UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Kari Lake; Mark Finchem,

Plaintiffs,

v.

Kathleen Hobbs, as Arizona Secretary of State; Bill Gates; Clint Hickman, Jack Sellers; Thomas Galvin; and Steve Gallardo, in their capacity as members of the Maricopa County Board of Supervisors; Rex Scott; Matt Heinz; Sharon Bronson; Steve Christy; Adelita Grijalva; in their capacity as members of the Pima County Board of Supervisors,

Defendants.

No. 2:22-cv-00677-JJT

DECLARATION OF ANDREW D. PARKER

I, Andrew D. Parker, hereby declare, under the penalty of perjury, and state the following:

1. I am an attorney with the law firm of Parker Daniels Kibort LLC and represent the Plaintiffs, Kari Lake and Mark Finchem, in the above-captioned matter.

2. Attached hereto as Exhibit A is a true and correct copy of EAC Doc. No. DVS-018-MTP-02, titled, "As Run Certification Test Plan – Modification," published by the United States Election Assistance Commission ("EAC") related to Dominion Voting Systems

Democracy Suite 5.5A. The EAC is a U.S. federal commission, established by the Help America Vote Act of 2002, that certifies voting systems. This document is published at the EAC website at https://www.eac.gov/sites/default/files/voting_system/files/Attachment_D_-_Dominion_D-Suite_5.5-A_As_Run_Test_Plan.pdf .

3. Attached hereto as Exhibit B is a true and correct copy of the Declaration of J. Alex Halderman filed on September 21, 2021 in the United States District Court for the Northern District of Georgia in case no. 1:17-cv-2989, *Curling v. Raffensperger*.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on June 29, 2022 */s/ Andrew D. Parker*

Andrew D. Parker

Exhibit A

As Run Certification Test Plan – Modification

Document Number: DVS-018-MTP-02

Prepared for:

Vendor Name	*Dominion Voting Systems*
Vendor System	*Democracy Suite 5.5-A*
EAC Application No.	*DVS-DemSuite5.5-A*
Vendor Address	*1201 18th Street, Suite 210* *Denver, Colorado 80202*

Prepared by:

4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

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

Revision History

Date	Release	Author	Revision Summary
December 12th, 2018	1.0	J. Panek	As Run Test Plan
December 15th, 2018	1.1	J. Panek	Updated to address EAC Comments

Disclaimer

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

Trademarks

- SLI is a registered trademark of SLI Compliance.
- All products and company names are used for identification purposes only and may be trademarks of their respective owners.

TABLE OF CONTENTS

1 INTRODUCTION

This Certification Test Plan outlines the test approach SLI Compliance will follow when performing system modification testing on the **Dominion Voting Systems (Dominion) Democracy Suite 5.5-A (D-Suite 5.5-A)** against the Voluntary Voting System Guidelines 1.0 (VVSG 1.0). The purpose of this document is to provide a clear understanding of the work SLI will conduct and a detailed plan outlining the test effort.

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

1.1 Description and Overview of the Certified System

This section contains a description of the previously certified system, the specific modifications to the current system version, and the impact of those modifications on the system and certification testing.

1.1.1 Definition of the Baseline Certified System

The **Dominion D-Suite 5.5-A** voting system is a paper-based optical scan voting system consisting of the following elements: Election Management System (EMS), ImageCast Central Count (ICC), ImageCast X BMD (ICX BMD), and ImageCast Precinct (ICP). The **D-Suite 5.5-A** voting system is a modification from the baseline EAC certified **Democracy Suite 5.5 (D-Suite 5.5)** voting system, which consists of software applications and devices described below.

Election Management System (EMS)

The **Dominion D-Suite 5.5-A** EMS consists of various components running as either a front-end/client application or as a back-end/server application. A listing of the applications and a brief description of each is presented below.

- **EMS Adjudication** - Responsible for adjudication, including reporting and generation of adjudicated result files from ImageCast Central tabulators and adjudication of write-in selections from ImageCast Precinct and ImageCast Central tabulators. This client component is installed on both the server and the client machines.
- **EMS Audio Studio** - 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.
- **EMS Election Data Translator** - End-user application used to export election data from election project and import election data into election project.

- **EMS Election Event Designer** - Integrates election definition functionality together with ballot styling capabilities and represents a main pre-voting phase end-user application
- **ImageCast Voter Activation** - Allows the poll workers to program smart cards for voters. The smart cards are used to activate voting sessions on ImageCast X.
- **EMS Results Tally and Reporting** - Integrates election results acquisition, validation, tabulation, reporting, and publishing capabilities and represents the main post-voting phase end-user application.
- **EMS Adjudication Service** - Provides ballot information such as contests, candidates and their coordinates from EMS to the Adjudication application.
- **EMS Application Server** - Responsible for executing long running processes, such as rendering ballots, generating audio files and election files, etc.
- **EMS Database Server** - Database which holds all the election project data, including pre-voting and post- voting data.
- **EMS Data Center Manager** - A system level configuration application used in EMS back-end data center configuration.
- **EMS Election Device Manager** - Used for production and programming of election files, and other accompanying files, for ImageCast X terminals.
- **EMS File System Service** - 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 ICP CF card, etc.
- **EMS NAS Server** - Server file repository of the election project file based artifacts, such as ballots, audio files, reports, log files, election files, etc.
- **Smart Card Helper Service** - Provides required data format for programming smart cards for ImageCast devices, or, for jurisdiction's voting registration system in case of integration.

ImageCast Precinct (ICP)

The ICP device is a hybrid precinct optical scan paper/DRE ballot counter designed to provide six major functionalities: ballot scanning, second chance voting, accessible voting, ballot review, tabulation, and poll worker functions.

ImageCast Central (ICC) Count Scanner

The ICC is a high-speed, central ballot scan tabulator based on Commercial off the Shelf (COTS) hardware, coupled with the custom-made ballot processing application software. It is used for high speed scanning and counting of paper ballots.

ImageCast X (ICX) Ballot Marking Device (BMD)

The Democracy Suite ImageCast X ballot marking platform is used for creation of paper cast vote records. These ballots can be scanned, reviewed, cast and tabulated at the polling location on an ImageCast Precinct device or later scanned and tabulated by the ImageCast Central optical ballot scanner. The ImageCast X also supports enhanced accessibility voting through optional accessories connected to the ImageCast X unit.

Table 1 – D-Suite 5.5 Software and Firmware

Application	Software Version
EMS Election Event Designer (EED)	5.5.12.1
EMS Results Tally and Reporting (RTR)	5.5.12.1
EMS Application Server	5.5.12.1
EMS File System Service (FSS)	5.5.12.1
EMS Audio Studio (AS)	5.5.12.1
EMS Data Center Manager (DCM)	5.5.12.1
EMS Election Data Translator (EDT)	5.5.12.1
ImageCast Voter Activation (ICVA)	5.5.12.1
EMS Adjudication	5.5.8.1
EMS Adjudication Service	5.5.8.1
Smart Card Helper Service	5.5.12.1
ImageCast Precinct	5.5.3-0002
ImageCast Central	5.5.3.0002
ImageCast X	5.5.10.25
Machine Configuration File (MCF)	5.5.10.20_20180806
Device Configuration File (DCF)	5.4.01_20170521

1.1.2 Modifications

- A modification has been made to ICX BMD straight party behavior to show a modal pop-up window when a voter attempts to undervote a partisan contest after selecting a partisan choice in the straight party contest. The pop-up clarifies that the voter needs to remove their straight-party vote and manually vote all partisan contests if they wish for one or more of those contests affected by the straight party vote to be undervoted.
- Default ICX BMD localizations have been updated to change the final voter session wording to reflect that the ballot is being printed rather than cast.
- Removed the ICX DRE configuration from this version of the system.

