700 Boulevard South
Suite 102
Huntsville, AL 35802
Phone (256)713-1111
Fax (256)713-1112

Test Report for EAC 2005 VVSG 1.0 Certification Testing Dominion Voting Systems Democracy Suite (D-Suite) Version 5.0-A Voting System

EAC Project Number: DVS1701

Version: Rev. E

Date: 8/11/17

U.S. Election Assistance Commission

VSTL

EAC Lab Code 1501

NVLAP®

NVLAP LAB CODE 200908-0

SIGNATURES

Approved by: Michael L Walker 8/11/17

Michael Walker, VSTL Project Manager — Date

Approved by: Wendy Owens 8/11/17

FOR Wendy Owens, VSTL Program Manager — Date

REVISIONS

Revision	Description	Date
NR	Initial Release	6/23/17
A	Updates per EAC Comments	7/18/17
B	Additional updates per EAC Comments to provide clarification and corrections	7/19/17
C	Removed highlights, updated EMS build document version in Table 3-1	7/21/17
D	Corrected typo in ICVA version	8/10/17
E	Corrected typo of ICVA version in Trusted Build	8/11/17

TABLE OF CONTENTS

1.0 INTRODUCTION

The purpose of this Test Report is to document the procedures that Pro V&V, Inc. followed to perform certification testing during a system modification campaign for the Dominion Voting Systems Democracy Suite (D-Suite) 5.0-A Voting System to the requirements set forth for voting systems in the U.S. Election Assistance Commission (EAC) 2005 Voluntary Voting System Guidelines (VVSG), Version 1.0. Prior to submitting the voting system for testing, Dominion Voting Systems submitted an application package to the EAC for certification of the D-Suite 5.0-A Voting System. The application was accepted by the EAC and the project was assigned the unique Project Number of DVS1701.

1.1 Description and Overview of EAC System Being Modified

The EAC Certified System that is the baseline for the submitted modification is described in the following subsections. All information presented was derived from the previous Certification Test Report, the EAC Certificate of Conformance and/or the System Overview.

The baseline system for this modification is the D-Suite 5.0 Voting System. Detailed descriptions of the D-Suite 5.0 test campaign are contained in Pro V&V Report No.TR-01-01-DVS-2016-01.01 Rev. D, which is available for viewing on the EAC's website at www.eac.gov and the As-Run Test Plan submitted as Attachment B of this report.

The D-Suite 5.0 Voting System is a paper-based optical scan voting system with a hybrid paper/DRE option consisting of the following major components: The Election Management System (EMS), the ImageCast Central (ICC), the ImageCast Precinct (ICP), and the ImageCast X (ICX).

Election Management System (EMS)

The D-Suite 5.0 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.

Front-end/Client applications:

- EMS Adjudication: Represents the client component 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. *(Note: The EMS Adjudication feature is optional)*

- EMS Audio Studio: A client application that 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.

- 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: A client application that integrates election definition functionality together with ballot styling capabilities and represents a main pre-voting phase end-user application

- ImageCast Voter Activation: An application, installed on a workstation or laptop at the polling place, which 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: A client application that integrates election results acquisition, validation, tabulation, reporting, and publishing capabilities and represents the main post-voting phase end-user application.

Back-end/Server applications:

- EMS Adjudication Service: Represents a server side application which provides ballot information such as contests, candidates and their coordinates from EMS to the Adjudication application.

- EMS Application Server: Represents a server side application responsible for executing long running processes, such as rendering ballots, generating audio files and election files, etc.

- EMS Database Server: Represents a server side RDBMS repository of the election project database which holds all the election project data, including pre-voting and post-voting data.

- EMS Data Center Manager: A server application that represents a system level configuration application used in EMS back-end data center configuration.

- EMS Election Device Management: Application used for production and programming of election files, and other accompanying files, for ImageCast X terminals.

- EMS File System Service: A back-end application that acts as 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: Represents a server side file repository of the election project file based artifacts, such as ballots, audio files, reports, log files, election files, etc.

- Smart Card Helper Service: A service that is installed on a workstation or laptop at the polling place, and 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.

For ballot scanning functionality the ICP scans marked paper ballots, interprets voter marks on the paper ballots and stores the ballots for tabulation when the polls are closed.

Second Chance voting refers to scenarios in which an error has been detected on the voter's paper ballot (e.g., blank ballot, undervoted ballot, overvoted ballot, misread ballot, cross-over voted ballot), and the ICP notifies the voter by displaying a message or providing an audio visual cue, that one of these situations has been detected, and offers the voter an opportunity to reject and fix their ballot, or to cast the ballot as-is.

