

PRO V&V



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

EAC VVSG 2.0 Certification Test Plan Liberty Vote USA, Inc. (LVU) Frontier 1.0 Voting System

Document Number: TP-01-01-LVU-2025-01

EAC Project Number: LVU-Frontier1.0

Document Version: 05

Date: 09/11/2026

U.S. Election Assistance Commission

VSTL

EAC Lab Code 1501



TESTING
NVLAP LAB CODE 200978-0

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

SIGNATURES

Approved by:

Michael Walker
Michael L. Walker, VSTL Program Manager

09/11/2026
Date

Approved by:

Wendy Owens
Wendy Owens, VSTL Program Director

09/11/2026
Date

Approved by:

Stacey Glover
Stacey Glover, QA Manager

09/11/2026
Date

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

REVISIONS

Revision	Description	Date
00	Initial Release	03/19/2026
01	Post-EAC Comments and grammatical edits	05/26/2026
02	Revised COTS Software Components	07/27/2026
03	Post-EAC Comments	08/18/2026
04	Post-EAC Comments	09/01/2026
05	Changed Hardware Test Labs	09/11/2026

TABLE OF CONTENTS

SECTION I: INTRODUCTION	1
Section I.1 References	1
Section I.2 Terms and Abbreviations	2
Section I.3 Target of Evaluation Description.....	3
Section I.3.1 System Overview	3
Section I.3.1.1 Block Diagram	5
Section I.3.1.2 System Limits	6
Section I.3.1.3 Supported Languages	9
Section I.3.1.4 Supported Functionality.....	10
Section I.4 Scope of Testing	11
Section I.5 Testing Responsibilities	16
Section I.6 Third Party Tests.....	17
SECTION II: PRE-CERTIFICATION TESTING AND ISSUES.....	17
Section II.1 Evaluation of Prior VSTL Testing.....	17
Section II.2 Evaluation of Prior Non-VSTL Testing.....	18
Section II.3 Known Field Issues.....	18
SECTION III: MATERIALS REQUIRED FOR TESTING.....	18
Section III.1 Software	18
Section III.2 Hardware/Equipment.....	22
Section III.3 Materials/Consumables.....	29
Section III.4 Proprietary Data	29
SECTION IV: TEST SPECIFICATIONS.....	30
Section IV.1 Requirements	30
Section IV.2 Test Case Development and Design.....	30
Section IV.2.1 Hardware Environmental Test Case Design	31
Section IV.2.2 Software Module Test Case Design and Data.....	31
Section IV.2.3 Software Functional Test Case Design and Data	31
Section IV.2.4 System-Level Test Case Design.....	32
Section IV.3 Test Procedure Development and Validation	32
SECTION V: TEST PROCEDURES	32

Section V.1 Physical Configuration Audit (PCA).....	32
Section V.2 Technical Data Package (TDP) Review.....	33
Section V.3 Source Code Review.....	40
Section V.4 Functional Configuration Audit (FCA).....	40
Section V.5 Security Review	41
Section V.6 Vulnerability Testing	44
Section V.7 Cryptographic Testing	45
Section V.8 Usability Review	45
Section V.9 Accessibility Review	45
Section V.10 System Integration Testing.....	46
Section V.11 Accuracy Test.....	47
Section V.12 Volume Test.....	48
Section V.13 Interoperability	49
Section V.14 Hardware Testing	49
Section V.14.1 Electrical Hardware Testing.....	51
Section V.14.2 Operational Hardware Testing.....	53
Section V.14.3 Non-Operational Hardware Testing.....	53
Section V.15 Product Safety Review.....	55
SECTION VI: TEST DATA	56
Section VI.1 Test Data Recording	56
Section VI.2 Test Data Criteria	56
Section VI.3 Test Data Reduction	57
SECTION VII: TEST CONDITIONS	57
Section VII.1 Facility Requirements	57
Section VII.2 Test Set-Up.....	57
Section VII.3 Test Sequence	58
SECTION VIII: TEST OPERATIONS PROCEDURES.....	58
APPENDIX A: PROJECT SCHEDULE	59

SECTION I: INTRODUCTION

The purpose of this Certification Test Plan is to document the procedures and test approach Pro V&V, Inc. will follow to perform certification testing during a new system test campaign on the Liberty Vote USA, Inc. (LVU) Frontier 1.0 Voting System (hereinafter referred to as ‘LVU Frontier 1.0’) against the requirements set forth for voting systems in the U.S. Election Assistance Commission (EAC) Voluntary Voting System Guidelines (VVSG) Version 2.0. Certification testing of the LVU Frontier 1.0 will be performed to ensure the applicable requirements of VVSG 2.0 and the EAC Testing and Certification Program Manual, Version 3.0 are met. Additionally, all EAC Request for Interpretations (RFI) and Notices of Clarification (NOC) relevant to the system under test will be incorporated in the test campaign.

Prior to submitting the voting system for testing, LVU submitted the application package to the EAC for certification of the LVU Frontier 1.0. The application was accepted by the EAC, and the project assigned the unique Project Number of LVU-Frontier1.0.

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

SECTION I.1 REFERENCES

- Election Assistance Commission (EAC) Voluntary Voting System Guidelines (VVSG) Version 2.0, “Principles and Guidelines” and “Requirements”
- Voluntary Voting System Guidelines Version 2.0 Test Assertions, Version 1.4
- Election Assistance Commission (EAC) Voting System Testing and Certification Program Manual, Version 3.0
- Election Assistance Commission (EAC) Voting System Test Laboratory Program Manual, Version 3.1
- National Voluntary Laboratory Accreditation Program NIST Handbook 150, 2020 Edition, “NVLAP Procedures and General Requirements (NIST Handbook 150)”
- National Voluntary Laboratory Accreditation Program NIST Handbook 150-22, 2021 Edition, “Voting System Testing (NIST Handbook 150-22-2021)”
- United States 107th Congress Help America Vote Act (HAVA) of 2002 (Public Law 107-252), dated October 2002
- Pro V&V, Inc. Quality Assurance Manual
- EAC Requests for Interpretation (RFI) and Notices of Clarification (NOC) (listed on www.eac.gov)
- Frontier 1.0 EAC Application Approval Letter, dated 02/19/2026

- LVU Frontier 1.0 Technical Data Package (*A listing of the LVU Frontier 1.0 documents submitted for this test campaign is listed Table V-1 of this Test Plan*)

SECTION 1.2 TERMS AND ABBREVIATIONS

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

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

SECTION I.3 TARGET OF EVALUATION DESCRIPTION

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

The LVU Frontier 1.0 Voting System is a paper-based optical scan voting system consisting of the following major components: Frontier Election Management System (EMS), Frontier Central, Frontier All-in-One, Frontier Precinct, and Frontier Ballot Marking Device (BMD).

SECTION I.3.1 SYSTEM OVERVIEW

Frontier Election Management System (EMS)

The Frontier Election Management System (EMS) represents a set of N-Tier software applications for pre-voting and post-voting election project activities that are applicable to jurisdictions of various sizes and geo-political complexities. The Frontier EMS set of applications are responsible for all pre-voting and post-voting groups of activities in the process of defining and managing elections. They consist of components running either as a front-end/client application or as a back-end/server application, as described below:

- Frontier Ballot Designer client application – integrates election definition functionality and represents a main pre-voting phase end-user application.
- Frontier Tally and Reporting client application – integrates election results acquisition, validation, tabulation, reporting and publishing capabilities and represents a main post-voting phase end-user application.
- Frontier Audio Studio client application – represents an end-user helper application used to record audio files for a given election project. As such, it is utilized during the pre-voting phase of the election cycle.
- Frontier Logger – represents a stand-alone application that runs on client or server machines and is used to gather diagnostics for troubleshooting.
- Frontier Data Importer – represents an end-user application to export election data from an election project and import election data into an election project.
- Frontier EMS Application Server (APPS) application – represents a server-side application responsible for executing long running processes, such as rendering ballots, generating audio files and election files.
- Frontier EMS Database Server application – represents a server-side RDBMS repository of the election project database which holds all the election project data, such as districts, precincts, candidates, contests, ballot layouts, tabulators, vote totals, and poll status.
- Frontier EMS Network Attached Storage (NAS) file repository – represents a server-side file repository for election project file-based artifacts, such as ballots, audio files, reports, log files, and election files.
- Frontier EMS Server Applications and Other Services

- Data Center Manager server application – represents a system level configuration application used in EMS back-end data center configuration.
- File System Service client application – a stand-alone service that runs on client machines, enabling access to low level operating system API for partitioning CF cards, reading raw partition on CF card, etc.
- Ballot Review Services – provides ballot information such as contest, candidates and their coordinates from the EMS to the Ballot Review client application
- Frontier Smart Card Helper Service – service that is installed on the Ballot Designer and Ballot Activation workstations to provide the required data format for programming technician, poll worker and voter smart cards for the Ballot Marking Devices.
- Frontier Ballot Review client application – optional application that reviews voter intent on a ballot-by-ballot basis from the central or precinct count devices utilized during either the absentee voting or post-voting activity phases.
- Frontier Ballot Activation – application installed on a workstation at the polling place that allows poll workers to program smart cards, which are used by voters to activate voting sessions on the Ballot Marking Device terminal.

The Frontier EMS platform is available in two deployable hardware configurations: Express and Standard.

- Frontier EMS Express hardware configuration - all EMS software components are installed on a single physical PC with the option to use the EMS client components on one or more physical PCs that are connected to the server through a Local Area Network (LAN).
- Frontier EMS Standard hardware configuration - the EMS server components are installed on a single physical server, in addition to the LAN switch devices, while the EMS client components are installed on one or more physical PCs or laptops. All system components are interconnected in a client-server local LAN environment.

Frontier Central

The Frontier Central system consists of a central, high-speed, optical scan ballot counter (tabulator) called the Frontier Central Ballot Counter and is used for processing absentee ballots (such as vote by mail). This ballot counter unit is based on COTS hardware coupled with custom made ballot processing application software. It is used for high-speed centralized scanning and counting of paper ballots.

Frontier All-in-One

The Frontier All-in-One system employs a precinct-level optical scan ballot counter (tabulator) in conjunction with an external ballot box. This tabulator is designed to mark and/or scan paper ballots, interpret voting marks, communicate these interpretations back to the voter (either visually through the integrated LCD display or audibly via integrated headphones), and upon the voter's acceptance, deposit the ballots into the secure ballot box. The unit also features an Audio Tactile Interface (ATI) which permits voters who cannot negotiate a paper ballot to generate a synchronously human and machine-readable ballot from elector-input vote selections.