- Removed the ICX Classic 15” device from this version of the system.
- Utilized Machine Configuration File v5.5.10.19 instead of the version certified with D-Suite 5.5, v5.5.10.20. The differences between the file versions are related to the VVPAT printer component, which is not included in the D-Suite 5.5-A system configuration.

1.1.3 Initial Assessment of Impact of the Modifications

An initial assessment of the impact that the modifications have on the system indicates that the functionality of the ICX BMD software has been changed in two very specific ways. Voter facing messaging during straight party voting, and updated localizations made to the final stage of a voter session will be tested.

Finally, hardening procedures will be thoroughly reviewed to ensure the process is accurate, fully documented, and that any changes made from the documents in the previous version of the system TDP have been reviewed by a Security Test Specialist.

1.2 References

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

1. Election Assistance Commission Voluntary Voting System Guidelines (EAC VVSG), Version 1.0 Volumes I and II.
2. NIST Handbook 150: 2016.
3. NIST Handbook 150-22: 2017.
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. SLI VSTL Quality System Manual, Rev. 2.6, prepared by SLI, dated March 28, 2018.

1.3 Terms and Abbreviations

The following terms and abbreviations will be used throughout this document:

Table 2 – Terms and Abbreviations

Term	Abbreviation	Description
Ballot Marking Device	BMD	An accessible computer-based voting system that produces a marked ballot (usually paper) that is the result of voter interaction with visual or audio prompts.
Compact Flash card	CF	This is a type of flash memory card in a standardized enclosure often used in voting systems to store ballot and/or vote results data.

Term	Abbreviation	Description
Commercial Off the Shelf	COTS	Term used to designate computer software, hardware or accessories that are ready-made and available for sale, lease, or license to the general public
Direct Recording Electronic	DRE	Voting systems that, using Touch Screen or other user interfaces, directly record the voter's selections in each race or contest on the ballot in electronic form.
Election Assistance Commission	EAC	An independent, bipartisan commission created by the Help America Vote Act (HAVA) of 2002 that operates the federal government's voting system certification program.
Election Management System	EMS	Typically a database management system used to enter jurisdiction information (district, precincts, languages, etc.) as well as election specific information (races, candidates, voter groups (parties), etc.). In addition, the EMS is also used to layout the ballots, download the election data to the voting devices, upload the results and produce the final results reports.
Functional Configuration Audit	FCA	The testing activities associated with the functional testing of the system.
National Institute of Standards and Technology	NIST	A non-regulatory federal agency within the U.S. Dept. of Commerce. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
National Voluntary Laboratory Accreditation Program	NVLAP	A division of NIST that provides third-party accreditation to testing and calibration laboratories.
Physical Configuration Audit	PCA	The testing activities associated with the physical aspects of the system (hardware, documentation, builds, source code, etc.).
Request For Information	RFI	A means used by testing laboratories and manufacturers to request that the EAC provide an interpretation of a technical issue related to testing of voting systems.
Requirements Matrix	N/A	A matrix that traces the VVSG requirements to the various test modules and test methods.

Term	Abbreviation	Description
Technical Data Package	TDP	The data package supplied by the vendor, which includes Functional Requirements, Specifications, End-user documentation, Procedures, System Overview, Configuration Management Plan, Quality Assurance Program, and manuals for each of the required hardware, software, firmware components of a voting system.
Voluntary Voting System Guidelines	VVSG	A set of specifications and requirements against which voting systems can be tested to determine if the systems provide all of the basic functionality, accessibility and security capabilities required for EAC certification.
Voter Verifiable Paper Audit Trail	VVPAT	An independent verification system for voting machines designed to allow voters to verify that their vote was cast correctly, to detect possible election fraud or malfunction, and to provide a means to audit the stored electronic results.
Voting System Test Lab	VSTL	An independent testing organization accredited by NVLAP and the EAC to conduct voting system testing for EAC certification.
Voting Test Specialist	VTS	An SLI employee within the Compliance division who has been qualified to perform EAC voting system certification testing.

1.4 Testing Responsibilities

The following project schedule contains owner assignments and identifies test procedure (module) development, test case (suite) development, 3rd party tests, and EAC and Manufacturer dependencies.

1.4.1 Project Schedule

The following schedule outlines the expected timeline for this project.

Task Name	Start	Finish
DVS D-Suite 5.5-A	**Mon 11/12/18**	**Wed 1/30/19**
Test Readiness Review (TRR)	**Mon 11/12/18**	**Fri 11/16/18**
Project Initiation	**Tue 11/20/18**	**Wed 11/21/18**
Client Deliverables	**Tue 11/20/18**	**Wed 11/21/18**
Receive and Setup Voting System Hardware	**Mon 11/12/18**	**Wed 11/14/18**
Documentation Review	**Wed 11/21/18**	**Wed 11/21/18**
Source Code Review	**Wed 11/21/18**	**Wed 11/21/18**
Test Plan	**Fri 11/30/18**	**Tue 12/11/18**
Create Test Plan	Fri 11/30/18	Fri 11/30/18
Submit Test Plan for EAC Review	Fri 11/30/18	Tue 12/11/18

Updates to Test Plan to Resolve EAC comments	Tue 12/11/18	Tue 12/11/18
EAC Review	Tue 12/11/18	Tue 12/11/18
Test Plan Complete	Tue 12/11/18	Tue 12/11/18
Trusted Build	**Thu 11/29/18**	**Fri 11/30/18**
Write Test Suites	**Wed 11/21/18**	**Mon 11/26/18**
Execute Test	**Wed 12/5/18**	**Fri 12/7/18**
Certification Test Report and Final Test Plan	**Tue 12/11/18**	**Mon 1/28/19**
Final updates to As Run Test Plan	Wed 12/12/18	Thu 12/13/18
Create Certification Report	Mon 12/3/18	Thu 12/13/18
EAC Review	Thu 12/13/18	Mon 1/14/19
Final updates to Test Report	Mon 1/14/19	Mon 1/14/19
EAC Review Complete	Mon 1/14/19	Mon 1/28/19
Project Closeout	**Mon 1/28/19**	**Wed 1/30/19**
Project Management	**Mon 11/12/18**	**Wed 1/30/19**

1.4.1.1 Owner Assignments

- System Analysis and Review will be conducted by Source Code Review, Security and Voting Test Specialists, with oversight by the Test Manager
- Source code review will be conducted by Source Code Review Specialists, with oversight by the Test Manager
- Documentation review will be conducted by Security and Voting Test Specialists, with oversight by the Test Manager
- Test Module Development will be conducted by Security and Voting Test Specialists, with oversight by the Test Manager
- Test Suite Development will be conducted by Security and Voting Test Specialists, utilizing SLI's formal Test Methods, with oversight by the Test Manager
- Formal Test Execution will be conducted by Security and Voting Test Specialists, with oversight by the Test Manager

1.4.1.2 Test Module Development

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

1.4.1.3 Test Suite Development

Test Suites will be developed to help group and focus testing around key areas of the voting system. The Test Suites will contain multiple test modules providing clear

and traceable test scripts and information. Depending on the type of system under test, various configurations will be identified within the suites. Potentially, variations of the same suite may be run multiple times in order to verify different configurations.

