-L6400DWVS Printer Driver	1.8.168.8
PDI	PDIPrint Thermal Printer Utility	1.6.6
PDI	PageScan Scanner SDK	7.1.0.7
PDI	PageScan USB Scanner Driver	4.0.0301.13
PDI	PDIPrintScanCut Driver for TPH850 printer	4.0.0.0
HP	HP LaserJet Pro 4001 4002 4003 4004 PCL 6	10.0.19041.1
HP	HP OfficeJet 200 Mobile Series	10.0.19041.1
OKI Data	OKI C844(PCL)	1.0.0.0

3.1.3 Additional Supporting Test Software

This section outlines all test specific software that will be used in the test campaign.

Table 5 – Additional Supporting Test Software

Manufacturer	Application	Version
Tenable	Nessus Professional	10.7.1
Wireshark Foundation	Wireshark	4.2.5
Mh-nexus	HxD	2.5.0.0
Kali	Kali Linux	2024.1
GCHQ	CyberChef	10.18.6
WebAIM.org	Contrast Checker	N/A



3.2 Verity Vanguard Equipment

The following equipment is required for the execution of the hardware, software, telecommunications, and security tests. This includes system hardware, general purpose data processing and communications equipment, and any test instrumentation required.

3.2.1 Verity Vanguard Custom Equipment

The following **Vanguard 1.0** custom equipment will be used in testing:

Table 6 – Verity Vanguard Custom Equipment

Manufacturer	Hardware	Model
Hart InterCivic	Precinct Scanner	Vanguard Vault
Hart InterCivic	Ballot Marking Device (BMD)	Vanguard Flex
Hart InterCivic	All-in-one (Limited Dexterity Mark, Verify, and Cast) device	Vanguard Adapt
Hart InterCivic	Ballot Issuance device	Vanguard Boost

3.2.2 COTS Equipment

The following Commercial Off-the-Shelf equipment will be used in testing:

Table 7 – Verity Vanguard COTS Equipment

Component	Component Type	Associated COTS Hardware
Manage	Workstation Software	<ul style="list-style-type: none"> • Runs on the following COTS workstations: <ul style="list-style-type: none"> ○ HP Z2 SFF G9 workstation ○ HP Z4 G4 workstation ○ HP P 24 G5, P24 G4, P244 monitors • Uninterruptible Power Supply for backup power: <ul style="list-style-type: none"> ○ Duracell DR660PSS
Define	Workstation Software	<ul style="list-style-type: none"> • Runs on the following COTS workstations: <ul style="list-style-type: none"> ○ HP Z2 SFF G9 workstation ○ HP Z4 G4 workstation ○ HP P 24 G5, P24 G4, P244 monitors • Uninterruptible Power Supply for backup power: <ul style="list-style-type: none"> ○ Duracell DR660PSS • Compatible with the following COTS printers: <ul style="list-style-type: none"> ○ Brother HL-L6400DW series mono laser printer ○ Brother HL-EX415DW series mono laser printer ○ HP LaserJet Pro 4001dn series mono laser printer • Supports local networked configuration for scale, compatible with the following COTS Ethernet switches: <ul style="list-style-type: none"> ○ HP 1405-8GV3 8-port Ethernet Switch ○



Component	Component Type	Associated COTS Hardware
Deploy	Workstation Software	<ul style="list-style-type: none"> • Runs on the following COTS workstations: <ul style="list-style-type: none"> ○ HP Z2 SFF G9 workstation ○ HP Z4 G4 workstation ○ HP P 24 G5, P24 G4, P244 monitors • Uninterruptible Power Supply for backup power: <ul style="list-style-type: none"> ○ Duracell DR660PSS • Compatible with the following COTS printers: <ul style="list-style-type: none"> ○ Brother HL-L6400DW series mono laser printer ○ Brother HL-EX415DW series mono laser printer ○ HP LaserJet Pro 4001dn series mono laser printer ○ OKI Data C831dn color laser printer ○ OKI Data C844dn color laser printer ○ OKI Data C911dn color laser printer ○ OKI Data C931e color laser printer ○ IntoPrint SP1360 color laser printer • Supports local networked configuration for scale, compatible with the following COTS Ethernet switches: <ul style="list-style-type: none"> ○ HP 1405-8GV3 8-port Ethernet Switch • Supports duplication of blank vDrives: <ul style="list-style-type: none"> ○ VinPower Digital USBShark-7T-BK ○ VinPower Digital SBDupeBoxES-23T, USBShark-23T-BK
Capture	Workstation Software	<ul style="list-style-type: none"> • Runs on the following COTS workstations: <ul style="list-style-type: none"> ○ HP Z2 SFF G9 workstation ○ HP Z4 G4 workstation ○ HP P 24 G5, P24 G4, P244 monitors • Uninterruptible Power Supply for backup power: <ul style="list-style-type: none"> ○ Duracell DR660PSS • Compatible with the following COTS printers: <ul style="list-style-type: none"> ○ Brother HL-L6400DW series mono laser printer ○ Brother HL-EX415DW series mono laser printer ○ HP LaserJet Pro 4001dn series mono laser printer • Compatible with the following COTS scanners <ul style="list-style-type: none"> ○ Canon DR-G2110 High-Speed scanner ○ Canon DR-G2140 High-Speed scanner • Supports local networked configuration for scale, compatible with the following COTS Ethernet switches: <ul style="list-style-type: none"> ○ HP 1405-8GV3 8-port Ethernet Switch
Results	Workstation Software	<ul style="list-style-type: none"> • Runs on the following COTS workstations: <ul style="list-style-type: none"> ○ HP Z2 SFF G9 workstation ○ HP Z4 G4 workstation ○ HP P 24 G5, P24 G4, P244 monitors • Uninterruptible Power Supply for backup power: <ul style="list-style-type: none"> ○ Duracell DR660PSS • Compatible with the following COTS printers:



Component	Component Type	Associated COTS Hardware
		<ul style="list-style-type: none"> ○ Brother HL-L6400DW series mono laser printer ○ Brother HL-EX415DW series mono laser printer ○ HP LaserJet Pro 4001dn series mono laser printer ● Supports local networked configuration for scale, compatible with the following COTS Ethernet switches: <ul style="list-style-type: none"> ○ HP 1405-8GV3 8-port Ethernet Switch
Ranked Choice	Workstation Software	<ul style="list-style-type: none"> ● Runs on the following COTS workstations: <ul style="list-style-type: none"> ○ HP Z2 SFF G9 workstation ○ HP Z4 G4 workstation ○ HP P 24 G5, P24 G4, P244 monitors ● Uninterruptible Power Supply for backup power: <ul style="list-style-type: none"> ○ Duracell DR660PSS ● Compatible with the following COTS printers: <ul style="list-style-type: none"> ○ Brother HL-L6400DW series mono laser printer ○ Brother HL-EX415DW series mono laser printer ○ HP LaserJet Pro 4001dn series mono laser printer
Libraries	Workstation Software	<ul style="list-style-type: none"> ● Runs on the following COTS workstations: <ul style="list-style-type: none"> ○ HP Z2 SFF G9 workstation ○ HP Z4 G4 workstation ○ HP P 24 G5, P24 G4, P244 monitors ● Uninterruptible Power Supply for backup power: <ul style="list-style-type: none"> ○ Duracell DR660PSS
Test Decks	Workstation Software	<ul style="list-style-type: none"> ● Runs on the following COTS workstations: <ul style="list-style-type: none"> ○ HP Z2 SFF G9 workstation ○ HP Z4 G4 workstation ○ HP P 24 G5, P24 G4, P244 monitors ● Uninterruptible Power Supply for backup power: <ul style="list-style-type: none"> ○ Duracell DR660PSS
Boost	Polling Place Device	<ul style="list-style-type: none"> ● Compatible with the following COTS printers: <ul style="list-style-type: none"> ○ Brother HL-L6400DW series mono laser printer ○ Brother HL-EX415DW series mono laser printer ○ HP LaserJet Pro 4001dn series mono laser printer ○ OKI Data C844dn color laser printer ● Uninterruptible Power Supply for backup power for printers: <ul style="list-style-type: none"> ○ Duracell DR660PSS ● Supports AutoBallot which is compatible with the following COTS barcode scanners: <ul style="list-style-type: none"> ○ Motorola/Zebra DS4308 handheld barcode scanner ○ Zebra Technologies DS4608 handheld barcode scanner
Flex	Polling Place Device	<ul style="list-style-type: none"> ● Supports AutoBallot which is compatible with the following COTS barcode scanners: <ul style="list-style-type: none"> ○ Motorola/Zebra DS4308 handheld barcode scanner ○ Zebra Technologies DS4608 handheld barcode scanner ● Supports Polling Place devices:



Component	Component Type	Associated COTS Hardware
		<ul style="list-style-type: none"> ○ Bausch & Lomb 819007 Full Page Framed Magnifier ○ Inclusion Solutions 436 Full Page Framed Magnifier
Adapt	Polling Place Device	<ul style="list-style-type: none"> ● Supports AutoBallot which is compatible with the following COTS barcode scanners: <ul style="list-style-type: none"> ○ Motorola/Zebra DS4308 handheld barcode scanner ○ Zebra Technologies DS4608 handheld barcode scanner ● Supports Polling Place devices: <ul style="list-style-type: none"> ○ Bausch & Lomb 819007 Full Page Framed Magnifier ○ Inclusion Solutions 436 Full Page Framed Magnifier

3.2.3 Supporting Hardware Test Equipment

The following hardware support equipment will be used in testing:

Table 8 – Additional Supporting Hardware Test Equipment

Hardware
Lock-pick tool set
Assorted screwdrivers
Stopwatch
Temperature/Humidity gauge
Decibel Sound reader

3.3 Test Materials

The following test materials are required for the performance of testing including, as applicable, test ballot layout and generation materials, test ballot sheets, test ballot cards and control cards, standard and optional output data report formats, and any other materials used in testing.

- Ballot stock (all supported sizes)
- Printed Vote Record (PVR) ballot stock
- CFast cards
- Thumb drives
- Ballot marking pens
- Printer paper rolls
- 2FA media
- Ballot Activation Media



4. TEST SPECIFICATIONS

The following are the specifications for testing to be conducted on the **Hart InterCivic Verity Vanguard 1.0**. The specifications contain details on the focus of testing, configuration(s), and the functions to be tested. Additional information is provided in the associated appendices.