Accessible voting allows voters with disabilities to listen to an audio representation of a ballot and use a hand held controller called an Audio Tactile Interface (ATI) to make vote selections, which are then saved directly to the ICP when the voter casts their Accessible Voting ballot.

The Ballot Review feature allows a voter to review their vote selections using an audio or visual representation, which displays or presents the voter with a complete listing of all contests contained on the ballot and an indication of the results which will be recorded for each contest once the voter's ballot is cast.

The Tabulation of paper ballots and Accessible Voting ballots cast by voters is performed when the polls are closed on the ICP unit and the unit tabulates the results, generates results files for aggregation into RTR, and prints a results report containing the results of the ballots cast.

For poll worker functions the ICP contains a small touch-screen LCD to allow the poll worker to initiate polling place activities, diagnostics and reports.

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 a solution that 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.

The ICX is a proprietary application which runs on any of the tablets listed in Table 1-21.

1.1.1 Details of System Tested

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

The system tested for this test campaign was the Democracy Suite (D-Suite) 5.0-A Voting System. The D- Suite 5.0-A Voting System is a modified voting system configuration that

introduces updated OpenSSL FIPS 140-2 validated cryptographic modules to the certified baseline Democracy Suite 5.0 system configuration. The following tables provide details of the 5.0-A system and its components.

Table 1-1. Democracy Suite 5.0-A EMS Software Component Descriptions

Software	Version	Filename	Configuration	
			Standard	Express
EMS Election Event Designer (EED)	5.0.16.1	setup.exe: EED_FED_CERT_Setup_x64.msi	X	X
EMS Results Tally and Reporting (RTR)	5.0.16.1	setup.exe: RTR_FED_CERT_Setup_x64.msi	X	X
EMS Application Server	5.0.16.1	setup.exe: APPS_FED_CERT_Setup_x64.msi	X	X
EMS File System Service (FSS)	5.0.16.1	setup.exe: FSSSetup.msi	X	X
EMS Audio Studio (AS)	5.0.16.1	setup.exe: EMSAudioStudioSetup.msi	X	X
EMS Data Center Manager (DCM)	5.0.16.1	DemocracySuiteEMS_DCM.exe	X	X
EMS Election Data Translator (EDT)	5.0.16.1	setup.exe: EDTSetup_x86.msi EDTSetup_x64.msi	X	X
ImageCast Voter Activation (ICVA)	5.0.16.1	setup.exe: ICVASetup.msi	X	X
EMS Adjudication (Adj)	5.0.0.44402	DVS ImageCast Adjudication Client Setup.msi	X	X
EMS Adjudication Service	5.0.0.44402	DVS Adjudication Services Setup.msi	X	X
EMS Election Data Manager (EDM)	5.0.6366.25253	setup.exe: EdmInstaller.msi	X	X
Smart Card Helper Service	5.0.6366.25232	setup.exe: SmartCardServiceSetup.msi	X	X

Table 1-2. Democracy Suite 5.0-A ICP Software Component Descriptions

Firmware/Software	Version	Filename
Election Firmware	5.0.2-US	cf2xx.sig
Firmware Updater	5.0.2-US	firmUp.enc
Firmware Extractor	5.0.2-US	FirmwareExtract.enc
Kernel (uClinux)	5.0.2-US	image.bin.gz
Boot Loader (COLILO)	20040221	colilo.bin
Asymmetric Key Generator	5.0.2-US	Keygen.enc

Table 1-2. Democracy Suite 5.0-A ICP Software Component Descriptions *(continued)*

Firmware/Software	Version	Filename
Asymmetric Key Exchange Utility	5.0.2-US	KeyExchange.enc
Firmware Extractor (Uses Technician Key)	5.0.2-US	TechExtract.enc

Table 1-3. Democracy Suite 5.0-A ICC Software Component Descriptions

Firmware/Software	Version	Filename
ImageCast Central Application	5.0.2-0001	ICCSetup_v5.0.0.15.exe

Table 1-4. Democracy Suite 5.0-A ICX Software Component Descriptions

Firmware/Software	Version	Filename
ICX Application	5.0-A.6366.2007	ICX.apk
ICX Security Certificate	N/A	icx_pkcs12.pfx
ICX Security Certificate Password	N/A	icx_pfx.pwd

Table 1-5. Democracy Suite 5.0-A EMS Client/Server Software Component Descriptions