Frontier Precinct

Frontier Precinct is a precinct-based optical scan ballot tabulator that is used in conjunction with compatible ballot storage boxes. The system is designed to scan marked paper ballots, interpret voter marks on the paper ballot, and safely store and tabulate each vote from each paper ballot

Frontier Ballot Marking Device (BMD)

The Frontier Ballot Marking Device (BMD) platform is a solution that is used for marking and printing uniform ballots. These ballots are later scanned and tabulated by the Frontier Central optical ballot counter and/or scanned, verified and cast on the Frontier Precinct. The Frontier BMD also supports enhanced accessibility voting through optional accessories connected to the Frontier BMD unit.

SECTION I.3.1.1 BLOCK DIAGRAM

The relationship between components and a high-level block diagram of the LVU Frontier 1.0 Voting System are depicted below in Figures I-1 and I-2, respectively.

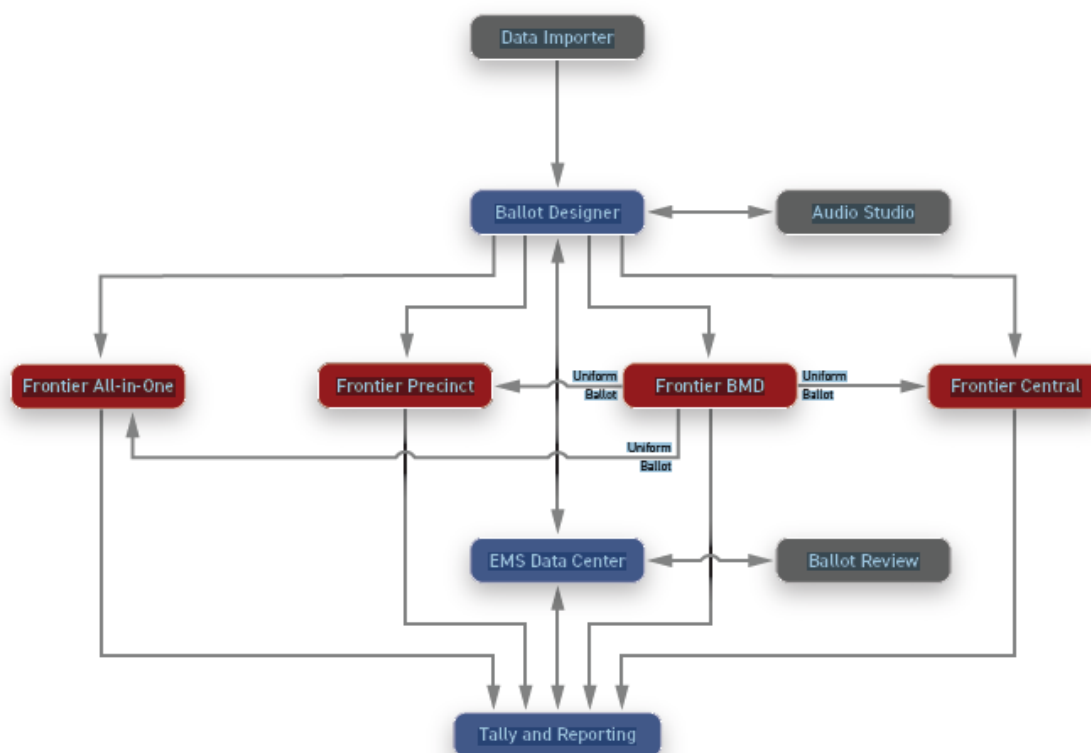


Figure I-1 Relationship between LVU Frontier 1.0 Components

Frontier - System High-Level Block Diagram

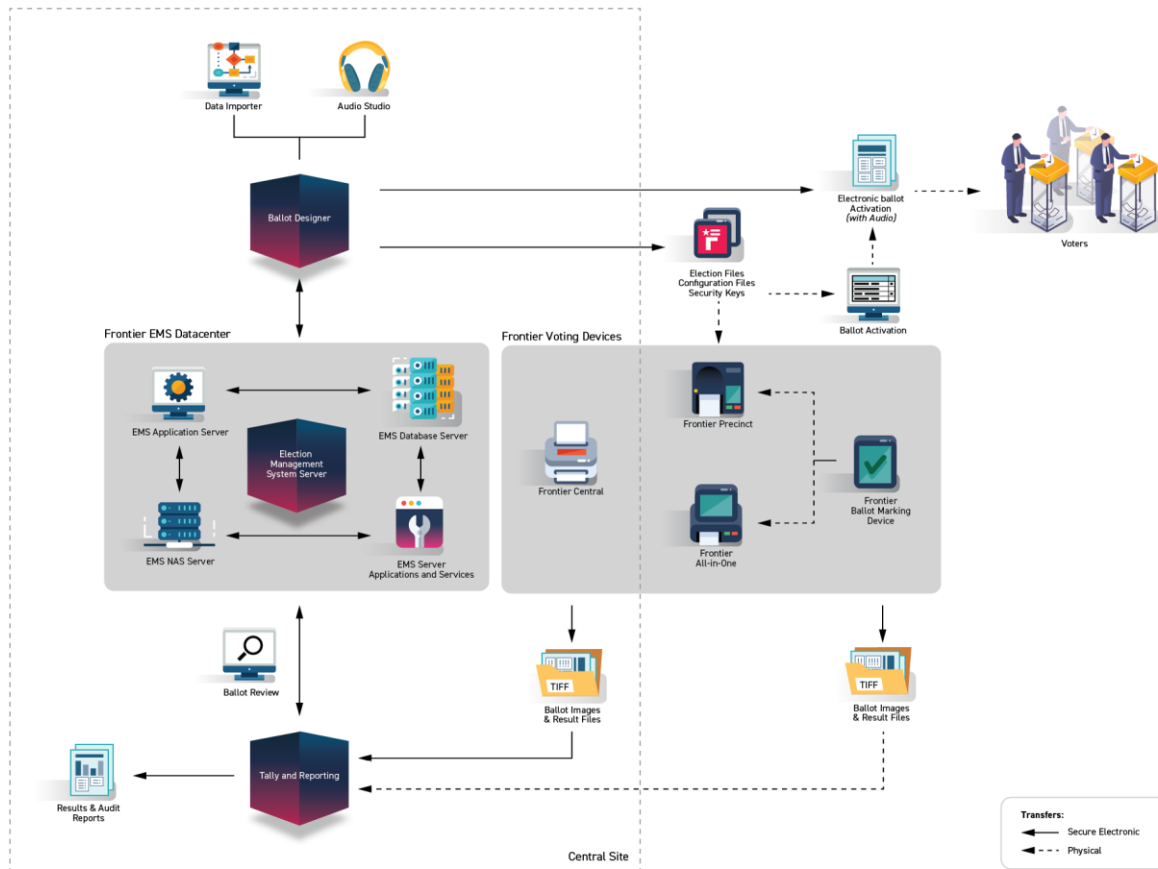


Figure I-2 High-level Block Diagram of the LVU Frontier 1.0 Voting System

SECTION I.3.1.2 SYSTEM LIMITS

LVU has defined the following performance characteristic limits and capacities for the LVU Frontier 1.0 Voting System components:

Table I-1 Frontier EMS System Capacity

Frontier EMS System Capacity			
<i>Per the Frontier 1.0 System Overview, the Frontier EMS platform does not impose any restrictions on the following system capacity aspects related to the problem domain: Number of Ballot Designer client applications simultaneously used within the system, Number of Tally and Reporting client applications simultaneously used within the system, Number of election projects supported by a single instance of the system, Size and complexity of the election project structure (number of political subdivisions, number of contests and candidates, number of polling locations, Frontier tabulators, etc.)</i> <i>System limitations regarding ballot orientation are:</i>			
Characteristic	Limiting Component	Limit	Comment
Ballot positions	Ballot	462**/292*	22 in. Ballot
Precincts in an election	EMS	1000; 250	Memory, Standard; Express
Contests in an election	EMS	1000; 250	Memory, Standard; Express
Candidates/Counters in an election	EMS	10000; 2500	Memory, Standard; Express
Candidates/Counters in a precinct	Ballot	462**/240*	22 in. Ballot
Candidates/Counters in a tabulator	Tabulators	10000; 2500	Memory, Standard; Express
Ballot Styles in an election	Tabulators	3000; 750	Memory, Standard; Express
Contests in a ballot style	Ballot Orientation and Type	153**/38*	22 in. Ballot (Landscape)
Candidates in a contest	Ballot	231**/240*	22 in. Ballot, Both EMS
Ballot styles in a precinct	Tabulators	5	Memory, Both EMS
Number of political parties	Tabulators	30	Memory, Both EMS
“Vote for” in a contest	Ballot	30**/24*	22 in. Ballot, Both EMS
Supported languages in an election	Tabulators	5	Memory, Both EMS
Number of write-ins	Ballot	462**/24*	22 in. Ballot, Both EMS
<i>Note: Per the Frontier 1.0 System Overview, all the above listed system capacity attributes are limited with regard to the number and size of the underlying computing and networking infrastructure: Frontier EMS hardware configuration deployed, Number of Gigabit Ethernet ports on the active network equipment, Number and size of the hard disk storage media on the EMS Database Server and NAS servers</i>			

*landscape

**portrait

Table I-2 Frontier All-in-One System Capacity

Per the Frontier 1.0 System Overview, the following is a list of recommended precinct system limitations:

- 2500 stored ballots per scanner unit
- 100 precincts per scanner unit
- 100 ballot styles per scanner unit
- 900-2000 voters per day depending on the ballot complexity)

Frontier All-in-One capacity can be measured by processing speed and memory card capacity. The ballot processing speed is defined by the ballot size (length). Images of all paper ballots are processed on the tabulator and saved on the memory card. Memory card size (available in 2 GB, 4 GB, 8 GB and 16 GB) is important in determining the ballot storage capacity.

Frontier All-in-One Ballot Image Capacity for Various Ballot Sizes and Memory Card Size					
Ballot Size	Approximate Ballot Image Size (KB)	Memory Card Size			
		2 GB	4 GB	8 GB	16 GB
Ballot Size (Single-Sided)					
8.5” x 11”	250	6000	14000	30000	62000
8.5” x 14”	277	5400	12600	27000	55800
8.5” x 17”	312	4800	11200	24000	49600
8.5” x 20”	334	4500	10500	22400	46400
8.5” x 22”	357	4200	9800	21000	43400
Ballot Size (Double-Sided)					
8.5” x 11”	357	4200	9800	21000	43400
8.5” x 14”	454	3300	7700	16500	34100
8.5” x 17”	499	3000	7000	15000	31100
8.5” x 20”	555	2700	6300	13500	27900
8.5” x 22”	624	2400	5600	12000	24800

Central Count System Capacity:

Depending on the scanner used, Frontier Central provides a scanning speed of up to 150 pages per minute.