4.1 Requirements

The **Hart InterCivic Verity Vanguard 1.0** will be tested to the approved EAC VVSG 2.0 requirements and test assertions, as well as all published RFIs. All EAC VVSG 2.0 requirements and associated test assignments can be found in “Attachment C – Verity Vanguard 1.0 Test Case Matrix”.

All requirements within VVSG 2.0 are verified against the **Hart InterCivic Verity Vanguard 1.0** voting system unless noted otherwise below.

4.1.1 Mapping of requirements to equipment type and features

All EAC VVSG 2.0 requirements and associated test assignments can be found in “Attachment C – Verity Vanguard 1.0 Test Case Matrix”.

4.1.2 Rationale for why some requirements are not applicable for this campaign

Verity Vanguard 1.0 does not implement the following VVSG 2.0 functionality:

- Group voting contest (1.1.4-R, 1.1.8-K)
- Top-2 IRV contest (1.1.4-S)
- COTS language extensions (2.1-B)
- Voter Speech (7.2-F)
- Telephone style handset (8.1-G)
- Cryptographic E2E verifiable (9.1.6)
- E2E cryptographic protocols (13.3-B)

4.2 Verity Vanguard Hardware Configuration and Design

The **Hart InterCivic Verity Vanguard 1.0**, as declared in the application for certification submitted to the EAC, consists of the following:

- A **Verity Define/Deploy** workstation is used to create the election definition and all election media.
- At the polling place level, **Vanguard Vault** optical scanners, **Vanguard Flex** ballot marking devices, and **Vanguard Adapt** all-in-one BMDs are employed. Vanguard Boost is an optional polling place ballot issuance device that will be utilized.



- The **Vanguard Capture** employs a high-speed COTS scanner in combination with a workstation for tabulation of absentee ballots.
- The consolidation, tally and reporting location employs a workstation with **Vanguard Results** software as well as a printer.

4.3 Software System Functions

The **Hart InterCivic Verity Vanguard 1.0** system operations documentation has been reviewed in conjunction with the Implementation Statement provided by the manufacturer. Based on VVSG 2.0 requirements, the applicable system functions have been identified for testing. The following key areas of voting system functionality will be evaluated during test case design.

4.3.1 Election Definition Creation – Vanguard Define

The Election Definition focus will target creation of contests, candidates, propositions, ballot formatting and instruction. All aspects of creating regional districts, jurisdictional parameters, grouping and displaying of associated election data will be analyzed and tested. In addition, the ability to support baseline election types, various other election types, voting variations and supported languages will be verified.

4.3.2 Election Media Creation – Vanguard Deploy

This area focuses on the creation and handling of media for the purposes of installing election data onto voting devices, as well as the creation of physical ballot layouts and creation of all media used to hold/transfer election data.

4.3.3 Pre-voting Aspects – Vanguard (Vault, Flex, Adapt, Boost, Capture)

Pre-voting aspects include pre-election preparatory, diagnostic, and election verification functions of a voting system. The focus will include device preparation, all required pre-voting tasks, and verification of manufacturer recommended pre-voting tasks.

4.3.4 Voting Aspects – Polling Place – Vanguard (Vault, Flex, Adapt, Boost)

Polling place aspects include all required and additional supported voting functions, including HAVA compliant requirements. This area will focus on all aspects of election functions and capabilities at the polling place, from opening of the polls through closing the polls and generating applicable reports.

4.3.5 Voting Aspects – Central Count – Vanguard Capture

The focus of the central count functions is primarily the usage of a COTS high speed scanner to scan large quantities of absentee ballots and passing each image to **Hart InterCivic Verity Vanguard 1.0** for interpretation of the voter's markings on the ballot.



4.3.6 Post Voting – Vanguard Results

This area will focus on all required election post-voting functions. This includes any additional supported election functions performed after closing the polls, device auditing and reporting aspects of the voting system.

4.3.7 Error Messaging and Recovery – Vanguard (All Components)

This area will focus on the system’s ability to generate appropriate error messaging within each system component and the system’s ability to recover from error conditions in order to proceed with all election functions.

4.3.8 Auditing – Vanguard (All Components)

This area will focus on device and system level auditing capabilities and will verify at a minimum the required audit functionality. This includes audit trail capability throughout the lifecycle of the voting system and audit log content requirements.

4.3.9 Security – Vanguard (All Components)

Overall system and device level logical and physical security aspects will be tested. Physical security will focus on the areas of integrity (ballot box doors, locks and seals) and detection (compromised ballot box doors, locks or seals). Logical security will focus on the areas of access controls, accountability, confidentiality, and integrity. These logical security areas will be applied to the OS, database, network (including verification that the voting system is not capable of establishing wireless connections) and application entities used by the EMS, BMDs and scanners employed within the voting system under test.

4.4 Test Case (Suite) Design

This section will detail the test suites to be utilized to verify **Verity Vanguard 1.0** to VVSG 2.0. Mapping of requirements to test cases/suites can be found in “Attachment C - Verity Vanguard 1.0 Test Case Matrix”.

Test cases define inputs, steps taken and expected results. Accept/reject criteria are based on requirements of the VVSG 2.0 and the system specification documents provided in the TDP.