1.4.1.4 Formal Test Execution

Formal execution of the approved Test Suites and modules will be conducted to verify the system's compliance with the VVSG requirements.

1.4.1.5 3rd Party Hardware Testing

No 3rd Party hardware testing is scheduled for this project.

1.4.1.6 EAC & Manufacturer Dependencies

The Test Plan will require EAC approval prior to finalization.

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

The source code must have all discrepancies resolved, be able to be built successfully, installed, as well as successfully complete operational status checks prior to Formal Test Execution.

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

Please see the Project Plan for a detailed listing of all activities within the scope of this test campaign.

1.5 Scope of Testing

1.5.1 Block Diagram

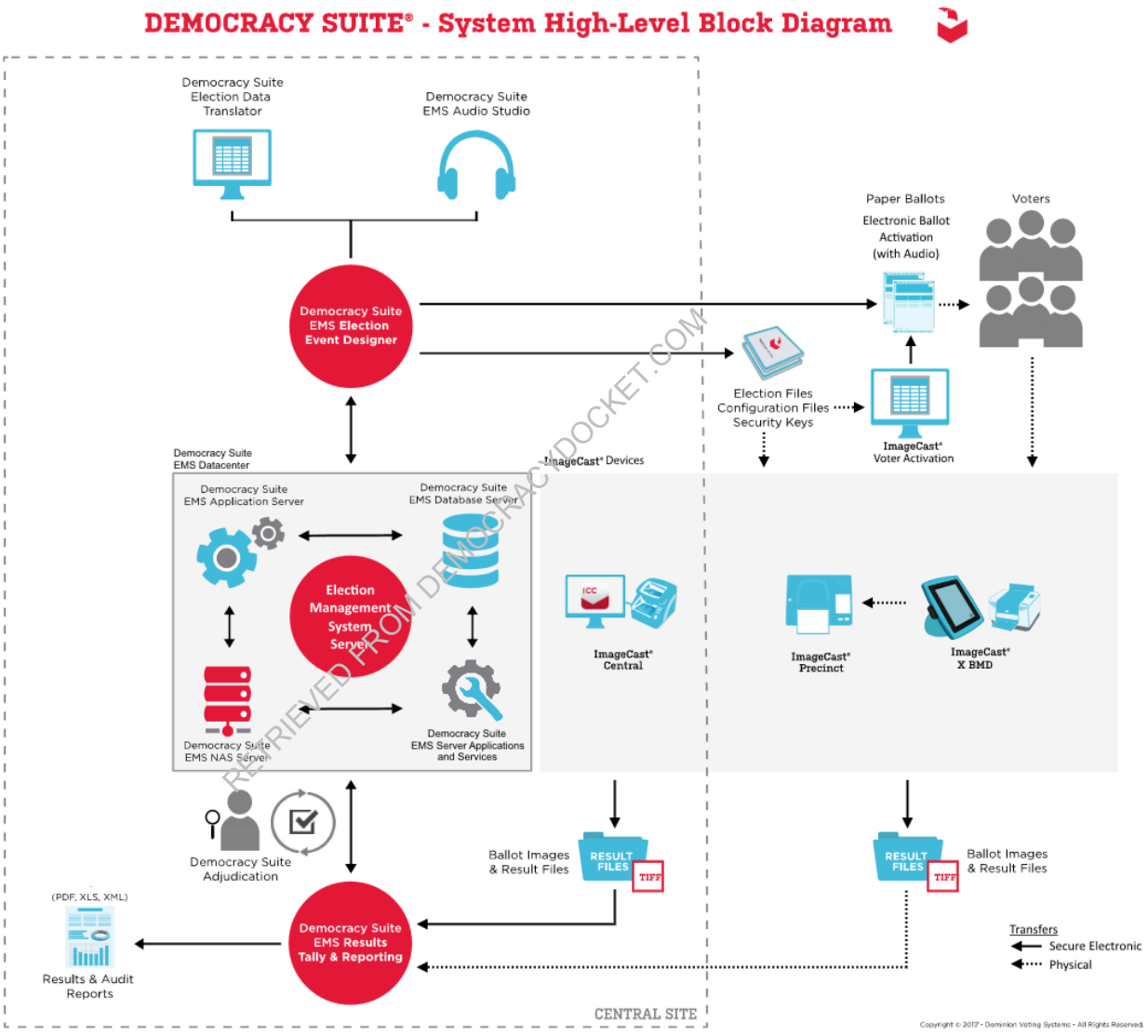

Figure 1: D-Suite 5.5-A Voting System Overview

1.5.2 System Limits

Per the TDP supplied by **Dominion**, system limits have not been modified in the **D-Suite 5.5-A** voting system.

Please refer to *2.02-DemocracySuiteSystemOverview-5.5-A.pdf*, section 5.1 System Capacity, for supported system limits.

1.5.3 Supported Languages

Per the TDP supplied by **Dominion**, supported languages have not been modified in the **D-Suite 5.5-A** voting system.

Please refer to *2.02-DemocracySuiteSystemOverview-5.5-A.pdf*, section 2.1.1 Languages Supported by Democracy Suite, for supported languages.

1.5.4 EAC Interpretations – RFI

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

This Certification Test Plan and the execution of tests for the voting system identified in this plan do not include any additional EAC interpretations.

1.5.5 EAC Notices of Clarification

As of the date this Certification Test Plan was created, there are no additional EAC NOCs that pertain to the execution of tests for the voting system identified in this plan that are not already in effect.

2 PRE-CERTIFICATION TESTING AND ISSUES

2.1 Evaluation of prior VSTL testing

VSTL testing has been performed on the version previous to the **Dominion D-Suite 5.5-A** voting system. The previous version of this system, **D-Suite 5.5**, is EAC certified, and will serve as the source code base for this evaluation.

State testing performed for the State of Pennsylvania found issues with state requirements on how straight party voting was handled, and with localization verbiage contained in the final stage of a voter session that indicated the word “cast” rather than “print”. During the security penetration test performed pursuant to the State of Pennsylvania "Attachment E to the Directive for Electronic Voting Systems", discrepancies were identified in the system that made it non-compliant with those requirements. Dominion made modifications to the documentation of D-Suite 5.5-A to bring the system into compliance with the State of Pennsylvania's requirements.

These issues were corrected in this release of the **D-Suite 5.5-A** voting system

2.2 Evaluation of prior non-VSTL testing

No prior state or non-VSTL lab testing is pertinent to the **Dominion D-Suite 5.5-A** voting system. Review of **Dominion's** internal testing is performed during the FCA review.

2.3 Known Field Issues

Review of the "Known Vulnerabilities" database, maintained by SLI, indicates that there are no known vulnerabilities to previous **Dominion** systems, which aren't already accounted for in SLI's Testing.

3 MATERIALS REQUIRED FOR TESTING

Any materials that are used in an election cycle must be provided to SLI to facilitate testing of the voting system. This section outlines these materials that are required.