Firmware/Software	Version	Filename	Configuration	
			Standard	Express
Microsoft Windows Server	2012 R2 Standard	Physical Media from Microsoft	X	
Microsoft Windows	8.1 Professional	Physical Media from Microsoft	X	X
.NET Framework	3.5	Physical Media from Microsoft	X	X
Microsoft Visual J#	2.0	vjredist64.exe vjredist.exe	X	X
Microsoft Visual C++ 2013 Redistributable	2013	vcredist_x64.exe vcredist_x86.exe	X	X
Java Runtime Environment	7u76	jre-7u76-windows-x64.exe jre-7u76-windows-i586.exe	X	X
Java Runtime Environment	8u77	jre-8u77-windows-x64.exe jre-8u77-windows-i586.exe	X	X
Microsoft SQL Server 2012 Standard	2012 Standard	Physical Media from Microsoft	X	
Microsoft SQL Server 2012 Service Pack 2	2012 SP2	SQLServer2012SP2-KB2958429-x64-ENU.exe	X	
Microsoft SQL Server 2012 SP2 Express with Advanced Services	2012 SP2	SQLEXPRADV_x64_ENU.exe		X

Table 1-5. Democracy Suite 5.0-A EMS Client/Server Software Component Descriptions *(continued)*

Firmware/Software	Version	Filename	Configuration	
			Standard	Express
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	X	X
Arial Narrow Fonts	N/A	ARIALN.TTF ARIALNB.TTF ARIALNBI.TTF ARIALNI.TTF	X	X
Maxim iButton Driver	4.04	install_1_wire_drivers_x86_v404.msi install_1_wire_drivers_x64_v404.msi	X	X
Adobe Reader DC	AcrobatDC	AcroRdrDC1501020060_en_US.exe	X	X
Microsoft Access Database Engine	2010	AccessDatabaseEngine.exe AccessDatabaseEngine_x64.exe	X	X
Open XML SDK 2.0 for Microsoft Office	2.0	OpenXMLSDKv2.msi	X	X

Table 1-6. Democracy Suite 5.0-A EMS Software Platform Unmodified COTS Component Descriptions

Firmware/Software	Version	Filename
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 Library for .NET	16.0	TXText Control.NET for Windows Forms 16.0.exe
SOX	14.3.1	sox.exe , libgomp-1.dll, pthreadgc2.dll, zlib1.dll
Log4net	1.2.10	log4net.dll, log4net.xml
NLog	1.0.0.505	NLog.dll
iTextSharp	5.0.5.0	itextsharp.dll
OpenSSL	1.0.2K	openssl.exe, lebeay32.dll, ssleay32.dll
SQLite	1.0.65.0	System.Data.SQLite.DLL (32-bit and 64-bit)

Table 1-6. Democracy Suite 5.0-A EMS Software Platform Unmodified COTS Component Descriptions *(continued)*

Firmware/Software	Version	Filename
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)
PdfToImage.dll	1.2	PdfToImage.dll
SharpSSh package	1.1.1.13	Tamir.SharpSSH.dll, Diffie.Hellman.dll, Org.Mentalis.Security.dll
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	4.3.1	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

Table 1-7. Democracy Suite 5.0-A ICP Unmodified COTS Component Descriptions

Firmware/Software	Version	Filename
OpenSSL	1.0.2K	Openssl-1.0.2K.tar.gz
OpenSSL FIPS Object Module	2.0.10 (Cert 1747)	Openssl-fips-2.0.10.tar.gz
PNG Reference Library	1.2.24	libpng-1.2.24.tar.gz
Zlib	1.2.3	Zlib-1.2.3.tar.gz

Table 1-8. Democracy Suite 5.0-A ICX (Includes EDM) Unmodified COTS Component Descriptions

Firmware/Software	Version	Filename
ASP.NET AJAX Control Toolkit	15.1.4.0	AjaxControlToolkit.Installer.15.1.4.0.exe
Entity Framework	6.1.3.net45	entityframework.6.1.3.nupkg
Ionics Zip Library	1.9.1.8	DotNetZipLib-DevKit-v1.9.zip
NLog Library	1.0.0.505	NLog-1.0-Refresh-bin.zip

Table 1-8. Democracy Suite 5.0-A ICX (Includes EDM) Unmodified COTS Component Descriptions *(continued)*