4.4.1 Software and Hardware Qualitative Examination Design

SLI Compliance will review any reports submitted by the manufacturer of previous testing conducted on the equipment contained in the **Hart InterCivic Verity Vanguard 1.0** voting system. The results will be compared against the hardware related guidelines of the EAC VVSG 2.0 to identify any additional testing required. In addition, SLI Compliance will create the following test suites to focus on accessibility and usability of the voting system:

- **Accessibility** test suite – Accessibility requirements for a voting system generally include both objectively measurable and other observable



requirements. In combination, the two types of requirements verify that the voting system components are accessible to as many voters as possible, including those who have a category of challenge that creates a need for assistance of some type. The voting systems should be self-contained such that the individual voter is able to cast their vote without assistance from another party. Accessibility calls for the voting system to take into account vision, varying degrees of vision, dexterity, mobility, aural issues, and speech and language proficiency.

- **Usability** test suite – Usability is defined as a measure of the effectiveness, efficiency, and satisfaction achieved by a specified set of users with a given product in the performance of specified tasks. In the context of voting, the primary user is the voter, the product is the voting system, and the task is the correct recording of the voter’s ballot selections. Testing is conducted to ensure voters are able to negotiate the process effectively, efficiently, and comfortably.

4.4.2 Hardware Test Case Design

Hardware environmental testing is performed to verify conformance to the EAC VVSG v2.0. Testing will be accomplished through a combination of testing performed by SLI Compliance and testing performed by qualified subcontractor labs. Please see “Section 1.4.1.4 – Third Party Hardware Testing”.

Hardware test suite - Third party testing, with SLI Compliance oversight, will be conducted on the following:

Hardware Test (Requirement)	Applicable Component				
	Vault	Flex	Adapt	Boost	Capture
Radiated Emissions, 30 MHz - 1 GHz & 1 GHz - 15 GHz. FCC Part 15. Class B.	Yes	Yes	Yes	Yes	No
Conducted Emissions, 150 kHz - 30 MHz FCC Part 15. Class B. 120 VAC / 60 Hz	Yes	Yes	Yes	Yes	No
Electrostatic Discharge (2.7-K)	Yes	Yes	Yes	Yes	No
Radiated RF Immunity (Electromagnetic Susceptibility) (2.7-G)	Yes	Yes	Yes	Yes	No
Electrical Fast Transient /Burst (2.7-I)	Yes	Yes	Yes	Yes	No
Surge Immunity (Lightning Surge) (2.7-I)	Yes	Yes	Yes	Yes	No
Conducted RF Immunity (2.7-J)	Yes	Yes	Yes	Yes	No
Voltage Dips and Interruptions (2.7-I)	Yes	Yes	Yes	Yes	No
Bench Handling (2.7-D)	Yes	Yes	Yes	Yes	No
Continuous Operation – Varied Environmental Conditions (2.7-C)	Yes	Yes	Yes	Yes	Yes
High Temperature (2.7-F)	Yes	Yes	Yes	Yes	No
Low Temperature (2.7-F)	Yes	Yes	Yes	Yes	No



Additional testing, performed by SLI, includes maintainability testing, hearing devices and assessment of reliability.

4.4.3 Software Module Test Case Design and Data

Source Code Review test suite – Incorporating the manufacturer’s software specifications as well as all pertinent VVSG 2.0 source code review requirements, SLI Compliance will validate that all software/firmware components of the system adhere to expected flow control parameters and specifications for data input and output.

4.4.4 Software Functional Test Case Design and Data

SLI Compliance will prepare functional test modules using the operator/user procedures contained within the **Verity Vanguard 1.0** TDP. Functionality of the voting system is exercised to verify that each functional component performs as expected.

4.4.4.1 Component-level Test Suite Design

Component-level test suites exercise the specific functions of each component of a voting system. Testing will focus on the functionality of each component within the **Verity Vanguard 1.0** voting system.

Each of the following components will be subject to focused testing in the identified test suites to verify that the functionality presented in the component meets all applicable VVSG 2.0 requirements, as presented in “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

Verity Vanguard WorkSpace (Manage, Users, Settings, Libraries, Test Decks, Rank Choice) test suite – The **Verity Vanguard WorkSpace** component will be given focused testing in order to verify that the Functionality presented in the component, meets all applicable VVSG 2.0 requirements, as presented in “Attachment C – Verity Vanguard 1.0 Test Case Matrix”.

Verity Vanguard Define and Deploy (Pre-Election EMS) test suite – The **Verity Vanguard Define and Deploy** component will be given focused testing in order to verify that the Functionality presented in the component, meets all applicable VVSG 2.0 requirements, as presented in “Attachment C – Verity Vanguard 1.0 Test Case Matrix”.

Verity Vanguard Flex (BMD) test suite – The **Verity Vanguard Flex** component will be given focused testing in order to verify that the Functionality presented in the component, meets all applicable VVSG 2.0 requirements, as presented in “Attachment C – Verity Vanguard 1.0 Test Case Matrix”.



Verity Vanguard Adapt (all-in-one BMD) test suite – The **Verity Vanguard Adapt** component will be given focused testing in order to verify that the Functionality presented in the component, meets all applicable VVSG 2.0 requirements, as presented in “Attachment C –Verity Vanguard 1.0 Test Case Matrix”.