3.1 Software/Firmware

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

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

3.1.1 Manufacturer Software/Firmware

The **Dominion D-Suite 5.5-A** voting system consists of the following software and firmware components:

- **Election Management System** software applications for all pre-voting and post-voting groups of activities in the process of defining and managing elections
  - EMS Adjudication
  - EMS Audio Studio
  - EMS Election Data Translator
  - EMS Election Event Designer
  - ImageCast Voter Activation
  - EMS Results Tally and Reporting
  - EMS Adjudication Service
  - EMS Application Server

- EMS Database Server
- EMS Data Center Manager
- EMS File System Service
- Smart Card Helper Service

- **ImageCast Central Count** central count scanner firmware
- **ImageCast X with BMD** precinct ballot marking device firmware
- **ImageCast Precinct** precinct hybrid optical scanner and DRE ballot tabulator firmware

Table 3 – Dominion D-Suite 5.5-A Software/Firmware

Application	Version
EMS Election Event Designer (EED)	5.5.12.1
EMS Results Tally and Reporting (RTR)	5.5.12.1
EMS Application Server	5.5.12.1
EMS File System Service (FSS)	5.5.12.1
EMS Audio Studio (AS)	5.5.12.1
EMS Data Center Manager (DCM)	5.5.12.1
EMS Election Data Translator (EDT)	5.5.12.1
ImageCast Voter Activation (ICVA)	5.5.12.1
EMS Adjudication	5.5.8.1
EMS Adjudication Service	5.5.8.1
Smart Card Helper Service	5.5.12.1
ImageCast Precinct	5.5.3-0002
ImageCast Central	5.5.3.0002
ImageCast X	5.5.10.30
Machine Configuration File (MCF)	5.5.10.19_20180706
Device Configuration File (DCF)	5.4.01_20170521

3.1.2 COTS Software/Firmware

This section details the COTS software and firmware utilized within the **Dominion D-Suite 5.5-A** voting system:

Table 1 – COTS Software/Firmware

Software/Firmware	Version	Filename
Microsoft Windows Server	2012 R2 Standard	Physical Media from Microsoft
Microsoft Windows	10 Professional	Physical Media from Microsoft

Software/Firmware	Version	Filename
.NET Framework	3.5	Physical Media from Microsoft
Microsoft Visual J#	2.0	vjredist64.exe, vjredist.exe
Microsoft Visual C++ 2013 Redistributable	2013	vcredist_x64.exe vcredist_x86.exe
Microsoft Visual C++ 2015 Redistributable	2015	vc_redist.x64.exe vc_redist.x86.exe
Java Runtime Environment	7u80	jre-7u80-windows-x64.exe jre-7u80-windows-i586.exe
Java Runtime Environment	8u144	jre-8u144-windows-x64.exe jre-8u144-windows-i586.exe
Microsoft SQL Server 2016 Standard	2016 Standard	Physical Media from Microsoft
Microsoft SQL Server 2016 Service Pack 1	2016 SP1	SQLServer2016SP1-KB3182545-x64-ENU.exe
Microsoft SQL Server 2016 SP1 Express	2016 SP1	SQLEXPRADV_x64_ENU.exe
Cepstral Voices	6.2.3.801	Allison (English): Cepstral_Allison_windows_6.2.3.801.exe Alejandra (Spanish): Cepstral_Alejandra_windows_6.2.3.801.exe
Arial Narrow Fonts	2.37a	ARIALN.TTF ARIALNB.TTF ARIALNBI.TTF ARIALNI.TTF
Maxim iButton Driver	4.05	install_1_wire_drivers_x86_v4 05.msi install_1_wire_drivers_x64_v4 05.msi
Adobe Reader DC	AcrobatDC	AcroRdrDC1501020060_en_US.exe
Microsoft Access Database Engine	2010	AccessDatabaseEngine.exe AccessDatabaseEngine_x64.ex e
Open XML SDK 2.0 for Microsoft Office	2.0	OpenXMLSDKv2.msi
Infragistics NetAdvanatage Win Forms 2011.1	2011 Vol.1	NetAdvantage_WinForms_20111.msi
Infragistics NetAdvanatage WPF 2012.1	2012 Vol.1	NetAdvantage_WPF_20121.msi
TX Text Control	16.0	TXText Control.NET for Windows

Software/Firmware	Version	Filename
Library for .NET		Forms 16.0.exe
SOX	14.3.1	sox.exe, libgomp-1.dll, pthreadgc2.dll, zlib1.dll
NLog	1.0.0.505	NLog.dll
iTextSharp	5.0.5	itextsharp.dll
OpenSSL	1.0.2k & 2.0.14 FIPS	openssl.exe, libeay32.dll, ssleay32.dll
SQLite	1.0.103.0	System.Data.SQLite.DLL (32-bit and 64-bit)
Lame	3.99.4	lame.exe
Speex	1.0.4	speexdec.exe and speexenc.exe
Ghostscript	9.04	gsdll32.dll (32-bit and 64-bit)
One Wire API for .NET	4.0.2.0	OneWireAPI.NET.dll
Avalon-framework-cvs-20020806	20020806	avalon-framework-cvs-20020806.jar
Batik	0.20-5	batik.jar
Fop	0.20-5	fop.jar
Microsoft Visual J# 2.0 Redistributable Package- Second Edition(x64)	2.0	vjc.dll, vjsjbc.dll, vjslibcw.dll, vjsnativ.dll, vjssupuilib.dll, vjsvwaux.dll
Entity framework	6.1.3	EntityFramework.dll
Spreadsheetlight	3.4.3	SpreadsheetLight.dll, SpreadsheetLight.xml
Open XML SDK 2.0 For Microsoft Office	2.0.5022.0	DocumentFormat.OpenXml.dll, DocumentFormat.OpenXml.xml
OpenSSL 1.0.2k	1.0.2k	openssl-1.0.2k.tar.gz
OpenSSl FIPS 2.0.10	2.0.10	openssel-fips-2.0.10.tar.gz
Zlib	1.2.3	Zlib-1.2.3.tar.gz
Google Text-to-Speech Engine	3.11.12	ARM: com.google.android.tts_3.11.12-210311121_minAPI19(armeabi-v7a)(nodpi).apk x86: com.google.android.tts_3.11.12-210311123_minAPI15(x86)(nodpi).apk

Software/Firmware	Version	Filename
ICX Prime Android 5.1.1 Image	0405	0405_5.1.1-01.12_user_android_x86.iso
ICX Classic Android 4.4.4 Image	0.0.98	byt_t_crv2_64-ota-BCX18-V0.0.98.zip
OpenSSL 1.0.2k	1.0.2k	openssl-1.0.2k.tar.gz
OpenSSl FIPS 2.0.10	2.0.10	openssel-fips-2.0.10.tar.gz
1-Wire Driver (x86)	4.05	install_1_wire_drivers_x86_v405.msi
1-Wire Driver (x64)	4.05	install_1_wire_drivers_x64_v405.msi
Canon DR-G1130 TWAIN Driver	1.2 SP6	G1130_DRIT_V12SP6.exe
Canon DR-M160II TWAIN Driver	1.2 SP6	M160II_DRIT_V12SP6.exe
Visual C++ 2013 Redistributable (x86)	12.0.30501	vcredist_x86.exe
uClinux	20070130	uClinux-dist-20070130.tar.gz
COLILO Bootloader	20040221	Colilo20040221.tar.gz
Zxing Barcode Scanner	4.7.5	BS-4.7.5.zip
SoundTouch	1.9.2	Soundtouch-1.9.2.tar.gz