Table I-3 Frontier Precinct Ballot Image Capacity

Per the Frontier 1.0 System Overview, the following is a list of recommended Frontier Precinct system limitations:

- 2500 stored ballots per scanner unit
- 100 EDs per scanner unit
- 100 ballot styles per scanner unit
- 900-2000 voters per day depending on the ballot complexity)

Frontier Precinct system capacity can be measured by processing speed and memory card capacity. The ballot processing speed is defined by the ballot size (length). Images of all paper ballots are processed on the tabulator and saved on the memory card. Memory card size (16 GB) determines the ballot storage capacity.

Frontier Precinct Ballot Image Capacity for Various Ballot Sizes		
Ballot Size	Approximate Ballot Image Size (KB)	Memory Card Size
		16 GB
Ballot Size (Single-Sided)		
8.5” x 11”	258	59900
8.5” x 14”	286	54200
8.5” x 17”	325	47700
8.5” x 20”	352	44000

Table I-3 Frontier Precinct Ballot Image Capacity (continued)

Ballot Size	Approximate Ballot Image Size (KB)	Memory Card Size
		16 GB
8.5" x 22"	382	40500
<i>Ballot Size (Double-Sided)</i>		
8.5" x 11"	382	40500
8.5" x 14"	476	32600
8.5" x 17"	517	30000
8.5" x 20"	564	27500
8.5" x 22"	633	24500

Frontier Ballot Marking Device (BMD) System Capacity:

The following is a list of recommended system limitations:

- 1000 EDs per unit
- 1000 ballot styles per unit
- 900-2000 voters per day depending on the ballot complexity
- Election file size should not exceed 10 GB
- Frontier BMD limits when using typical project parameters:
 - Not more than 18 vote-for positions, as dictated by space available on a 22" hand-marked ballot.
 - Max 216 choices per contest
 - Max 108 contests on Letter paper
 - Max 153 contests on Legal paper

SECTION I.3.1.3 SUPPORTED LANGUAGES

The LVU Frontier 1.0 supports the following languages:

Table I-4 Supported Languages

Language	Frontier All-in-One	Frontier Precinct	Frontier BMD
Arabic	Yes	Yes	Yes
Bengali	Yes	Yes	Yes
Cantonese	Audio Only	No	Yes
Chinese	Yes	Yes	Yes
English	Yes	Yes	Yes
Gujarati	Yes	Yes	No
Hindi	Yes	Yes	No
Japanese	Yes	Yes	No
Khmer	Yes	Yes	Yes
Korean	Yes	Yes	No
Nepali	Yes	Yes	No

Table I-4 Supported Languages (*continued*)

Language	Frontier All-in-One	Frontier Precinct	Frontier BMD
Mandarin	Audio Only	No	Yes
Punjabi	Yes	Yes	No
Russian	No	No	Yes
Spanish	Yes	Yes	Yes
Tagalog	Yes	Yes	No
Tamil	Yes	Yes	No
Telugu	Yes	Yes	No
Vietnamese	Yes	Yes	No
Yupik	No	No	Yes

SECTION I.3.1.4 SUPPORTED FUNCTIONALITY

The LVU Frontier 1.0 is designed to support the following voting variations:

- General Election
- Closed Primary
- Open Primary
- Early Voting
- Partisan/Non-Partisan Offices
- Write-In Voting
- Primary Presidential Delegation Nominations
- Split Precincts
- Vote for N of M
- Ballot Rotation
- Provisional or Challenged Ballots
- Straight Party Voting
- Cross-Party Endorsement
- Rank Choice Voting

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

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

SECTION I.4 SCOPE OF TESTING

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

As a new system, the LVU Frontier 1.0 will be evaluated against all applicable requirements contained in the principles and guidelines. To accomplish this, Pro V&V has defined multiple test areas relevant to each Principle. Tests will be executed within each test area to evaluate the applicable Requirements. Table I-3 details the VVSG 2.0 Principles, Guidelines, and associated test areas.

Table I-3 VVSG 2.0 Test Areas

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

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

VVSG 2.0 Guideline	VSTL Test Areas
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.	
Principle 3: Transparent <i>The voting system and voting processes are designed to provide transparency.</i>	
3.1 - The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood. 3.2 - The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection. 3.3 - The public can understand and verify the operations of the voting system throughout the entirety of the election.	TDP Review, Usability, FCA, System Integration Testing
Principle 4: Interoperable <i>The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.</i>	
4.1 - Voting system data that is imported, exported, or otherwise reported, is in an interoperable format. 4.2 - Standard, publicly available formats for other types of data are used, where available. 4.3 - Widely-used hardware interfaces and communications protocols are used. 4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.	Interoperability, TDP Review, FCA, System Integration Testing, PCA
Principle 5: Equivalent and Consistent Voter Access <i>All voters can access and use the voting system regardless of their abilities.</i>	
5.1 - Voters have a consistent experience throughout the voting process within any method of voting. 5.2 - Voters receive equivalent information and options in all modes of voting	Usability, Accessibility, FCA, TDP Review

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

VVSG 2.0 Guideline	VSTL Test Areas
Principle 6: Voter Privacy <i>Voters can mark, verify, and cast their ballot privately and independently.</i>	
6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections. 6.2 - Voters can mark, verify, and cast their ballot or other associated cast vote record, without assistance from others	Usability, Accessibility, FCA, TDP Review
Principle 7: Marked, Verified, and Cast as Intended <i>Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.</i>	
7.1 - The default voting system settings present a ballot usable for the widest range of voters, and voters can adjust settings and preferences to meet their needs. 7.2 - Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes and selections. 7.3 - Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.	Usability, Accessibility, FCA, TDP Review
Principle 8: Robust, Safe, Usable, and Accessible <i>The voting system and voting processes provide a robust, safe, usable, and accessible experience.</i>	
8.1 - The voting system’s hardware, software, and accessories are robust and do not expose users to harmful conditions. 8.2 - The voting system meets currently accepted federal standards for accessibility. 8.3 - The voting system is evaluated for usability with a wide range of representative voters, including those with and without disabilities. 8.4 - The voting system is evaluated for usability with election workers.	Usability, Accessibility, FCA, TDP Review
Principle 9: Auditable <i>The voting system is auditable and enables evidence-based elections.</i>	
9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results. 9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.	Source Code Review, TDP Review, FCA, Security Tests, Accuracy, Interoperability, Accessibility, Cryptographic Testing

Table I-3 VVSG 2.0 Test Areas (continued)

VVSG 2.0 Guideline	VSTL Test Areas
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.	
Principle 10: Ballot Secrecy <i>The voting system protects the secrecy of voters' ballot selections.</i>	
10.1 - Ballot secrecy is maintained throughout the voting process.	FCA, Usability, Accessibility, TDP Review, Security Tests, Cryptographic Testing
10.2 - The voting system does not contain nor produce records, notifications, information about the voter, or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.	
Principle 11: Access Control <i>The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.</i>	
11.1 - The voting system enables logging, monitoring, reviewing, and modifying of access privileges, accounts, activities, and authorizations.	Security Testing, Vulnerability Testing, FCA
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	
Principle 12: Physical Security <i>The voting system prevents or detects attempts to tamper with voting system hardware.</i>	
12.1 - The voting system supports mechanisms to detect unauthorized physical access.	Security Testing, Vulnerability Testing, FCA, TDP Review, Penetration Testing
12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.	
Principle 13: Data Protection <i>The voting system protects data from unauthorized access, modification, or deletion.</i>	
13.1 –The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.	Security Tests, FCA, TDP Review, Cryptographic Testing

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

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

Pro V&V has determined that Requirements associated with E2E Verifiable Voting Systems functionality are not applicable to the LVU Frontier 1.0. These Requirements include the following:

- 9.1.6 – Cryptographic E2E verifiable
- 9.1.6-A– Verified cryptographic protocol
- 9.1.6-B – Independent evaluation of E2E cryptographic protocol implementation

9.1.6-C, 9.1.6-C.1, 9.1.6-C.2 – Cryptographic ballot selection verification by voter
9.1.6-D, 9.1.6-D.1, 9.1.6-D.2 – Methods for cryptographic ballot selection verification
9.1.6-E, 9.1.6-E.1, 9.1.6-E.2, 9.1.6-E.3, 9.1.6-E.4, 9.1.6-E.5 – Ballot receipt
9.1.6-F – Disputes involving ballot receipts
9.1.6-G, 9.1.6-G.1, 9.1.6-G.2 – Evidence export
9.1.6-H – Mandatory ballot availability
9.1.6-I, 9.1.6-I.1, 9.1.6-I.2 – Verification of encoded vote documentation
9.1.6-J, 9.1.6-J.1, 9.1.6-J.1.a, 9.1.6-J.1.b, 9.1.6-J.2 – Verifier reference implementation
9.1.6-K – Privacy preserving, universally verifiable ballot tabulation
10.2.4-A – Voting information in receipts
13.3-B – E2E cryptographic voting protocols

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

SECTION I.5 TESTING RESPONSIBILITIES

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

Owner Assignments

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

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

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

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

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

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

SECTION I.6 THIRD PARTY TESTS

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

SECTION II: PRE-CERTIFICATION TESTING AND ISSUES

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

SECTION II.1 EVALUATION OF PRIOR VSTL TESTING

The LVU Frontier 1.0 is a new voting system that has not previously been tested in the EAC Program. Full functional and hardware testing will be performed on the system and a complete TDP review will be performed on all submitted documentation.

Prior to approval of the application for testing, the LVU Frontier 1.0 was subjected to Penetration Testing in accordance with Section 4.5 of the *EAC Voting System Testing and Certification Program Manual, Version 3.0*. The purpose of the test was to assess the security posture of the LVU Frontier 1.0 voting system prior to entering the EAC's Testing & Certification program. Penetration Testing was conducted in two phases: Phase I (Pre-Testing Assessment) and Phase II (Penetration Testing). The penetration testing report including identified vulnerabilities and risk ratings, as well as guidance on how to mitigate the discovered weaknesses was then submitted to the EAC as part of the Test Readiness Review (TRR).