Verity Vanguard Boost (Ballot Issuance) test suite – The **Verity Vanguard Boost** component will be given focused testing in order to verify that the Functionality presented in the component, meets all applicable VVSG 2.0 requirements, as presented in “Attachment C –Verity Vanguard 1.0 Test Case Matrix”.

Verity Vanguard Vault (Precinct Scanner) test suite – The **Verity Vanguard Vault** component will be given focused testing in order to verify that the Functionality presented in the component, meets all applicable VVSG 2.0 requirements, as presented in “Attachment C –Verity Vanguard 1.0 Test Case Matrix”.

Verity Vanguard Capture (Central Scanning) test suite – The **Verity Vanguard Capture** component will be given focused testing in order to verify that the Functionality presented in the component, meets all applicable VVSG 2.0 requirements, as presented in “Attachment C –Verity Vanguard 1.0 Test Case Matrix”.

Verity Vanguard Results (Post Election EMS) test suite – The **Verity Vanguard Results** component will be given focused testing in order to verify that the Functionality presented in the component, meets all applicable VVSG 2.0 requirements, as presented in “Attachment C –Verity Vanguard 1.0 Test Case Matrix”.

4.4.4.2 VVSG 2.0 Verification Test Suite Design

The test suites in this section address specific areas of VVSG requirements.

Ballots test suite – Examines both paper ballots and electronically displayed ballots. Paper ballot test cases review ballots for their use of contrast, color, text size, font, use of plain language, use of supported languages, ability to prevent split contests, and ability to support multipage ballots.

Electronic ballot testing establishes the ease of use by the common voter, including examination against screen requirements such as digital contrast, use of color, text size and scaling ability, font readability, use of plain language, and use of supported languages. In addition, some aspects of device functionality applicable to electronic



ballots include the ability to prevent split contests, scroll, and establish a touch area for navigation and selection. See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

Interoperability test suite – Deals with the concept of interoperability, as defined by VVSG 2.0. Interoperability has two main areas of focus: common data formats, and common hardware interfaces/COTS products.

Common data formats deals with the ability of VVSG 2.0 certified voting systems to transfer data to different voting systems. To do this, VVSG 2.0 looks to ensure that devices are capable of importing and exporting data in common data formats, requires manufacturers to provide complete specification of how the format is implemented, and requires that encoded data uses publicly available, no-cost methods.

Common hardware interfaces/COTS products looks to extend that interchangeability aspect by enforcing the use of common methods (for example, a USB) for all hardware interfaces. Additionally, it looks at verifying that COTS devices continue to meet all relevant VVSG 2.0 requirements. See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

Software Setup and Validation test suite – Verifies that the voting system has the capability and written instructions for proper setup and verification of the components of the system, in preparation for an election.

All aspects of each system component should be verified to be in proper working order, from having the correct/expected software installed, to proper boot up and verification of all included components.

Any potential issues that may arise during installation, including files that do not meet the installation criteria, should also be addressed, such that the jurisdiction will understand what is occurring and how it should be handled. See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

System Identification and Installation test suite – Focuses on verification of the installation process for each component of the voting system, as well as obtaining and verifying the post-install signatures. See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

Supply Chain Risk Management test suite – Covers the requirement that a voting system’s documentation contains a supply chain risk management strategy, a list of critical components defined by criticality analysis, and hardware and software information for the critical components. See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

Pre-election Voting Devices test suite – Examines the basic aspects of loading the election definition and verifying that everything is properly loaded, running test ballots, and verifying that test ballots are cleared prior to opening of polls. Any calibrations that may be required for a device are examined as well. Equipment readiness and



ability to report is also included. See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

4.4.5 System-level Test Suite Design

Testing of the system involves exercising the specific functions of each component of a voting system as well as the entire voting system. Testing will focus on the functionality of the election management system, polling place devices, and devices required for communications and data loading and will then focus on functionality of the integrated voting system.

System level test suites will include the following:

Election Validations: Election test suites are created to replicate each type of election that can be implemented by the jurisdiction. Within the election types, pertinent voting variations that are applicable to that type of election will be validated and verified. Each suite will have a particular focus in order to test the voting system’s implementation of a given requirement or set of requirements. Each test suite below is explained in terms of how it differs from a general high-level test, such as the one used in the Test Readiness Review.

GenVariation1 test suite: Definition is created, with a focus on validating N of M voting, partisan offices, non-partisan offices, ranked order voting, straight party voting, ballot rotations, ballot formatting, precincts and districts, languages, additional voting variations, applicable voting system extensions, and tally and reporting functionality.

GenVariation2 test suite: Additional definition is added, with a focus on validating recalls, cross party endorsement, cumulative voting, write-ins, languages, additional voting variations, applicable voting system extensions, HAVA concerns as well as considerations such as pre-vote capabilities.

OpenPrimary test suite: This suite creates an election definition to conform to an Open Primary election with a focus on validating presidential delegation nominations, blanket primary contests, as well as additional voting variations and applicable voting system extensions.

ClosedPrimary test suite: This suite creates an election definition to conform to a Closed Primary election with a focus on validating presidential delegation nominations as well as additional voting variations and applicable voting system extensions.