3.2 Equipment

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

3.2.1 Manufacturer Equipment

The following manufacturer equipment will be used in testing:

Table 2 – Manufacturer Equipment

Device	Model
ImageCast Precinct Hybrid Optical Scanner and DRE	PCOS-320C
ImageCast Precinct Hybrid Optical Scanner and DRE	PCOS-320A
ICP Ballot Box	BOX-330A

3.2.2 COTS Equipment

This section details the COTS equipment utilized within the **Dominion D-Suite 5.5-A** voting system:

Table 3 – COTS Equipment

Device	Model
ICX aValue 21" Tablet (SID-21V)	C10A003700689
ICX aValue 21" Tablet (HID-21V)	1708100078
Dell OptiPlex 3050 All In One	DP/N 0Y0VVT
Canon imageFormula DR-G1130 Scanner	GF306276
Canon imageFORMULA DR-M160-II	GX333152, GX333300
OKI C931e Ballot Printer	N36100A
Dell Precision T3420 PC	HLZ7HQ2, 66V9HQ2
HP LaserJet Pro Printer M402dn	PHB5F39374, PHB5H33434
Dell Monitor P2417H	CN0KH09GQDC0086M5F7B-A06 CN-0KH0NG-QDC00-83L-879L-A05
Dell Latitude 3480 Laptop	4Q424L2
Maxim iButton Programmer DS9490R# with DS1402	[DVS-Maxim-001] thru [DVS-Maxim-005]
APC Smart-UPS SMT1500	3S1806X01308
Dell X1026 Network Switch	E11W002
Enabling Devices Sip and Puff	[DVS-enabling devices-001] - [DVS-enabling devices-002]
Cyber Acoustics Headphones ACM-70	[DVS-cyber acoustics-001] - [DVS-cyber acoustics-002]
Enablemart # 88906 Rocker (Paddle) Switch	[DVS-paddle-001]
IOGEAR SDHC/microSDHC 0U51USC410 Card Reader	8632, 8633
Lexar USB 3.0 Dual-Slot Reader	24021564209347
ATI-USB Handset	06465020102-724 DVS-ATIUSB-001
ACS PC-Linked Smart Card Reader ACR39U	RR374-081395, RR374-046907
Dell PowerEdge R640	DP/N 0JKFH7

3.3 Test Materials

All test materials are required to be provided by **Dominion** for the performance of testing including, as applicable, test ballot layout and generation materials, test ballot sheets, test ballot cards and control cards, standard and optional output data report formats, and any other materials used in testing.

3.4 Deliverable Materials

Please see section 4.5.1 of this Certification Test Plan for the full list of documents delivered in the TDP.

4 TEST SPECIFICATIONS

The following are the specifications for testing to be conducted on the **Dominion D-Suite 5.5-A** voting system**.** The specifications contain details on the focus of testing, configuration(s), and the functions to be tested. Additional information is provided in the associated appendices.

4.1 Requirements

The **Dominion D-Suite 5.5-A** will be tested to the approved VVSG 1.0 requirements. Modifications made to the **Dominion D-Suite 5.5-A** voting system are detailed in section "1.1.2 Modifications" and dictate evaluation against the following pertinent VVSG requirements:

- 2.4.3 Producing Reports
- 2.1.4 Integrity
- 2.1.6 Election Management System
- 5.2 Software Design and Coding Standards
- 7.4 Software Security
- 9.7.1 Physical Configuration Audit
- 9.7.2 Functional Configuration Audit

4.2 Hardware Configuration and Design

The **Dominion D-Suite 5.5-A** voting system, as declared in the application for certification submitted to the EAC, consists of:

- An EMS workstation with minimum requirements of the following:

  EMS Express Server Hardware Configuration:
  - Workstation class computer
  - Dual quad core CPU (Intel i5 series)
  - 16 GB RAM minimum
  - Dual 500 GB in RAID 1 mode (mirror)
  - DVD reader
  - Smart UPS
  - USB Compact Flash card reader
  - USB iButton Security Key reader

EMS Express Client Hardware Configuration:
- Workstation class computer
- Single or Dual quad core CPU (Intel i5 series)
- 8 GB RAM minimum
- 500 GB HDD minimum
- DVD reader
- USB Compact Flash card reader
- USB iButton Security Key reader

EMS Standard Server Hardware Configuration:
- Server class computer
- Dual quad core CPU (Intel Xeon E5 series)
- 32 GB RAM minimum
- Dual 1TB in RAID 1 mode, and 4x 1TB in RAID 10 mode
- Dual power supply
- DVD reader
- Smart UPS

EMS Standard Client Hardware Configuration:
- Workstation class computer
- Single or Dual quad core CPU (Intel i5 series)
- 8 GB RAM minimum
- 500 GB HDD minimum
- DVD reader
- USB Compact Flash card reader
- USB iButton Security Key reader

- At the precinct level, optical scanners and ballot marking devices are employed.
- The central count location employs a high-speed COTS scanner for tabulation of absentee ballots.

4.3 Software System Functions

The **Dominion D-Suite 5.5-A** system operations documentation has been reviewed in conjunction with the Supported Functionality Declaration provided by the manufacturer. Based on this review, the applicable system functions have been identified for testing. The following key areas of voting system functionality will be evaluated during test case design.

4.4 System-level Test Design

Testing of the System involves exercising the specific functions of each component of a voting system as well as the entire voting system. Testing will focus on the functionality of an election management system, the polling place devices, and

devices required for communications and data loading and will then focus on functionality of the integrated voting system.

- **Election Validations** - Election suites are created to replicate each type of election that can be implemented by the jurisdiction. Within the election types, pertinent voting variations that are applicable to that type of election will be validated and verified. Each suite will have a particular focus in order to test the voting system's implementation of a given requirement or set of requirements.
    - **General** - A general election designed to test all variations of the Pennsylvania Straight Party Method, to ensure all modifications and Straight Party functionality are working correctly as documented, and in accordance with the VVSG 1.0 requirements.
    - **Closed Primary** - An Integration Test Suite designed to verify proper integration of system components will be conducted using a Closed Primary.

4.5 TDP Evaluation

SLI is completing an assessment of the deliveries of the Technical Data Package for **Dominion D-Suite 5.5-A** against the **Dominion D-Suite 5.5-A** TDP. All modifications to previously reviewed documentation will be reviewed. Hardening procedures will be thoroughly reviewed to ensure the process is accurate, fully documented, and that any changes made from the documents in the previous version of the system TDP have been reviewed by a Security Test Specialist.

Any subsequent re-deliveries of the TDP items will be the result of fixes to discrepancies identified in the remaining FCA or PCA activities, or due to updates to the hardening procedures as a result of recommendations based on the findings from the penetration test performed for Pennsylvania.