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

SECTION II.2 EVALUATION OF PRIOR NON-VSTL TESTING

No prior non-VSTL testing of the LVU Frontier 1.0 was considered for this test campaign.

SECTION II.3 KNOWN FIELD ISSUES

The LVU Frontier 1.0 is being submitted for evaluation as a new system that has not been fielded; therefore, there are no fielded systems preceding this system. The LVU Frontier 1.0 may serve as the baseline to subsequent systems submitted for evaluation in the future. At that time, any known field issues on the baseline system or any subsequent certified versions derived from the LVU Frontier 1.0 system will be addressed in the associated published test plans.

SECTION III: MATERIALS REQUIRED FOR TESTING

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

The materials required for testing of the LVU Frontier 1.0 include all materials to enable the test campaign to occur. This includes the applicable hardware and software as well as the TDP and test support materials, as described in the following subsections.

SECTION III.1 SOFTWARE

This subsection lists the system proprietary and COTS software as provided in the manufacturer's System Overview document.

Frontier EMS Software Configuration:

- EMS Application Suite 1.0.5.1, containing:
 - Ballot Designer
 - Tally and Reporting (incl. Election Readiness Dashboard)
 - Audio Studio

- Data Importer
- Application Server Manager
- EMS Logger
- Security Hardening
- EMS Server Application & Services
 - Data Center Manager
 - File System Service
 - Smart Card Helper Service
- MBS Version (Frontier Central) – FrontierCentral_1.0.4.1_EAC_1.0_20260123
- MBS Version (Frontier Precinct) – FrontierPrecinct_1.0.3.1_EAC_1.0_20260113
- MBS Version (Frontier All-in-One) – FrontierAll-in-One_1.0.3.1_EAC_1.0_20260113
- MCF Version (Frontier BMD) – MCF_1.0.3.1_20260127
- *Optional Ballot Review 1.0.4.1*
- EMS Standard Server Configuration
 - Microsoft Windows Server 2022
 - .NET Framework 3.5
 - .NET Framework 4.8
 - Internet Information Services (IIS)
 - Microsoft SQL Server 2022 Standard
 - SQL Server Management Studio
 - Microsoft Visual C++ 2013 Redistributable
 - Microsoft Visual C++ 2015 Redistributable
 - Adobe Reader DC
 - Dell Drivers
 - Fonts
 - Arial Narrow (2.37a)
 - Optional:
 - Cepstral Voices 6.2.3
 - Ballot printer drivers
 - Report printer drivers
 - UPS drivers
 - RAID utility
- EMS Express Server Configuration
 - Microsoft Windows 11 Professional
 - .NET Framework 3.5
 - .NET Framework 4.8
 - Microsoft Defender
 - Internet Information Services (IIS)
 - Microsoft SQL Server 2022 Standard
 - SQL Server Management Studio
 - Microsoft Visual C++ 2013 Redistributable

- Microsoft Visual C++ 2015 Redistributable
- Adobe Reader DC
- Dell Drivers
- Fonts
 - Arial Narrow (2.37a)
- Optional:
 - Cepstral Voices 6.2.3
 - iButton Driver
 - Ballot printer drivers
 - Report printer drivers
 - UPS drivers
 - RAID utility
- EMS Domain Controller Server Configuration
 - Microsoft Windows Server 2022
 - .NET Framework 3.5
 - .NET Framework 4.8
 - DNS Service
 - DHCP Service
 - Internet Informational Services (IIS)
 - Dell Drivers
 - Optional
 - UPS drivers
 - Microsoft Defender
- EMS Standard and Express Client Configuration
 - Microsoft Windows 11 Pro
 - .NET Framework 3.5
 - .NET Framework 4.8
 - Microsoft Defender
 - Internet Informational Services (IIS)
 - Microsoft Visual C++ 2013 Redistributable
 - Microsoft Visual C++ 2015 Redistributable
 - iButton Driver
 - Adobe Reader DC
 - Dell Drivers
 - Optional
 - Report printer drivers
 - Ballot printer drivers
 - UPS drivers

Frontier Ballot Activation Software Configuration:

- Ballot Activation 1.0.5.1
- Microsoft Windows 11 Pro
 - .NET Framework 3.5
 - .NET Framework 4.8
 - Microsoft Defender
 - Internet Information Services (IIS)
- Microsoft Visual C++ 2013 Redistributable
- Microsoft Visual C++ 2015 Redistributable
- iButton Driver
- Adobe Reader DC
- Dell Drivers

Frontier Central Client Software Configuration:

- Frontier Central Software Application 1.0.4.1
- Microsoft Windows 11 Pro
 - .NET Framework 3.5
 - .NET Framework 4.8
 - Microsoft Defender
 - Internet Information Services (IIS)
- Microsoft Visual C++ 2013 Redistributable
- Microsoft Visual C++ 2015 Redistributable
- iButton Driver
- Adobe Reader DC
- Dell Drivers
- Scanner Drivers
- Optional
 - Report printer drivers
 - Ballot printer drivers
 - UPS drivers

Frontier Ballot Marking Device Software Configuration:

- Android OS Version 8.1.0-3.1.0
- Frontier Ballot Marking Device Application 1.0.4.1

Frontier All-in-One Software Configuration:

- Frontier Precinct Firmware 1.0.4.1
- Linux 2.6.30
- Kernel 2.6.30
- U-BOOT 1.3.4

Frontier Precinct Software Configuration:

- Frontier Precinct Firmware 1.0.4.1
- Linux 4.9.11X
- Kernel 4.9.11
- U-BOOT 2017.03

SECTION III.2 HARDWARE/EQUIPMENT

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

EMS Express Server Hardware Configuration:

- Desktop Computer
 - Dell Pro Max Slim XE
 - Dell Precision 3460 XE
- Network Switches
 - Dell x1008
 - Cisco 8-port Switch (CBS350-8T-E-2G)
 - Cisco 8-port Switch (C1300-8T-E-2G)
- Auxiliary Equipment:
 - LCD Monitor:
 - Dell P2426H
 - Dell 3225DE
 - Dell P2425H
 - Dell P2422H
 - Dell P2419H
 - Dell P2417H
 - UPS:
 - Tripp Lite SMART1500RMXL2U
 - APC SMT1500C Smart-UPS
 - CyberPower PR1500LCD
 - iButton to 1-Wire USB Adapter: Dallas Maxim DS1402-RP8+
 - iButton Reader/Writer: Dallas Maxim DS9490R#
 - Compact Flash / SD Reader: Lexar Professional USB 3.0 Dual-Slot Card Reader
 - Compact Flash / SD Reader: Kingston USB 3.0 High-Speed Media Reader

- Compact Flash / SD Reader: Hoodman Steel USB3
- Compact Flash / SD Reader: Delkin Devices DDREADER-44
- Compact Flash / SD Reader: IOGEAR GFR381
- Smart Card Reader: Advanced Card Systems ACR38U
- Smart Card Reader: Advanced Card Systems ACR39U
- Smart Card Reader: HID Omnikey 3121 FIPS-201
- Keyboard, Mouse, Headset with microphone, Audio Adapter networking switch – COTS computing accessories
- EMS Report Printer: HP M404dn laser or equivalent

EMS Standard Server Hardware Configuration:

- Server Computer
 - Dell PowerEdge R660
- Domain Controller Server
 - Dell PowerEdge R260
- Network Switches
 - Dell x1026
 - Cisco 24-port Switch (CBS350-24T-4G)
 - Cisco 24-port Switch (C1300-24T-4G)
- Auxiliary Equipment:
 - LCD Monitor:
 - Dell P2425H
 - Dell P2422H
 - Dell P2419H
 - Dell P2417H
 - UPS:
 - Tripp Lite SMART1500RMXL2U
 - APC SMT1500C Smart-UPS
 - CyberPower PR1500LCD
 - Keyboard, Mouse, KVM Switch, Headset with microphone, Audio Adapter networking switch – COTS computing accessories

EMS Standard Client Hardware Configuration:

- Desktop Computer

- Dell Pro Max Slim XE
- Dell Precision 3460 XE
- Auxiliary Equipment:
 - iButton to 1-Wire USB Adapter: Dallas Maxim DS1402-RP8+
 - iButton Reader/Writer: Dallas Maxim DS9490R#
 - Compact Flash / SD Reader: Lexar Professional USB 3.0 Dual-Slot Card Reader
 - Compact Flash / SD Reader: Kingston USB 3.0 High-Speed Media Reader
 - Compact Flash / SD Reader: Hoodman Steel USB3
 - Compact Flash / SD Reader: Delkin Devices DDREADER-44
 - Compact Flash / SD Reader: IOGEAR GFR381
 - Smart Card Reader: Advanced Card Systems ACR38U
 - Smart Card Reader: Advanced Card Systems ACR39U
 - Smart Card Reader: HID Omnikey 3121 FIPS-201
 - LCD Monitor:
 - Dell P2425H
 - Dell P2422H
 - Dell P2419H
 - Dell P2417H
 - UPS:
 - Tripp Lite SMART1500RMXL2U
 - APC SMT1500C Smart-UPS
 - CyberPower PR1500LCD
 - Keyboard, Mouse, Headset with microphone, Audio Adapter networking switch – COTS computing accessories
 - EMS Report Printer: HP M404dn laser or equivalent

Frontier Central Client Hardware Configuration:

- Desktop Computer
 - Dell Pro Max Slim XE (Canon or InoTec Scanner Configurations)
 - Dell Precision 3460 XE (Canon Configuration)
 - Dell OptiPlex XE4 (InoTec Configuration)
- Scanner:
 - Canon DR-G2140 (Imprinter Optional)