Error Message/Recovery test suite: The test suite will focus on error messaging and recovery in key areas of the system identified from researching previous testing and voting system documentation to help identify potential failure points. Voting systems can be subject to various conditions, and when the system exceeds limitations, errors are typically found. Testing of error messaging will focus on the appropriate error messages being generated in response to a specific error and content of the message



as well as error recovery. See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

System Audit test suite: Election audit trails provide the supporting documentation for verifying the accuracy of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation. This testing focuses on validating the audit capability throughout the entire voting system, including availability, generation, integrity, and accuracy of the system’s audit content capability to ensure it meets the applicable requirements of VVSG 2.0. See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

Accuracy test suite: This testing focuses on the ability of the 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. Required accuracy is defined in terms of an error rate that for testing purposes represents the maximum number of errors allowed while processing a specified volume of data.

Accuracy testing is conducted at both the device level and the system level.

At the system level, all test suites will be exercised and reviewed to validate that the accumulation, tallying and reporting mechanisms at the system level are able to accurately perform their functions. Accuracy for the system must have zero errors for 10 million ballot marking positions exercised during the course of the test campaign.

At the device level, each device is subjected to scrutiny to verify that the requirements for accuracy are met.

For the device level accuracy test, each tabulator will be used to scan a minimum of 1.55 million ballot position marks.

See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

Volume test suite: Tests a system’s response when subjected to large volumes of data, “more than the expected”, as called out in the standards. Volume testing is typically considered a type of non-functional testing. However, as a voting system’s primary function is to accumulate, tally, and pass a volume of data (votes), the VSTL approaches volume testing as a functional test. Experience has shown that large amounts of data can slow a system, or even cause failures and loss of data due to architectural limitations. Utilizing the VSTL’s experience with voting systems, the testing will focus on not only passing large amounts of data but how the system operates and handles the data in key areas of functionality within the voting system. See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

Stress test suite: Tests a system’s “response to transient overload conditions.” Experience has shown that when passing a dataset through a system that eclipses the system architectural limitations, failures can occur and result in the loss of critical data. Utilizing the VSTL’s experience with voting systems, the testing will focus on



the system's ability to operate after the limitations have been exceeded and if failures occur, how the data is maintained or recovered in key areas of functionality within the voting system. See "Attachment C – Verity Vanguard 1.0 Test Case Matrix."

4.5 Security Functions

4.5.1 Security Test

The Security Test Suites are SLI Compliance's tests for verifying that a voting system will correspond to security requirements in the EAC VVSG v 2.0. They incorporate systems security provisions, unauthorized access, deletion or modification of data, audit trail data, and modification or elimination of security mechanisms. The vendor documentation will be reviewed to ensure sufficient detail is present to operate the voting system in a secured manner. Where the vendor statements assert the voting system is secured via mechanisms and seals, procedures will test the presence and effectiveness of such controls.

In its security testing, SLI Compliance identifies the specific threats that are tested for and the associated risk if a flaw or exception is identified in a voting system. The tests used by SLI Compliance are designed to ensure that the voting system meets or exceeds the requirements in the VVSG, including verification that the voting system is not capable of establishing wireless connections. For any instance where an anomaly or possible security flaw is identified, the potential risk is reported and evaluated.

Security testing includes testing each individual component of the system and the system as a whole. As such, each type of precinct optical scanner, BMD, modem, central count scanner, EMS, tally and reporting application, etc. will be subjected to review, as will the system as a whole and its interactions between components.

Access Control test suite: The voting system must be capable of maintaining authorization information and authentication capabilities for all systems, services, and users that interact with the voting system. All devices included in the test campaign receive access control security testing. Device usernames and passwords will be tested for proper authentication capabilities and to verify that password requirements are sufficient. In addition, multi-factor authentication will be tested to verify the bolstering of user account security such that leaked credentials alone will not expose the voting system to account misuse. Each user account will be tested for permissions and role assignments based on documented roles and proper role-based access control (RBAC) implementations. Minimum permission and access rules will be tested to ensure the voting system provides each user with only the permissions relevant to the role's documented purpose. Voting system components are tested through interaction with devices and visual inspection of authentication during user login and user activity. See "Attachment C – Verity Vanguard 1.0 Test Case Matrix."

Data Protection test suite: Ensuring the end-to-end integrity of election system data guarantees the authenticity of the data. System and software cryptographic implementations are tested for computational security and efficacy of encrypting data.



Cryptographic modules are verified against the Cryptographic Module Validation Program (CMVP) and evaluated concerning algorithm strength in bits and key lengths. In addition, configuration files are tested for accessibility restrictions. Testing is conducted through documentation review and simulation of documented events to identify key components. Necessary cryptographic artifacts are exfiltrated and analyzed externally to verify algorithm strengths and key lengths, while configuration files are reviewed locally on voting system components to verify alignment with documented configuration procedures. See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