SLI will conduct a PCA review of all vendor traced documents submitted for review in the delivery of the **Dominion D-Suite 5.5-A** TDP. These include:

Table 7 – TDP Documents

Doc. #	Description	Version
2.05	Democracy Suite Adjudication Software Design and Specification	5.5-A::117
2.08	Democracy Suite Adjudication System Operation Procedures	5.5-A::166
2.09	Democracy Suite Adjudication System Maintenance Manual	5.5-A::95
2.02	Democracy Suite System Overview	5.5-A::155
2.06	Democracy Suite System Security Specification	5.5-A::563
2.07	Democracy Suite System Test and Verification	5.5-A::192
2.10	Democracy Suite Personnel Deployment and Training Requirements	5.5-A::128

Doc. #	Description	Version
2.11	Democracy Suite Configuration Management Process	5.5-A::373
2.12	Democracy Suite Quality Assurance Program	5.5-A::156
2.13	Democracy Suite System Change Notes	5.5-A::155
2.03	Democracy Suite EMS Functional Description	5.5-A::372
2.05	Democracy Suite EMS Software Design and Specification	5.5-A::326
2.08	Democracy Suite EMS System Operations Procedures	5.5-A::723
2.09	Democracy Suite EMS System Maintenance Manual	5.5-A::143
	Democracy Suite EMS System Installation and Configuration Procedure	5.5-A::334
2.03	Democracy Suite ImageCast Central Functionality Description	5.5-A::180
2.05	Democracy Suite ImageCast Central Software Design and Specification	5.5-A::119
2.08	Democracy Suite ImageCast Central System Operation Procedures	5.5-A::209
	Democracy Suite ImageCast Central Installation and Configuration Procedure	5.5-A::184
2.03	Democracy Suite ImageCast Precinct Functionality Description	5.5-A::176
2.04.1	Democracy suite ImageCast Precinct System Hardware Characteristics	5.5-A::92
2.04	Democracy Suite ImageCast Precinct System Hardware Specification	5.5-A::147
2.05	Democracy Suite ImageCast Precinct Software Design and Specification	5.5-A::152
2.08	Democracy Suite ImageCast Precinct System Operation Procedures	5.5-A::273
2.09	Democracy Suite ImageCast Precinct System Maintenance Manual	5.5-A::121
2.03	Democracy Suite ImageCast X Functionality Description	5.5-A::96
2.05	Democracy Suite ImageCast X Software Design and Specification	5.5-A::98
2.08	Democracy Suite ImageCast X System Operation Procedures	5.5-A::85
2.09	Democracy Suite ImageCast X System Maintenance Manual	5.5-A::76
	Democracy Suite ImageCast X Installation and Configuration Procedure	5.5-A::87
	Democracy Suite ImageCast Adjudication User Guide	5.5-A::143
	Canon imageFORMULA DR-G1130 DR-G1100 User Manual	
	Canon imageFORMULA DR-M160-II User Manual	
	Democracy Suite Election Data Translator User Guide	5.5-A::93
	Democracy Suite EMS Audio Studio User Guide	5.5-A::39
	Democracy Suite EMS Election Event Designer User Guide	5.5-A::321
	Democracy Suite EMS Results Tally and Reporting User Guide	5.5-A::145
	Democracy Suite ImageCast Central User Guide	5.5-A::129
	Democracy Suite ImageCast Precinct User Guide	5.5-A::57

Doc. #	Description	Version
	Democracy Suite ImageCast Voter Activation User Guide	5.5-A::56
	ImageCast X User Guide	5.5-A::252
	Dell Latitude E7450 Owner's Manual	Rev. A00
	Cyber Acoustics ACM-70B Stereo Headphones Product Sheet	
	Democracy Suite ImageCast C++ Coding Standard	5.5-A::55
	Democracy Suite C# Automated Code Review Process	5.5-A::50
	Dell Latitude E7450/Latitude 7450 Regulatory Compliance Sheet	Revision A09
	Dell OptiPlex 9020 AIO Regulatory Compliance Sheet	Revision A09
	Dell OptiPlex 9030 AIO Regulatory Compliance Sheet	Revision A09
	Dell Networking X-Series Specification Sheet	Version 1.9
	Dell OptiPlex 9020 All-in-One Technical Specification Sheet	
	Dell OptiPlex 9030 All-in-One Technical Specification Sheet	
	Dell OptiPlex 3050 All-in-One Regulatory Compliance Sheet	Revision A11
	Google Java Style Dominion XML	1.0
	Dominion Voting Systems Java Coding Standards	Version: 1.0
	Dominion Voting Systems JavaScript Coding Standards	Version: 1.0
	ICX Machine Configuration File (MCF) Parameters Settings	5.5-A::31
	Democracy Suite ImageCast Device Configuration Files	5.5-A::101
	Democracy Suite ImageCast Printing and Finishing Specification	5.5-A::95
	Democracy Suite ImageCast Total Results File Format	5.5-A::58
	Democracy Suite ImageCast Precinct Election Definition Files	5.5-A::78
	Democracy Suite ImageCast Precinct Extracting Firmware Contents	5.5-A::37
	Democracy Suite ImageCast Precinct Firmware Update Procedure	5.5-A::64
	Democracy Suite ImageCast Precinct Level One (L1) Maintenance Manual	5.5-A::63
	Democracy Suite ImageCast Precinct Technical Guide	5.5-A::48
	Usability Test Report of ImageCast Precinct 5.0 with 36 Participants for VVSG 1.0	5.0::10
	Usability Test Report of ImageCast X 5.0 with 36 Participants for VVSG 1.0	5.0::13
	YEDU.E95463 Uninterruptible Power-supply Equipment Sheet	2011-11-08
	Dell Latitude E7440 Regulatory Compliance Sheet	Revision A09
	Dell Latitude E7470 Owner's Manual	Rev. A02
	Dell Latitude 3480 Regulatory Compliance Sheet	Revision A11
	Dell PowerEdge R630 Regulatory Compliance Sheet	Revision A10
	Dell Precision T1700 MT Regulatory Compliance Sheet	Revision A09
	Dell PowerConnect 2808 Product Safety. EMC, and Environmental DataSheet	

Doc. #	Description	Version
	Dell PowerConnect 2816 Product Safety. EMC, and Environmental DataSheet	
	SMC1500 APC Smart-UPS Product Data Sheet	
	Smart Pro SM1500 Datasheet	
	APC Smart-UPS 230V Product Information Sheet	
	HP M402dn Datasheet	Rev. 2
	HP M402dne Datasheet	May 2016
	Dell Latitude 3480 Owner's Manual	Rev. A00
	Dell Latitude 3470 Owner's Manual	Rev. A00
	Dell Precision T3420 Owner's Manual	Rev. A00
	aValue HID-21V-BTX-A1R User Manual	Revision 2.0
	aValue SID-21V-Z37-A1R Data Sheet	Revision 1.0
	aValue SID-21V Quick Reference Guide	
	aValue SID-21V Fact Sheet	
	APC Installation and Operation Back-UPS Pro BR1000G	EN 990-3804B 10/2014
	APC Smart-UPS SMT1500 Operation Manual	EN 990-3534D 03/2013
	APC Back-UPS BE600M1 User Guide	EN-990-5679 09/2015
	Dell OptiPlex 7440 All-In-One Owner's Manual	Rev. A01
	Dell OptiPlex 3050 All-In-One Owner's Manual	Rev. A00
	Dell P2417H Monitor User's Guide	Rev. A01
	Dell P2217H Monitor User's Guide	Rev. A05
	Dell PowerEdge R630 Owner Manual	Rev. A03
	Lexar Pro USB 3 Dual Slot Reader	Rev A
	Democracy Suite Windows Build Document	5.5-A::33
	Democracy Suite ImageCast Precinct Firmware Build and Install	5.5-A::86
	ImageCast X Build	5.5-A::53
	Dell PowerEdge R640 Technical Guide	Rev. A00
	Dell PowerEdge R640 Owner's Manual	Rev. A01
	Dell Latitude 3480 Owner's Manual	Rev. A00
	Dell OptiPlex 3050 All-In-One Owner's Manual	Rev. A01

4.6 Source Code Review

4.6.1.1 Source Code Review

The certification campaign for the **Dominion D-Suite 5.5-A** voting system includes software, firmware, and configuration files from **Dominion D-Suite 5.5** that have been modified by and are proprietary to **Dominion**. SLI will conduct a source code review of all modified source code in the delivery of the voting system TDP for **Dominion D-Suite 5.5-A** for compliance to the VVSG 1.0, Volume 2, Section 6.6.