- Canon DR-G1130 (Imprinter Optional)
- InoTec HiPro 821 with Integrated Imprinter
- Auxiliary Equipment:
 - iButton to 1-Wire USB Adapter: Dallas Maxim DS1402-RP8+
 - iButton Reader/Writer: Dallas Maxim DS9490R#
 - Compact Flash / SD Reader: Lexar Professional USB 3.0 Dual-Slot Card Reader
 - Compact Flash / SD Reader: Kingston USB 3.0 High-Speed Media Reader
 - Compact Flash / SD Reader: Hoodman Steel USB3
 - Compact Flash / SD Reader: Delkin Devices DDREADER-44
 - Compact Flash / SD Reader: IOGEAR GFR381
 - LCD Monitor:
 - Planar PCT2235 (Canon Configuration)
 - Dell P2424HT (Canon or InoTec Configurations)
 - Lenovo 10QXPAR1US (InoTec Configuration)
 - Lenovo 11GCPAR1US (InoTec Configuration)
 - Dell P2418HT (InoTec Configuration)
 - UPS:
 - CyberPower PR1500LCD-VTVM
 - Keyboard, Mouse, Headset with microphone, Audio Adapter networking switch – COTS computing accessories
- Election Media:
 - iButton Dallas Maxim DS1963S-F5+ (with Key Ring Mount DS9093A+)
 - USB Memory Device (16GB): Centon (BiCS4) PN: C4-CT-U3P2-16.3
 - USB Memory Device (16GB): Centon S4-CM-U3P2-16.1
 - USB Memory Device (16GB): Apacer EH353-M APHA016GAG0CG-3TM
 - USB Memory Device (8GB): Centon (BiCS4) PN: C4-CT-U3P2-8.3
 - USB Memory Device (8GB): Centon S4-CM-U3P2-8.1
 - USB Memory Device (8GB): Apacer EH353-M APHA008GAG0CG-3TM
 - USB Memory Device (64GB): Apacer (BiCS5) AN3.112GGS.00231
 - USB Memory Device (128GB): Apacer (BiCS5) AN3.112HGS.00131
 - USB Memory Device (32GB): Centon (20nm) PN: C4-CT-U3P2-32.6
 - USB Memory Device (64GB): Centon (20nm) PN: C4-CT-U3P2-64.1

- USB Memory Device (128GB): Centon (20nm) PN: C4-CT-U3P2-128.1
- Compact Flash Memory Cards (16GB): Centon C4-CM-CF-16.4
- Compact Flash Memory Cards (8GB): RiTek RDCF8G-233XMCB2-i
- Compact Flash Memory Cards (8GB): SanDisk SDCFHS-008G
- Compact Flash Memory Cards (4GB): SanDisk SDCFHS-004G
- Compact Flash Memory Cards (16GB): Apacer AP-CF016GLBNS-NDNR4T-DVS

Frontier Ballot Activation Hardware Configuration:

- Dell Laptop
 - Dell Pro 14
 - Dell Latitude 3340
 - Dell Latitude 3420
- Auxiliary Equipment:
 - Smart Card Reader: Advanced Card Systems ACR38U
 - Smart Card Reader: Advanced Card Systems ACR39U
 - Smart Card Reader: HID Omnikey 3121 FIPS-201
- Election Media:
 - USB Memory Device (16GB): Centon (BiCS4) PN: C4-CT-U3P2-16.3
 - USB Memory Device (16GB): Centon S4-CM-U3P2-16.1
 - USB Memory Device (16GB): Apacer EH353-M APHA016GAG0CG-3TM
 - USB Memory Device (8GB): Centon (BiCS4) PN: C4-CT-U3P2-8.3
 - USB Memory Device (8GB): Centon S4-CM-U3P2-8.1
 - USB Memory Device (8GB): Apacer EH353-M APHA008GAG0CG-3TM
 - USB Memory Device (64GB): Apacer (BiCS5) AN3.112GGS.00231
 - USB Memory Device (128GB): Apacer (BiCS5) AN3.112HGS.00131
 - USB Memory Device (32GB): Centon (20nm) PN: C4-CT-U3P2-32.6
 - USB Memory Device (64GB): Centon (20nm) PN: C4-CT-U3P2-64.1
 - USB Memory Device (128GB): Centon (20nm) PN: C4-CT-U3P2-128.1
 - Smart Cards: ACS ACOS-6-64 v3090 and ACOS-6-64 v3100
 - Smart Cards: CardLogix C7

Frontier Precinct Hardware Configuration:

- PCOS-331A

- PCOS-331B (w/o Imprinter)
- Ballot Box: Stackable Molded Plastic BOX-350A
- Ballot Box: Collapsible Plastic: ElectionSource IM-COLLAPSIBLE BIN
- Audio-Tactile Interface (ATI-USB) box
- Election Media:
 - iButton (Pollworker): Dallas Maxim DS1963S-F5+ (w/Black Key Ring Mount DS9093A+)
 - iButton (Admin/Tech): Dallas Maxim DS1963S-F5+ (w/Yellow Key Ring Mount DS9093AY+)
 - SDHC Memory Cards (16GB): Centon (BiCS5) PN: C4-ET-SDU3-16.1
 - SDHC Memory Cards (8GB): Centon (BiCS4) PN: S4-ET-SDU3-8.1
 - SDHC Memory Cards (8GB): Centon S4-CM-SDHU1-8G-002
 - SDHC Memory Cards (8GB): Centon C4-CM-SDU1-8.2
 - SDHC Memory Cards (8GB): Apacer (BiCS5) PN: AJ3.148FSA.00105
- Optional Hardware:
 - Headphone: Cyber Acoustics ACM-70, ACM-70B or equivalent

Frontier All-in-One Hardware Configuration:

- PCOS-410B
- Ballot Box: Stackable Molded Plastic BOX-410A
- Audio-Tactile Interface (ATI-Serial) box
- Light Pole for Ballot Boxes
- Election Media:
 - iButton (Pollworker): Dallas Maxim DS1963S-F5+ (w/Black Key Ring Mount DS9093A+)
 - iButton (Admin/Tech): Dallas Maxim DS1963S-F5+ (w/Yellow Key Ring Mount DS9093AY+)
 - Compact Flash Memory Cards (16GB): Centon C4-CM-CF-16.4
 - Compact Flash Memory Cards (8GB): RiTek RDCF8G-233XMCB2-i
 - Compact Flash Memory Cards (16GB): Apacer AP-CF016GLBNS-NDNR4T-DVS
- Optional Hardware:
 - Headphone: Cyber Acoustics ACM-70, ACM-70B or equivalent
 - Sip & puff: Enabling Device #972
 - Sip & puff: 970K (Pkg of 10)
 - Paddle Switches: Enabling Device #971
 - Paddle Switches: AbleNet 10033400 (2x)

- Paddle Switch Cable: Hosa Technology YMM-261 (for use with AbleNet switches)

Frontier Ballot Marking Device Hardware Configuration:

- Avalue SID-15V-Z37 (15.6 in. screen w/ intrusion detection)
- Avalue SID-21V-Z37 (21.5 in. screen w/ intrusion detection)
- Avalue HID-21V-BTX (21.5 in. screen w/ intrusion detection)
- Audio-Tactile Interface (ATI-USB) box
- USB Busy LED Indicator
- UPS:
 - APC SMT1500C
 - CyberPower PR1500LCD-VTVM
- Printer:
 - HP M402dne
 - HP M404dn
 - HP M501dn
 - HP 4001dn
- Election Media:
 - USB Memory Device (128GB): Apricorn AEGIS Secure Key 3NX PN: ASK3-NX-128GB
 - USB Memory Device (32GB): Apricorn AEGIS Secure Key 3NX PN: ASK3-NX-32GB
 - USB Memory Device (16GB): Centon (BiCS4) PN: C4-CT-U3P2-16.3
 - USB Memory Device (16GB): Centon S4-CM-U3P2-16.1
 - USB Memory Device (16GB): Apacer EH353-M APHA016GAG0CG-3TM
 - USB Memory Device (8GB): Centon (BiCS4) PN: C4-CT-U3P2-8.3
 - USB Memory Device (8GB): Centon S4-CM-U3P2-8.1
 - USB Memory Device (8GB): Apacer EH353-M APHA008GAG0CG-3TM
 - USB Memory Device (64GB): Apacer (BiCS5) AN3.112GGS.00231
 - USB Memory Device (128GB): Apacer (BiCS5) AN3.112HGS.00131
 - USB Memory Device (32GB): Centon (20nm) PN: C4-CT-U3P2-32.6
 - USB Memory Device (64GB): Centon (20nm) PN: C4-CT-U3P2-64.1
 - USB Memory Device (128GB): Centon (20nm) PN: C4-CT-U3P2-128.1
 - Smart Cards: ACS ACOS-6-64 v3090 and ACOS-6-64 v3100
 - Smart Cards: CardLogix C7

- Optional Hardware:
 - Headphone: Cyber Acoustics ACM-70, ACM-70B or equivalent
 - Sip & puff: Enabling Device #972
 - Sip & puff: 970K (Pkg of 10)
 - Paddle Switches: Enabling Device #971
 - Paddle Switches: AbleNet 10033400 (2x)
 - Paddle Switch Cable: Hosa Technology YMM-261 (for use with AbleNet switches)

SECTION III.3 MATERIALS/CONSUMABLES

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

Table III-3 LVU Frontier 1.0 Materials/Consumables

Material	Description(s)
Tamper Evident Security Seals	Adhesive tamper evident security seal, Novavision Part# XSG21-08RESN
Printer Cartridges	HP Printer Cartridges for each of the HP Printers in the Frontier BMD System
Smart Cards	Programmable Smart Cards for voters, poll workers, and technicians for the Frontier BMD System
Stereo Breakout Cable	3.5mm stereo male plug to dual 3.5mm mono female plugs
3.5mm Stereo Cable	3.5mm stereo male plug to 3.5mm stereo female plug
iButton Security Tokens	iButton Security Token with lanyards
Permanent Markers	Fine Tip Sharpie Permanent Markers
Ethernet Cables	Cat5e Ethernet Cables
Paper Rolls	Replacement Thermal Paper Rolls for the Frontier Precinct and All-in-One tabulators
Sip & Puff Disposable Straws	Disposable straws for use with the Sip & Puff input device
Ballot Stock	Ballot Paper Stock for printing ballots
A/C Power Cables	3-Prong A/C Power Cables
USB Thumb drives	8 GB and 16 GB USB Thumb drives

SECTION III.4 PROPRIETARY DATA

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

SECTION IV: TEST SPECIFICATIONS

Certification testing of the LVU Frontier 1.0 submitted for evaluation will be performed to ensure the applicable requirements of the VVSG 2.0, the VVSG 2.0 Test Assertions, Version 1.4 (or current), and the EAC Testing and Certification Program Manual, Version 3.0, are met. Additionally, all EAC Request for Interpretations (RFI) and Notices of Clarification (NOC) relevant to the system under test will be incorporated in the test campaign. A complete listing of the EAC RFIs and NOCs is available on the EAC website.

SECTION IV.1 REQUIREMENTS

To evaluate the LVU Frontier 1.0 test requirements, each Principle of the VVSG 2.0 will be analyzed in conjunction with a preliminary TDP review to determine the applicable Requirements. The preliminary TDP is performed to gather information concerning the system under test and its capabilities or design intentions. Additionally, a TDP review will be performed throughout the test campaign. The TDP Review includes the Initial Review, the Regulatory/Compliance Review, and the Final Review. This review is conducted to determine if the submitted technical documentation meets the regulatory, customer-stated, or end-user requirements and includes reviewing the documents for stated functionality review and verification.