Physical Security test suite: The voting system is required to have physical security controls implemented to prevent and deter unauthorized access and properly produce alerts if the system encounters errors. Connectivity or lack thereof must be logged for all scanners, BMDs, and other voting system components during activated voting stages. Connections to device ports must also be logged and configured to minimally allow connectivity only to other voting system components for necessary documented procedures. Any physical housing for voting system storage or transportation must secure the system and produce evidence if tampering is experienced. Any physical locks on the voting system are required to at minimum support different keying schemes including a key owner-unique scheme. Any security controls dependent on power must maintain their state upon loss of power and require a backup power supply. Such requirements are tested through physical inspection and interaction with all relevant voting system components. See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

System Integrity test suite: System integrity tests the overall security of the voting system with respect to environmental factors. This includes consideration of supply chain attacks, attack surface analyses and limitations, and software verification. Documented risk assessments are evaluated for identified risks and associated acceptances or mitigations as well as procedural and operational security measures in place. Physical components of the voting system are tested to ensure that connections to logical components are properly disabled or limited to documented connections with other voting system components. In addition, software checks are completed to ensure all resident programs are verified with allow lists and that any errors or disallowed software trigger a display of obvious and accurate indications of the error. *The system is examined to verify that no wireless capability is available.* See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

4.6 TDP Evaluation

TDP Evaluation test suite: Examines the provided Technical Data Package, which includes a system overview and documents the system’s functionality, hardware, software, security, test and verification specifications, operations procedures, maintenance procedures, and personnel deployment and training requirements, as well as public documentation, for completeness and accuracy in describing the system. Jurisdiction/voter facing documentation in particular needs to be complete,



such that a jurisdiction/voter is able to successfully implement/use the voting system. As such, all system features must be included and implementation/usage be accurately depicted for each of the required hardware, software and firmware components of the **Hart InterCivic Verity Vanguard 1.0** voting system. See “Attachment C – Verity Vanguard 1.0 Test Case Matrix.”

For a complete list of all items included in the TDP, please refer to “Attachment E – Technical Data Package Listing.”

4.7 Source Code Review

The test campaign for the **Hart InterCivic Verity Vanguard 1.0** voting system includes software and firmware that have been created as proprietary to **Hart**, as well as review of any commercial off the shelf products. SLI Compliance will conduct a source code review of all proprietary source code and modified COTS products delivered in the voting system TDP for compliance to the EAC VVSG v 2.0 software code requirements.

The coding languages involved in Verity Vanguard 1.0’s applications include:

- C /C++
- C#

Source code review tools used by SLI Compliance include:

- **Cloc Line Counter**: A commercial application used to determine the counts of executable and comment lines;
- **Module Finder**: An SLI Compliance proprietary application used to parse module names from C/C++ and VB code and populate the identified module names into the review documents;
- **ExamDiff Pro**: A commercial application used to compare revised code to previously reviewed code; and
- **Checkmarx**: A commercial SCA application used to review the source code for vulnerabilities and data flow issues.

Any subsequent re-reviews of source code will be the result of fixes to discrepancies identified in the certification testing activities.

COTS operating systems and software used in the voting system will be verified as authentic and unmodified.

4.8 Trusted Build

The Trusted Build will be conducted prior to the official testing and will be completed on site at SLI Compliance’s facility or a secure lab at the vendor’s facility approved by SLI Compliance. SLI Compliance will use its approved standard lab procedure that details the processes for controlling, managing, and conducting the Trusted Build. This process includes the following:



- **Preparation for the Trusted Build** – Obtaining and reviewing Hart’s procedure for constructing the build platform, verifying the target build platform, and acquiring and verifying the necessary materials.
- **Execution of the Trusted Build** – SLI Compliance will perform the Trusted Build using the step-by-step build procedure provided by Hart to create a pristine build environment. SLI Compliance records and ascertains the following items throughout the build process:
 - ✧ Build environment and file hashes at various key points.
 - ✧ Build environment hardware characteristics.
 - ✧ Build results from code compilation and file hashes.
 - ✧ Final software install files and file hashes.
 - ✧ Build virtual machine files.
- **Deliverables to Testing** – Upon completion of the Trusted Build, certain items are sent to the SLI Compliance test group. The final result will be a media containing the following:
 - ✧ Final software install files.
 - ✧ Hash values to validate install files.
- **Final Record Keeping and Archiving Procedures** – At the conclusion of the Trusted Build process, SLI Compliance completes all final record keeping and archiving procedures at SLI Compliance’s facility. This record keeping includes any unique identifiers, results of the build with version numbers and dates and descriptions of all hashes and images in the repository.

4.9 Standard VSTL Test Methods and Uncertainty of Test Data Measurement

This test campaign utilizes Standard VSTL test methods and nominal type test data only.

4.10 EAC Interpretations

The test engagement described in this Test Plan utilizes only standard VSTL test methods that conform to the EAC Testing and Certification Program Manual and the identified voting system standard.

This Test Plan and the execution of tests for the voting system identified in this plan do include all EAC interpretations (RFI) and notices of clarification (NOC) that have been published as of the date of this document (Please see “Revision History” on page “ii”).



5. TEST DATA

Test data for the **Hart InterCivic Verity Vanguard 1.0** voting system has been compiled such that all functionality declared will be tested to determine conformance to the standards.