Source Code Review Tools utilized by SLI include:

- Module Finder: an SLI proprietary application used to parse module names from C/C++ and VB code and populate the identified module names into the review documents
- ExamDiff Pro: a commercial application used to compare revised code to previously reviewed code

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

COTS operating systems and software used in the voting system will be verified to be authentic and unmodified in the **Dominion D-Suite 5.5-A** test campaign.

4.7 Trusted Build

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

- Preparation for the Trusted Build - Obtaining and reviewing **Dominion's** procedure for constructing the build platform, verifying the target build platform, and acquiring and verifying the necessary materials.
- Execution of the Trusted Build – SLI will perform the Trusted Build by using the step-by-step build procedure, as provided by **Dominion Voting Systems** to create a pristine build environment. SLI records and ascertains the following items throughout the build process:
    - Build environment and file hashes at various key points
    - Build environment hardware characteristics
    - Build results from code compilation and file hashes
    - Final software install files and file hashes
    - Build virtual machine files

- Deliverables to Testing – Upon completion of the Trusted Build, certain items are sent to the SLI test group. The final result will be a media containing the following:
    - Final software install files
    - Hash values to validate install files
- Final Record Keeping and Archiving Procedures – At the conclusion of the Trusted Build process, SLI completes all final record keeping and archiving procedures at SLI's facility. This record keeping includes any unique identifiers, results of the build with version numbers and dates and descriptions of all hashes and images in the repository.

4.8 Standard VSTL Test Methods and Uncertainty of Test Data Measurement

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

5 TEST DATA

Test data for the **Dominion D-Suite 5.5-A** voting system has been compiled such that all functionality declared will be tested to determine conformance to the standards.

5.1 Data Recording

SLI has evaluated the system functionality, as described by manufacturer technical documentation, as well as requirements as listed in the EAC VVSG 1.0 and made determinations as to expected results of all data inputs into the **Dominion D-Suite 5.5-A** voting system. This includes:

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

The data is contained in one master data record, including each input and each expected output. This data is incorporated into the appropriate test suite, populating test modules with exact expected data for the function being tested.

Testing information is recorded in the test suites, as well as in test notebooks, which are utilized according to SLI's standard lab procedure *SLP-VC-30 - Test Notebooks*.

5.2 Test Data Criteria

SLI has evaluated the system functionality as described by manufacturer technical documentation, as well as requirements as listed in the EAC VVSG 1.0, and made determinations as to expected output of all data inputs into the **Dominion D-Suite 5.5-A** voting system. A data matrix has been recorded into one master data record that couples data inputs to their expected output, as determined above. The system's execution shall be measured against the expected results.

6 TEST PROCEDURE AND CONDITIONS

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

6.1 Facility Requirements

Four secure labs are available with appropriate power supply and space to accommodate the various configurations defined within this Certification Test Plan. Temperature/humidity gauges will be employed in order to determine the appropriate conditions exist during testing.

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

- Temperature: 64°F - 79°F (17.7°C - 26.1°C)
- Relative Humidity: 20 to 90%
- Atmospheric Pressure: Local Site Pressure

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

6.2 Test Setup

Configurations of the **Dominion D-Suite 5.5-A** will be deployed that conform to each specific test suite's needs. Some configurations will consist of standalone implementations, while other configurations will utilize networked implementations of

various applications. In all instances, the **Dominion D-Suite 5.5-A** documentation will be followed in the setup of the configurations.

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

6.3 Test Sequence

While there is no required sequence for performing voting system certification testing and audits, there are prerequisite tasks for some testing. Any needed prerequisites are contained within the suite for that test.

6.4 Test Operations Procedures

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

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

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

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

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

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

7 Approval Signature

Traci Mapps
VSTL Director
December 15th, 2018

End of Certification Test Plan

Exhibit B

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF** **J. ALEX HALDERMAN** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. My July 1, 2021, expert report describes numerous security vulnerabilities in Georgia's Dominion ICX BMDs. These include flaws that would allow attackers to install malicious software on the ICX, either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems. They are not general weaknesses or theoretical problems, but

rather specific flaws in the ICX software, and I am prepared to demonstrate proof-of-concept malware that can exploit them to steal votes cast on ICX devices.

3. Some of these critical vulnerabilities could be at least partially mitigated through changes to the ICX software if Dominion implemented such changes and jurisdictions deployed them. However, it would likely take months for Dominion to assess the problems, develop responsive software updates, test them, obtain any necessary approvals from the EAC and state-level certification authorities, and distribute the new software to states, as well as additional time for localities to install the changes. But Dominion cannot begin this process, because (to my knowledge) they have yet to learn what is in my report.

4. My analysis also concludes that the ICX is very likely to contain other, equally critical flaws that are yet to be discovered. Jurisdictions can mitigate this serious risk through procedural changes, such as reserving BMDs for voters who need or request them. Election officials cannot make an informed decision about such urgent policy changes or any other mitigations until they have assessed the technical findings in my report. However, to my knowledge, the Georgia Secretary of State's Office has yet to even request access to it, despite Plaintiffs' repeated offers to make it available to appropriate individuals at the Secretary's Office.

5. Nor do these problems affect Georgia alone. In 2022, the ICX will be used in parts of 16 states.[1] Nevada will use it as the primary method of in-person voting in certain areas of the state. Louisiana is slated to use it for early voting in a DRE configuration where there is not even a paper trail. It will be used for accessible voting in Alaska and large parts of Arizona, California, Colorado, and Michigan. It will also see some use in parts of Illinois, Kansas, Ohio, Missouri, New Jersey, Pennsylvania, Tennessee, and Washington State. Officials in these jurisdictions too must act to update the software and their procedures, but they cannot do so without information about the problems. Continuing to conceal those problems from those who can—and are authorized to—address them, to the extent possible, serves no one and only hurts voters (and heightens the risk of compromise in future elections).

6. The most effective way to ensure that the necessary information gets to the parties responsible (without also falling into the wrong hands) would be to share my report with the Cybersecurity and Infrastructure Security Agency (CISA), which operates a Coordinated Vulnerability Disclosure (CVD) program for just this purpose. CISA is a federal agency that collaborates with state and local governments, election officials, federal partners, and vendors to manage risks to U.S. election

---

[1] See Verified Voting, "Verifier Search – November 2022," https://verifiedvoting.org/verifier/#mode/search/year/2022/model/ImageCast%20X.

infrastructure.[2] Under CISA's CVD process, agency staff would independently validate the vulnerabilities, work with Dominion to develop software updates as necessary, and facilitate sufficient time for affected states and localities to apply mitigation strategies.[3] CISA strives to disclose "accurate, neutral, objective information focused on technical remediation and mitigation" and to "correct misinformation where necessary,"[4] making it well qualified to coordinate the disclosure of such sensitive vulnerabilities.