The Pro V&V designated Test Areas utilized to evaluate the LVU Frontier 1.0 to the requirements set forth in the VVSG 2.0, are described in the subsections that follow.

SECTION IV.2 TEST CASE DEVELOPMENT AND DESIGN

For each test area, Pro V&V will utilize baseline test cases augmented with specially designed test cases tailored to the specific design of the LVU Frontier 1.0. Additionally, specific election definitions will be designed for the Operational Status Check, Volume & Stress Test, and the Logic & Accuracy Tests.

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

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

SECTION IV.2.1 HARDWARE ENVIRONMENTAL TEST CASE DESIGN

No previous examinations have been performed on the LVU Frontier 1.0. The voting system hardware shall be subjected to the tests specified in Section V.14. Testing will be performed by personnel verified by Pro V&V to be qualified to perform the test. Pro V&V will utilize a third-party test facility for performance of the electrical and environmental tests. All pre and post operational status checks shall be conducted by Pro V&V personnel.

SECTION IV.2.2 SOFTWARE MODULE TEST CASE DESIGN AND DATA

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

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

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

SECTION IV.2.3 SOFTWARE FUNCTIONAL TEST CASE DESIGN AND DATA

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

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

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

SECTION IV.2.4 SYSTEM-LEVEL TEST CASE DESIGN

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

SECTION IV.3 TEST PROCEDURE DEVELOPMENT AND VALIDATION

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

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

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

SECTION V: TEST PROCEDURES

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

SECTION V.1 PHYSICAL CONFIGURATION AUDIT (PCA)

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

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

The PCA will be conducted in two phases: Initial (to baseline the system prior to test commencement) and Final (to verify final software and hardware configurations). Additionally, Pro V&V will perform a physical examination of the hardware to determine if any component of the voting system contains any wireless technologies. When applicable, the inspection may include taking off covers and disassembling devices. If such technologies are discovered, Pro V&V will perform an inspection, functional verification, and security evaluation of the noted capability.

SECTION V.2 TECHNICAL DATA PACKAGE (TDP) REVIEW

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

- Initial TDP Review

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

- Compliance Review

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

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

- Consistency/Completeness Review

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

A listing of all documents contained in the LVU Frontier 1.0 is provided below:

Liberty Documents

- Frontier System Overview
- Frontier System Security Specification
- Frontier System Test and Verification Specification
- Frontier Personnel Deployment and Training Requirements
- Frontier Configuration Management Plan
- Frontier Quality Assurance Program
- Frontier System Change Notes

Frontier EMS Documents

- Frontier EMS Functionality Description
- Frontier EMS Software Design and Specification
- Frontier EMS System Operations Procedures
- Frontier EMS System Maintenance Manual
- Frontier EMS Client Workstation Installation and Configuration Procedure
- Frontier EMS Express Installation and Configuration Procedure
- Frontier EMS Ballot Activation and Installation Configuration Procedure
- Frontier Domain Member Server Installation and Configuration Procedure
- Frontier Domain Member Client Workstation Installation and Configuration Procedure
- Frontier Domain Controller Installation and Configuration Procedure

Frontier Central Documents

- Frontier Central System Functionality Description
- Frontier Central Software Design and Specification
- Frontier Central System Operation Procedures
- Frontier Central Installation and Configuration Procedure

Frontier All-in-One Documents

- Frontier All-in-One System Functionality Description
- Frontier All-in-One System Hardware Specifications
- Frontier All-in-One Software Design and Specifications
- Frontier All-in-One System Operations Procedures
- Frontier All-in-One System Maintenance Manual
- Frontier All-in-One Installation and Configuration Procedure

Frontier Precinct Documents

- Frontier Precinct System Functionality Description
- Frontier Precinct System Hardware Specification
- Frontier Precinct Firmware Installation Procedure
- Frontier Precinct Software Design and Specification
- Frontier Precinct System Operation Procedures
- Frontier Precinct System Maintenance Manual

Frontier Ballot Marking device (BMD) Documents

- Frontier BMD System Functionality Description
- Frontier BMD Software Design Specification
- Frontier BMD System Operation Procedures
- Frontier Ballot Marking Device System Installation and Configuration Procedure
- Frontier Ballot Marking Device HID-21 System Installation and Configuration Procedure
- Frontier BMD System Maintenance Manual

Liberty User Guides

- Frontier All-in-One User Guide
- Frontier Ballot Review User Guide
- Frontier Ballot Marking Device User Guide

- Frontier Central User Guide
- Frontier Audio Studio User Guide
- Frontier Automated Test Deck User Guide
- Frontier Ballot Activation User Guide
- Frontier Ballot Designer User Guide
- Frontier Data Importer User Guide
- Frontier Logger User Guide
- Frontier Tally and Reporting User Guide
- Frontier Precinct User Guide

Liberty Supplementary Documents

- Frontier C++ Coding Standard
- Frontier Common Data Format Mapping
- Frontier Printing and Finishing Specifications
- Frontier System Identification Guide
- Frontier Tabulator Surface Cleaning Guide
- Frontier Total Results File Format
- Frontier All-in-One Li-Ion Battery Maintenance Procedure
- Frontier All-in-One Level One (L1) Maintenance Manual
- Frontier All-in-One Machine Behavior Settings
- Frontier All-in-One Usability Test Report for VVSG 2.0
- Frontier BMD Machine Configuration File Settings for Landscape Mode
- Frontier BMD Machine Configuration File Settings for Portrait Mode
- Frontier BMD Usability Test Report for VVSG 2.0
- Frontier Central Machine Behavior Settings
- Frontier EMS Common Data Format Mapping
- Frontier EMS Exporting and Verifying Logs in Common Data Format
- Frontier Precinct Extracting Firmware Contents and Verifying SHA256 Values
- Frontier Precinct Level One (L1) Maintenance Manual
- Frontier Precinct Machine Behavior Settings
- Frontier Precinct Usability Test Report for VVSG 2.0

- Java Coding Standards
- JavaScript Coding Standards

COTS Supplemental

- Ablenet Single Switch Manual
- ACM-70B Stereo Headphones
- ACS AC0s6 Multi-Application and Purse Card Functional Specifications
- ACS ACR38x CCID Smart Card Reader Reference Manual
- ACS ACR39 Series PC-linked Smart Card Readers Reference Manual
- APC Installation and Operation Rack Power Distribution Unit AP9562
- APC SMT1500 Installation Guide
- APC SMT1500 Operation Manual
- APC SMT1500C Operation Manual
- Apricorn Aegis Secure Key 3NX Compliance
- Apricorn Aegis Secure Key 3NX Quick Start Guide
- Apricorn Aegis Secure Key 3NX Compliance
- Avalue HID-21V-BTX-B1R User Manual
- Avalue HID-21V-BTX User Manual
- Avalue SID-15V Quick Reference Guide
- Avalue SID-15V-Z37-A1R User Manual
- Avalue SID-21V Fact Sheet
- Avalue SID-21V-Z37-A1R User Manual
- Avalue SID-21V Quick Reference Guide
- Canon DR-G1130 User Guide
- Canon DR-G2140 DR-G2110 DR-2090 User Manual
- Cisco Business 350 Series Managed Switches Data Sheet
- Cisco Business 350 Series Managed Switches Quick Start Guide
- Cisco C1300 Series Switches Admin Guide
- Cisco C1300 Series Switches Data Sheet
- CyberPower RoHS Declaration of Compliance
- CyberPower Smart App Sinewave Series PR1500LCD User's Manual

- Delkin DD Reader Datasheet
- Dell Latitude 3340 2-in-1 Product Compliance Datasheet
- Dell Latitude 3340/Latitude 3340 2-in-1 Service Manual
- Dell Latitude 3340/Latitude 3340 2-in-1 Setup and Specifications
- Dell Latitude 3420 Compliance Datasheet
- Dell Latitude 3420 Setup and Specifications Guide
- Dell Networking X-Series Spec Sheet
- Dell Networking X1000 and X4000 Series Switches User Guide
- Dell OptiPlex XE4 SFF Product Compliance Datasheet
- Dell OptiPlex XE4 Small Form Factor Service Manual
- Dell OptiPlex XE4 Small Form Factor Setup and Specifications
- Dell P2417H Monitor User's Guide
- Dell P2418HT User's Guide
- Dell P2418HT Worldwide Regulatory Compliance Engineering and Environmental Affairs
- Dell P2419H Monitor User's Guide
- Dell P2422H Monitor User's Guide
- Dell P2422H Product Compliance Datasheet
- Dell P2424HT Quick Start Guide
- Dell P2424HT User Guide
- Dell P2424HT Product Compliance Datasheet
- Dell P2425H Quick Start Guide
- Dell P2425H User Guide
- Dell PowerEdge R660 Product Compliance Datasheet
- Dell PowerEdge R660 Installation and Service Manual
- Dell PowerEdge R260 Installation and service Manual
- Dell Precision 3460 SFF Product Compliance Datasheet
- Dell Precision 3460 Small Form Factor Service Manual
- Dell Precision 3460 Small Form Factor Setup and Specifications
- Dell Pro 14 PC14250 Owners-Manual
- Dell Pro Max Slim FCS1250 Owners-Manual

- HIC Coding Standard Manual
- HIC++ Standards Model for C++
- HID Omnikey 3121 Assembly Procedure
- HID Omnikey 3121 User Guide
- HID Omnikey 3121 Datasheet
- HP LaserJet Pro 4001, 4002 User Guide
- HP LaserJet Pro 4001 series Setup Guide
- HP LaserJet Pro M402dn Datasheet
- HP LaserJet Pro M402dne Datasheet
- HP Laser Jet Pro M402, M403 User Guide
- HP Laser Jet Pro M403-M304, M404-M405 User Guide
- HP LaserJet Pro M404 series Datasheet
- HP LaserJet Pro M501 User Guide
- InoTec HiPro Scanner Brochure
- InoTec HiPro Scanner User Manual
- IOGEAR GFR381 USB 3.0 Compact Flash Memory Card Reader
- Kingston FCR-HS4 USB 3.0 Datasheet
- Lenovo ThinkCentre TIO24Gen3Touch User Guide
- Lenovo ThinkCentre TIO24Gen4Touch User Guide
- Lexar Professional USB 3.0 Dual-Slot Reader Quick Start Guide
- Planar PCT2235 Touch LED LCD Monitor User's Guide
- Tripp-Lite SmartPro SM1500RMXL2UTAA Datasheet
- Tripp-Lite Smart1500 Owner's Manual

Frontier Build Documents

- Frontier Central Build Procedure
- Frontier All-in-One Firmware Build, Prerequisite Setup and Installation
- Frontier Precinct Firmware Build Procedure
- Frontier Ballot Marking Device Build Procedure
- Frontier Android Build Procedure
- Frontier EMS Windows Build Document

SECTION V.3 SOURCE CODE REVIEW

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

The submitted source code will be subjected to a compliance review. Once the compliance review is performed and the source is deemed stable enough to proceed with testing, the source code and all additional packages will be compiled into a Compliance Build. Following successful completion of the FCA, a Trusted Build will be performed. The trusted build consists of inspecting the submitted source code, COTS, and third-party software products and combining them to create the executable code following the documented process from the *“United States Election Assistance Commission Voting System Testing and Certification Program Manual Version 3.0”* Section 4.8. Performance of the trusted build includes the build documentation review.