5.1 Data Recording

SLI Compliance has evaluated the system functionality, as described by manufacturer technical documentation, as well as requirements as listed in the EAC VVSG v2.0, and made determinations as to expected results of all data inputs into the **Hart InterCivic Verity Vanguard 1.0** voting system. This includes:

- Election type
- Precincts of all types
- Districts
- Offices
- Contests
- Candidates
- Parties
- Issues/Referendums
- Voting variations employed
- Votes cast for each candidate/issue/referendum
- Devices used
- Vote consolidation data from one device/level to the next

This data is incorporated into the appropriate test suite, populating test modules with expected data for the function being tested.

Testing information is recorded in the test suites and test notebooks according to SLI Compliance's relevant standard lab procedures.

5.2 Test Data Criteria

SLI Compliance has evaluated the system functionality as described by manufacturer technical documentation, as well as requirements as listed in the EAC VVSG v 2.0, and made determinations as to expected output of all data inputs into the **Hart InterCivic Verity Vanguard 1.0** voting system. A data matrix has been recorded into one master data record that couples data inputs to their expected output, as determined above. The system's execution shall be measured against the expected results.



5.3 Test Data Reduction

SLI Compliance processes the test data by manually recording input data into each pertinent module within the test suites as well as the exact output that is generated, e.g., the vote counts when the data is consolidated.

6. TEST PROCEDURE AND CONDITIONS

This section describes the test conditions and procedures for execution of test suites. If a particular sequence is mandatory for the execution of suites, a rationale will be given. Additionally, this section is used to describe procedures for setting up equipment to be used in the test suite execution.

6.1 Facility Requirements

Testing will be performed on site at SLI Compliance in Colorado.

Multiple secure labs are available with appropriate power supply and space to accommodate the various configurations defined within this test plan.

Temperature/humidity gauges will be employed in order to confirm whether the appropriate conditions exist during testing.

Unless otherwise specified herein, all remaining tests, including system level functional testing, shall be performed at standard ambient conditions:

- Temperature: 25°C ± 10°C (77°F ± 18°F)
- Relative Humidity: 20 to 90%
- Atmospheric Pressure: Local Site Pressure

All TDP and test documentation is stored on site at SLI Compliance's facility in a project directory on SLI Compliance's secure Voting server.

Environmental hardware testing for hardware components of the **Hart InterCivic Verity Vanguard 1.0** voting system will be performed at NVLAP or A2LA accredited testing laboratories, as listed in section "1.4.1.4 Third Party Hardware Testing". These labs have been audited by SLI Compliance to NVLAP Handbook 150-22 requirements.

6.2 Test Setup

All components of the **Verity Vanguard 1.0** voting system will be set up as documented in the TDP.

Successful completion of operational status checks will indicate that the system is ready for test execution.



6.3 Test Sequence

There is no required sequence for performing voting system testing, other than the execution of the General and Primary Elections. Each test suite is designed to be self-contained, other than usage of one of the General or Primary election definitions. Audit testing is done on an ongoing basis, examining the audit logs produced in each of the other test suites.

7. TEST OPERATIONS PROCEDURES

An inventory has been performed to verify the voting equipment received contains hardware and software elements as defined in the TDP prior to commencement of testing.

Throughout the testing effort, test suites and modules will be marked as follows:

- **Accept** – Test is accepted as successful.
- **Reject** – Test is rejected as unsuccessful.
- **NT** – Not Testable is used for test modules that cannot be completed. For example, if failure of one test modules failure precludes attempting subsequent test modules, the latter will be marked as NT.

Test results **Reject and NT** will include comments by the test engineer explaining the reason for the result.

Issues encountered during review and testing will be documented on the Discrepancy Report. Test findings showing that an aspect of the voting system does not conform to the requirements of the identified test standard will be marked as **Documentation Discrepancies** or **Functional Discrepancies**.

Issues that are encountered during testing or documentation review but are not addressed by the applicable standard will be added to the Discrepancy Report and noted as **Informational**. The vendor has the option whether to address Informational issues. All responses provided by the vendor are noted in the Discrepancy Report attachment to the Voting System Test Report.



8. APPROVAL SIGNATURES

WHEREOF as of the day and year set forth below SLI Compliance VSTL authorized signatory has reviewed and approved Voting System Test Plan “*HIN-23003-TP-01*” for **Hart InterCivic Verify Vanguard 1.0**.

Signature: *Traci Mapps*

Name: Traci Mapps

Title: Vice President, SLI Compliance

Date: June 13, 2024

End of Verity Vanguard 1.0 Voting System Test Plan

Statement of Independence

Voting Systems Compliance Testing Statement of Independence

The SLI Compliance® Voting Systems Compliance Testing Statement of Independence reads as follows:

The management and staff of SLI Compliance, along with SLI Compliance's testing subcontractors and their employees, shall maintain an independent decisional relationship between themselves and SLI Compliance's clients, affiliates, or other organizations so that the Company's capacity to render test reports objectively and without bias is not adversely affected.

SLI Compliance, along with SLI Compliance's testing subcontractors and their employees, shall maintain independence from Voting System Manufacturing clients whose systems are under VSTL test or are scheduled for a VSTL voting system test campaign. Specifically, employees shall not have a direct beneficial interest in a voting system product.



4720 Independence Street, Wheat Ridge, CO 80033
844/754-8683 (toll free) 303/422-1566
info@slicompliance.com
www.slicompliance.com
✈ [@slicompliance](https://twitter.com/slicompliance)