7. Geoff Hale, Director of CISA's Election Security Initiative, has confirmed to me that, if the Court permits it, the agency would be willing to receive my expert report and carry out coordinated vulnerability disclosure activities as appropriate (see Exhibit 1). Mr. Hale requests that I and my assistant Drew Springall be available for consultation with CISA during the CVD process, which we would be willing to do subject to the Court's permission.

8. Informing responsible parties about the ICX's vulnerabilities is becoming more urgent by the day. Foreign or domestic adversaries who are intent on

---

[2] Cybersecurity and Infrastructure Security Agency, "Election Infrastructure Initiative," https://www.cisa.gov/election-security.

[3] Cybersecurity and Infrastructure Security Agency, "Coordinated Vulnerability Disclosure Process," https://www.cisa.gov/coordinated-vulnerability-disclosure-process.

[4] *Id.*

attacking elections certainly could have already discovered the same problems I did, yet Georgia's 2022 primaries are less than nine months away, and other states that use the ICX will conduct high-profile elections even sooner. It is important to recognize the possibility that nefarious actors already have discovered the same problems I detail in my report and are preparing to exploit them in future elections. Providing my report to CISA through its CVD program will ensure that Dominion and affected jurisdictions are able to begin appropriate mitigations as soon as possible. Continuing to withhold my report from CISA puts voters and election outcomes in numerous states at unnecessary, and avoidable, risk.

9. I understand that State Defendants object to disclosure to CISA on the argument that my report should be used only for this lawsuit. But this ignores the implications of my report and my role in this matter. I am not a party to this lawsuit. I am an independent expert who was engaged to conduct an impartial assessment of the security and reliability of the Dominion BMD system, using (in part) election equipment that the Court ordered I be provided. I have done that, as reflected in my lengthy, detailed report and other submissions in this matter. As an independent expert and member of the election integrity community, I have a professional obligation to take appropriate steps to ensure that the severe vulnerabilities my report describes are properly remediated, to the extent possible, and that those tasked with

election security and administration across the country have the information they need to make responsible, informed decisions about election procedures, including the equipment used, the manner and purposes for which it is used (including whether it is used at all), the steps needed to secure that equipment and other aspects of the election systems in which it is used, and more. In short, my professional obligations do not end at the boundaries of this lawsuit, nor do the serious risks to voters and elections that my report discusses in depth. Additionally, I can imagine no prejudice to anyone in this lawsuit (or beyond) from disclosure of my report to CISA, nor am I aware of any claim of prejudice from any of the parties.

10. I of course have complied, and will continue to comply, with all directives from the Court regarding disclosure of my work in this matter. I submit this declaration to explain why I believe disclosure of my report to CISA is critically important (and not just for Georgia) and to respectfully ask that the Court allow that disclosure, rather than accept State Defendants' position that my findings must not be shared beyond the confines of this lawsuit, including with those who are authorized to address the vulnerabilities with the ICX and stand ready to do so. If my findings regarding the ICX actually present no meaningful risks to voters and election outcomes and therefore require no remediation, as I gather State Defendants would have the Court believe, CISA is well positioned to determine that. If, on the other

hand, my findings do warrant remediation, as I believe they do, then CISA is well positioned to work with Dominion and the appropriate authorities around the country to implement remedial measures. I can see no reason to prevent (or further delay) that important work for future elections. And I note that none of State Defendants' experts have disputed my findings regarding the ICX machines. Only Dr. Juan Gilbert has responded to my sealed report, and he has not examined the machines (or used them) to my knowledge.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 21st day of September, 2021 in Ann Arbor, Michigan.

J. ALEX HALDERMAN

EXHIBIT 1

Gmail **J. Alex Halderman <halderman@gmail.com>**

Vulnerability Disclosure

Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov> Thu, Aug 19, 2021 at 12:15 PM
To: "J. Alex Halderman" <jhalderm@umich.edu>
Cc: Andrew Springall <andrew.springall@gmail.com>

Prof. Halderman,

Thank you for your email. Yes, CISA would be willing to receive the report regarding possible vulnerabilities in election infrastructure for inclusion in CISA's Coordinated Vulnerability Disclosure (CVD) process and would carry out any further coordinated disclosures activities as appropriate. As we share on our public website (https://www.cisa.gov/coordinated-vulnerability-disclosure-process), CISA's CVD program coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s). Note that part of our process may also involve validating any alleged vulnerabilities, planned mitigations, remediations, or patches with the security researcher who discovered the alleged vulnerability, so we would appreciate if you could continue to be available for consultation during the CVD process as well.

As shared on our website, please submit any vulnerability reports for CVD coordination using the form here: https://www.kb.cert.org/vuls/report/

Best,

Geoff

From: J. Alex Halderman <jhalderm@umich.edu>
Sent: Wednesday, August 18, 2021 4:37 PM
To: Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov>
Cc: Andrew Springall <andrew.springall@gmail.com>
Subject: Vulnerability Disclosure

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Dear Mr. Hale,

We are writing to you in your capacity as Director of the Election Security Initiative at the federal Cybersecurity and Infrastructure Security Agency (CISA).

We understand that the Election Security Initiative at CISA works to ensure the physical security and cybersecurity of the systems and assets that support the Nation's elections, including through detection and prevention, information sharing and awareness, and incident response.

As you may be aware from recent press reports, one of us (Halderman) is presently serving as an expert witness for the plaintiffs in Curling v. Raffensperger (Civil action no. 1:17-CV-2989-AT, N.D. Ga.), a case that concerns the security of Georgia's election system. A year ago, the court granted plaintiffs access to an ICP ballot scanner and ICX ballot marking device as used in Georgia in order to test their security. Following months of analysis, on July 1, Dr. Halderman submitted an expert report that describes several very serious vulnerabilities we found in the equipment, which, to our knowledge, have not been previously documented or disclosed.

Given the nature of the vulnerabilities and the time that would be necessary to mitigate them before the 2022 midterm elections, we believe it is critical for Dominion and affected jurisdictions (which include Georgia and parts of many other states) to begin taking responsive action soon. It is also vitally important to prevent information sufficient to exploit the vulnerabilities from falling into the wrong hands, and to avoid fueling election-related misinformation if possible.

Currently, disclosure of the expert report to anyone other than outside litigation counsel for the parties is strictly prohibited by the Court’s protective order and by recent directives from the judge. However, if permitted by the Court, we would like to share the report with CISA and ask your agency to carry out appropriate further disclosure of the information it contains to Dominion and affected jurisdictions as you see fit, under CISA's coordinated vulnerability disclosure (CVD) program (https://www.cisa.gov/coordinated-vulnerability-disclosure-process).

We understand that under this process, CISA will work with the vendor (Dominion) for mitigation development and the issuance of patches or updates and to facilitate sufficient time for affected end users to obtain, test, and apply mitigation strategies. We further understand that CISA strives to disclose "accurate, neutral, objective information focused on technical remediation and mitigation" and to "correct misinformation where necessary".

Please confirm that CISA would be an appropriate agency to handle coordinated vulnerability disclosure for election infrastructure under these circumstances, and that you would be willing to receive the report (subject to the Court's permission) and carry out further disclosures as you deem appropriate.

Sincerely,

J. Alex Halderman

Drew Springall