A combination of automated source code review and manual source code review methods will be used to review the submitted source code. The complete source code will be reviewed utilizing the automated source code tools described in the LVU Frontier 1.0 Software Design and Specification documents. These tools include Yarn Lint version 1.22.19, SonarSource SA SonarQube platform with Java plugin, version 8.9.16, and Parasoft C/C++test, both of which are listed on the Mitre Common Weakness Enumeration (CWE) Compatibility Product and Services List.

To validate the tools, Pro V&V utilized Samate Software Assurance Reference Dataset (SARD). This dataset provides ‘Pristine vs. Dirty’ sample test data, in this case source code, and a ‘Flawed and Fixed’ dataset. These samples allow for the tool to be validated. Pro V&V will then follow the LVU Frontier 1.0 TDP to install the automatic source code review tools. Once the tools are installed, validated, and the review executed, Pro V&V will verify the results obtained match the expected results. No modifications to the tools are required, only importing of the LVU rule set. Findings from the automated review tool will be manually reviewed to ensure that all source code is VVSG 2.0 compliant.

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

SECTION V.4 FUNCTIONAL CONFIGURATION AUDIT (FCA)

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

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

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

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

SECTION V.5 SECURITY REVIEW

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

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

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

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

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

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

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

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

Administrative Evaluation

The Administrative Security Evaluation begins with reviewing the TDP package for assessor orientation to the system while evaluating the breadth and depth of security topics covered. The documentation will be assessed for coverage, clarity, correctness, consistency, and effectiveness of the documented security controls.

The assessment evaluates the security controls' effectiveness in protecting confidentiality, integrity, availability, and accountability within the system. The evaluation also assesses that ample and appropriate controls are implemented within the system to provide adequate protection to the system. This evaluation spans all security defenses and phases mentioned above. The assessment extends beyond the TDP Review to evaluate the compliance in fulfilling the requirements outlined in the VVSG and/or related requirements. The assessment includes a review of the vendor's submitted threat matrix provided in the TDP to evaluate security controls for effectiveness in protecting against threats.

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

- Frontier EMS: Privilege Escalation, Permissions & Roles, Access Controls
- Frontier BMD: Permissions & Roles, Access Controls
- Frontier Precinct: Permissions & Roles, Access Controls
- Frontier All-in-One: Permissions & Roles, Access Controls
- Frontier Central: Permissions & Roles, Access Controls

Examples of these attacks are provided below:

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

Physical Evaluation

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

- Frontier EMS: Removing Protective Measures, Detection & Prevention
- Frontier BMD: Removing Protective Measures, Detection & Prevention
- Frontier Precinct: Removing Protective Measures, Detection & Prevention
- Frontier All-in-One: Removing Protective Measures, Detection & Prevention
- Frontier Central: Removing Protective Measures, Detection & Prevention

Examples of these attacks are provided below:

Packet Capture – Physically manipulating the security measures in place to gain access.

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

Technical/Logical Evaluation

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

To perform the Security Review, qualified test personnel will develop and execute specifically designed test cases in an attempt to defeat the access controls and security measures documented in the system TDP. The test cases will be developed utilizing the requirements found in Principles 11-15 to verify that each identified security feature and procedure meets requirements and functions as expected and documented. Qualified personnel will also perform each type of identified evaluation (Administrative, Physical, and Technical/Logical) on the LVU Frontier 1.0 system.

Additionally, the LVU Frontier 1.0 submitted threat matrix identifying the system's risks and vulnerabilities was evaluated for completeness and to determine that mitigating controls were adequately implemented. The evaluation of the system shall be accomplished by utilizing a combination of functional testing and source code review. All findings will be reported to the EAC and Liberty Vote.

Pro V&V will use multiple security techniques to examine various security measures of the LVU Frontier 1.0 Voting System. Examples of possible attack vectors may include but are not limited to SQL Injection Attacks, Network Scans, Packet Captures, and Brute Force Attacks. For each component the following tasks may include:

- Frontier EMS: SQL Injection Attacks, Network Scans

- Frontier BMD: Brute Force Attack
- Frontier Precinct: Brute Force Attack
- Frontier All-in-One: Brute Force Attack
- Frontier Central: Packet Capture, Brute Force Attack

Examples of these attacks are provided below:

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

SQL Injection - Using SQL Injection on the Frontier EMS to try to modify the database

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

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

Additionally, network analysis tools will be used to obtain network packet captures to examine communication and authentication attempts between all LVU Frontier 1.0 devices, and to assess that appropriate encryption is utilized across all devices.

SECTION V.6 VULNERABILITY TESTING

Vulnerability is a system weakness related to security procedures, internal controls, flaws, features, or user errors that can potentially be exploited by a threat source. To assess the vulnerability of the LVU Frontier 1.0 system, qualified personnel will evaluate the system by executing test cases developed to specific requirements contained in the principles listed below:

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

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

The test cases will be executed to verify the system meets the requirements and functions as expected and documented. Additionally, qualified personnel will perform each type of identified evaluation (Administrative (to include a review of the system vulnerability management plan submitted as part of the system TDP), Physical, and Technical/Logical) on the LVU Frontier 1.0 system.

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

SECTION V.7 CRYPTOGRAPHIC TESTING

Cryptographic testing will be performed to assess the LVU Frontier 1.0 System to the following Principle:

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

To perform the Cryptographic Testing, qualified personnel will evaluate the system by executing test cases developed to the specified requirements contained within the principle to verify the system meets the requirements and functions as expected and documented. Qualified personnel will also perform each type of identified evaluation (Administrative, Physical, and Technical/Logical) on the LVU Frontier 1.0 system.

SECTION V.8 USABILITY REVIEW

A Usability Review will be performed to examine how users interact with the system. The purpose of the Usability Review is to assess the usability of the LVU Frontier 1.0 system. Usability is defined in the VVSG 2.0 as, “Effectiveness, efficiency, and satisfaction with which a specified set of users can achieve a specified set of tasks in a particular environment. Usability in the context of voting refers to voters being able to cast valid votes as they intended quickly, without errors, and with confidence that their contest selections were recorded correctly. It also refers to the usability of the setup and operation of voting equipment in the polling place.” The Usability Review consists of tasks that address voter confidentiality (privacy and independence), integrity (accuracy), and availability (usability).

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

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

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

SECTION V.9 ACCESSIBILITY REVIEW

Per VVSG 2.0, the voting system shall be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters. Accessibility is dependent upon voter confidentiality (privacy and independence), integrity (accuracy), and availability (usability).

Accessibility features must be integrated into the manufacturer's voting system so that accessibility for voters with disabilities is supported throughout the voting session, including any steps to activate the ballot at the voting station, ballot marking, verification, and casting. This requirement ensures accessibility to the voter throughout the entire session. Not only are individual system components (such as ballot markers, paper records, and optical scanners) accessible, but they also support voters with disabilities throughout the process of voting from activation through casting.

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

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

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

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

SECTION V.10 SYSTEM INTEGRATION TESTING

The System Integration area of testing is a system level test that evaluates the integrated operation of both hardware and software. Compatibility of the voting system software components or subsystems with one another, and with other components of the voting system environment, shall be determined through functional tests integrating the voting system software with the remainder of the system. Additionally, the system will be configured exactly as it would for normal field use per the procedures detailed in the LVU Frontier 1.0 technical documentation. This includes connecting all supporting equipment and peripherals including ballot boxes, voting booths (regular and accessible), and any physical security equipment such as locks and ties.

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

Three general elections with the following breakdowns:

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

Three primary elections with the following breakdowns:

- Primary Election PRIM-01: This election is designed to functionally test a Closed Primary Election with multiple ballots and support for common voting variations. This election contains thirty-one contests and six parties compiled into eighteen ballot styles, each ballot containing six contests.
- Primary Election PRIM-02: Open Primary Election held in two precincts. This election contains thirteen contests compiled into three ballot styles. One contest is in all three ballot styles; all other contests are independent.
- Primary Election PRIM-03: A Closed Primary Election held in two precincts. This election contains ten contests and is compiled into two ballot styles. Two of the contests are in both ballot styles. The other eight contests are split between the two parties' ballots. This election is designed to functionally test the handling of multiple ballot styles, support for at least three languages including a character-based language, support for common voting variations, and audio support for at least three languages and an ADA binary input device.

SECTION V.11 ACCURACY TEST

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

Principle 1: High Quality Design

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

1.2-A – Assessment of accuracy

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

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

1.2-B – Reliably detectable marks

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

1.2-C – Minimum ballot positions

A minimum of 10,000,000 ballot positions must be read by the voting system and tabulated accurately.

1.2-G – Misfeed rate benchmark

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

To meet the requirements of 1.2-C, the LVU Frontier 1.0 system under test must read a minimum of 10,000,000 ballot positions and tabulate accurately. The requirement shall be broken down by component using the following minimum ballot positions read and tabulated accurately:

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

Frontier Precinct – 3,340,000

Frontier All-in-One – 3,340,000

Frontier Central – 5,010,000

Total – 13,360,000

Prior to test initiation, a Test Case and Election Definition specific to the Accuracy Test will be developed. The accuracy requirements for the LVU Frontier 1.0 will be met by executing the Test Case utilizing a test deck composed of pre-marked and hand-marked ballots of each ballot length supported by the system. This test deck will be processed until the required minimum number of ballot positions to be tabulated is met.

SECTION V.12 VOLUME TEST

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

SECTION V.13 INTEROPERABILITY

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

Principle 4: Interoperable

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

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

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

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

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

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

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

SECTION V.14 HARDWARE TESTING

The LVU Frontier 1.0 is a new system submitted for testing to the VVSG 2.0; therefore, the full of Hardware Testing will be required for all components. VVSG 2.0 Hardware Testing consists of electrical

hardware testing, an operational environmental test, and various non-operational environmental tests, as described below:

Electrical Hardware Tests

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

Non-Operational Environmental Hardware Tests

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

Operational Environmental Hardware Test

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

Table V-2 LVU Frontier 1.0 Hardware Testing Overview

Hardware Test	VMSG 2.0 Requirement	Applicable Component			
		Frontier Precinct	Frontier All-in-One	Frontier BMD	Frontier Central
Radiated Emissions	1.2-I	Yes	Yes	Yes	No
Conducted Emissions	1.2-I	Yes	Yes	Yes	No
Radiated Immunity	2.7-G	Yes	Yes	Yes	No
Conducted RF Immunity	2.7-J	Yes	Yes	Yes	No
Lightning Surge	2.7-I	Yes	Yes	Yes	No
Electrical Fast Transient	2.7-I	Yes	Yes	Yes	No
Electrostatic Disruption	2.7-K	Yes	Yes	Yes	No
Electrical Power Disturbance	2.7-I	Yes	Yes	Yes	No
Non-Operational Low Temperature	2.7-F	Yes	Yes	Yes	No
Non-Operational High Temperature	2.7-F	Yes	Yes	Yes	No
Non-Operational Humidity	2.7-F	Yes	Yes	Yes	No
Non-Operational Bench Handling	2.7-D	Yes	Yes	Yes	No
Non-Operational Transportation Vibration	2.7-E	Yes	Yes	Yes	No
Continuous Operation – Varied Environmental Conditions	2.7-C	Yes	Yes	Yes	Yes
Electrical Supply (Battery Backup)	2.7-H	Yes	Yes	Yes	No

SECTION V.14.1 ELECTRICAL HARDWARE TESTING

The LVU Frontier 1.0 is a new system submitted for testing to the VVSG 2.0; therefore, the full suite of Electrical Hardware Testing will be required for components as listed in the above table. VVSG 2.0 Electrical Hardware Testing consists of the following tests:

- **Electrical Supply (Battery Backup)**

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

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

Note: The Frontier Central, the Central Count Component of the LVU Frontier 1.0, will not be evaluated against the 2-hour battery backup requirement. The Frontier Central will be evaluated to verify it provides for a graceful shutdown to allow switching to an alternate power source.

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

Requirement 2.7-I (Withstand conducted electrical disturbances)

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

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

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

- **Electrical Fast Transient (EFT)**

Requirement 2.7-I (Withstand conducted electrical disturbances)

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

The test for Electrical Fast Transient shall be conducted in compliance with the test specified in IEC 61000-4-4 (2012).

- **Lightning Surge**

Requirement 2.7-I (Withstand conducted electrical disturbances)

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

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

- **Electrostatic Disruption (ESD)**

Requirement 2.7-K (Electrostatic discharge immunity)

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

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

The test for Electrostatic Disruption shall be conducted in compliance with the test specified in IEC 61000-4-2 (2008).

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

Requirement 2.7-J (Emissions from other connected equipment)

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

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

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

- **Electromagnetic Susceptibility (Radiated Immunity)**

Requirement 2.7-G (Electrical disturbances)

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

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

- **Conducted RF Immunity**

Requirement 2.7-J (Emissions from other connected equipment)

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

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

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

SECTION V.14.2 OPERATIONAL HARDWARE TESTING

Operational Hardware Testing

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

- **Operational Hardware Test**

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

- This test is similar to the low and high temperature tests of MIL-STD-810H, Methods 502.7 and 507.6, with test conditions that correspond to the requirements of the performance standards. This procedure tests system operation under various environmental conditions for at least 96 hours. During 72 hours of operating time, the equipment shall be in a test chamber under the test conditions imposed for both temperature and humidity. For the remaining 24 hours, the equipment shall be operated at room temperature or in ambient conditions. The system shall be powered for the entire period of this test; the power may be disconnected for maintenance or if necessary for removal of the system from the test chamber during the ambient portion of testing. Operation shall consist of exercising ballot-counting cycles, which vary by system type, for 15 minutes of each hour, and at the maximum rate calculated from the manufacturer's documented throughput rates.

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

SECTION V.14.3 NON-OPERATIONAL HARDWARE TESTING

Non-Operational Hardware Testing

Non-Operational Hardware Testing consists of the following: Bench Handling, Transportation Vibration, Humidity, Low Temperature, and High Temperature. These tests are intended to simulate exposure to conditions typically encountered during the handling and transportation of voting equipment between storage facilities and polling places, including physical shock and vibration associated with handling and

transportation of equipment between a storage facility and a deployment site and temperature/humidity conditions that may be encountered during storage in an uncontrolled environment.

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

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

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

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

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

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

- **Humidity Test (Non-Operational)**

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

This test simulates non-operating physical environmental conditions simulating temperature-related and humidity related stresses faced during storage of system components. This test is equivalent to the procedure of MIL-STD-810H, Method 507.6, Procedure I- Natural (Hot-Humid) Storage. The minimum duration for this test is 10 days or 10 x 24-hour cycles. Relative humidity ranges of 25% to 80% and temperature ranges from 88° F to 105° F shall be tested.

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

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

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

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

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

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

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

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

SECTION V.15 PRODUCT SAFETY REVIEW

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

- **Principle 8, Requirement 8.1-K (Eliminating Hazards)**

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

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

- **Requirement 2.1.1 (Workmanship)**

2.1.1-A – General build quality

All manufacturers of voting systems must practice proper workmanship by:

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

2.1.1-B – Durability estimation

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

1. Estimated replacement rates (e.g., 3 years, 10 years);
2. Estimated costs per replacement;
3. Estimated warranty types and costs;
4. Associated replacement policies, services, and available maintenance agreements; and
5. Plans for collecting, maintaining, and reporting data to the EAC to support and validate estimates.

2.1.1-C – Durability of paper

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

2.1.1-D – Ensure compatibility of specified paper and ink

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

2.1.2-C – Nameplate and labels

All voting devices must:

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

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

SECTION VI: TEST DATA

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

SECTION VI.1 TEST DATA RECORDING

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

SECTION VI.2 TEST DATA CRITERIA

The LVU Frontier 1.0 shall be evaluated against all applicable requirements contained in the VVSG 2.0. A *VVSG 2.0 Cross Reference Matrix* specific to the LVU Frontier 1.0 will be utilized during the test campaign to ensure that all applicable VVSG 2.0 requirements are addressed. The matrix will contain the requirement number, title, and text for each VVSG 2.0 requirement, a listing of applicable system

components, Artifact and Result Artifact IDs (Test Case IDs, Test Result IDs, Test Reports, etc.), and any applicable notes.

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

SECTION VI.3 TEST DATA REDUCTION

Test data shall be processed and recorded in the Engineering Notebook on the LVU Frontier 1.0 dedicated project Smartsheet and the relevant Test Cases.

SECTION VII: TEST CONDITIONS

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

SECTION VII.1 FACILITY REQUIREMENTS

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

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

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

SECTION VII.2 TEST SET-UP

All voting system equipment shall be received and documented using Pro V&V established QA procedures. Upon receipt of all hardware, an inspection will be performed to verify that the equipment received is free from obvious signs of damage and/or degradation that may have occurred during transit. If present, this damage shall be recorded, photographed, and reported to the Liberty Vote Representative. Additionally, a comparison shall be made between the recorded serial numbers/part numbers and those listed on shipper's manifestation and any discrepancies shall be reported to the LVU Representative. TDP items and all source code received shall be inventoried and maintained by Pro V&V during the test campaign. During test performance, the system shall be configured as it would be for normal field use. This includes connecting all supporting equipment and peripherals.

SECTION VII.3 TEST SEQUENCE

The LVU Frontier 1.0 will be evaluated against all applicable requirements in the VVSG 2.0. There is no required sequence for test performance; however, there may be prerequisite tasks for some testing. If so, the predecessor task will be identified within the test case.

SECTION VIII: TEST OPERATIONS PROCEDURES

Pro V&V will identify PASS/FAIL criteria for each executed test case. The PASS/FAIL criteria will be based on the specific expected results of the system. In the case of an unexpected result that deviates from what is considered standard, normal, or expected, a root cause analysis will be performed.

Pro V&V will evaluate every VVSG 2.0 requirement applicable to the LVU Frontier 1.0 voting system. Any deficiencies noted will be reported to the EAC and the manufacturer. If it is determined that there is insufficient data to determine compliance, this test plan will be altered, and additional testing will be performed.

APPENDIX A: PROJECT SCHEDULE

Task Name	Start Date	End Date	Assigned To	Title
Project Commencement	01/21/26	02/19/26		
EAC Kickoff Meeting	01/21/26	01/21/26	Michael Walker	Program Manager
Application Approval from EAC	02/19/26	02/19/26	Michael Walker	Program Manager
TDP	12/02/25	07/29/26		
TDP Submission	12/02/25	12/02/25	Michael Walker	Program Manager
TDP Review (Initial, Compliance, Final)	12/03/25	07/29/26	Michael Walker	Program Manager
Test Plan	03/02/26	04/28/26		
Test Plan Creation	03/02/26	03/13/26	Michael Walker	Program Manager
Test Plan (Review and Approval)	03/13/26	04/28/26	Michael Walker	Program Manager
Source Code	12/02/25	02/25/26		
Source Code Submission	12/02/25	12/02/25	Michael Walker	Program Manager
Source Code (Review and Compliance Build)	12/03/25	02/25/26	Michael Walker	Program Manager
System Delivery & Setup	12/02/25	03/04/26		
PCA	12/02/25	12/02/25	Michael Walker	Program Manager
System Setup	12/03/25	12/03/25	Michael Walker	Program Manager
System Loads & Hardening	03/02/26	03/04/26	Michael Walker	Program Manager
System Level Testing	03/18/26	08/05/26		
System Level Test Design and Execution	03/18/26	08/05/26	Michael Walker	Program Manager
Trusted Build and System Integration	07/02/26	08/05/26		
Trusted Build	07/02/26	07/07/26	Michael Walker	Program Manager
System Integration	07/30/26	08/05/26	Michael Walker	Program Manager
Test Report	08/06/26	10/07/26		
Test Report Creation	08/06/26	08/12/26	Michael Walker	Program Manager
Test Report (Review and Approval)	08/13/26	10/07/26	Michael Walker	Program Manager