Firmware/Software	Version	Filename
SQLite	1.0.98.0	sqlite-netFx451-binary-bundle-x64-2013-1.0.98.0.zip
Google Text-to-Speech Engine	3.8.16	ARM: com.google.android.tts_3.8.16-210308160_minAPI15(armeabi-v7a)(nodpi).apk x86: com.google.android.ttscom.google.android.tts_3.8.16-210308163_minAPI15(x86)(nodpi).apk

Table 1-9. Democracy Suite 5.0-A ICC Software Build Library Source Code (Unmodified COTS)

Firmware/Software	Version	Filename
OpenSSL	1.0.2K	openssl-1.0.2K.tar.gz
OpenSSL FIPS Object Module	2.0.10 (Cert 1747)	openssl-fips-2.0.10.tar.gz

Table 1-10. Democracy Suite 5.0-A ICC Runtime Software Components (Unmodified COTS)

Firmware/Software	Version	Filename
1-Wire Driver (x86)	4.04	install_1_wire_drivers_x86_v404.msi
1-Wire Driver (x64)	4.04	install_1_wire_drivers_x64_v404.msi
Kofax VRS	4.5 Build 269	Kofax_VRS4_50_269_DR-G1130.iso
Kofax VRS Service Pack 1	4.5.1	vrs45sp1setup.exe
Canon DR-G1130 Driver	1.2 SP4	Physical Media from Canon
Canon DR-G1130 Component Installer	4.50	CI-DR-G1130.exe
Visual C++ 2013 Redistributable (x86)	12.0.30501	vcredist_x86.exe

Table 1-11. Democracy Suite 5.0-A ICP Modified COTS Software Component Descriptions

Firmware/Software	Version	Filename
uClinux	20070130	uClinux-dist-20070130.tar.gz
COLILO Bootloader	20040221	Colilo20040221.tar.gz

Table 1-12. Democracy Suite 5.0-A ICX Modified COTS Software Component Descriptions

Firmware/Software	Version	Filename
Zxing Barcode Scanner	4.7.5	BS-4.7.5.zip
SoundTouch	1.9.2	Soundtouch-1.9.2.tar.gz

Table 1-13. Democracy Suite 5.0-A EMS Software Build Environment Component Descriptions

Firmware/Software	Version	Filename
Windows 8.1 Professional	8.1	Physical Media from Microsoft
.NET Framework 3.5	3.5	Physical Media from Microsoft
Internet Information Server (IIS)	6	Physical Media from Microsoft
7-Zip	9.20 (64 Bit)	7z920-x64.msi
Visual Studio 2013 Premium	2013.5	vs2013.5_prem_enu.iso
ImgBurn	2.5.7.0	SetupImgBurn_2.5.7.0.exe
Infragistics NetAdvantage Win Forms 2011.1	2011.1	NetAdvantage_WinForms_20111.msi
Infragistics Net Advantage – WPF 2012.1	2012.1	NetAdvantage_WPF_20121.msi
TX Text Control 16.0.NET	16	TX Text Control.NET for Windows Forms 16.0.exe
Speex	1.0.4	speex_win32_1.0.4_setup.exe
Microsoft Visual J#	2.0	vjredist64.exe
iTextSharp	5.0.5	itextsharp-5.0.5-dll.zip
Ghostscript	9.0.4	gs904w32.exe gs904w64.exe
Nlog	1.0.0.505	NLog-1.0-Refresh-bin.zip
OneWireAPI.NET	4.0	1-wiresdkver400_beta2.zip
Lame	3.99.4	lame3.99.4-20120130.zip
Sox	14.3.1	sox-14.3.1-win32.zip
Avalon Framework	20020806	avalon-framework-cvs-20020806.jar.zip
Fop	0.20-5	fop-0.20.5.jar
Batik	0.20-5	batik-1.5-fop-0.20-5.jar
SharpSSH	1.1.1.13	SharpSSH.zip
SQLite	1.0.65.0	SQLite-1.0.65.0-binaries.zip
OpenSSL	1.0.2K	openssl-1.0.2K.tar.gz
OpenSSL FIPS Object Module	2.0.10 (Cert 1747)	openssl-fips-2.0.10.tar.gz

Table 1-13. Democracy Suite 5.0-A EMS Software Build Environment Component Descriptions
(continued)

Firmware/Software	Version	Filename
ActivePerl	5.20.2	ActivePerl-5.20.2.2002-MSWin32-x86-64int-299195.msi
Patch	2.5.9-7	patch-2.5.9-7-bin.zip
ISOnewspaper	30.4	ISOnewspaper30v4_gr.icc.zip
Ogg Vorbis Encoder	2.88	oggenc2.88-1.3.5-generic.zip
Ogg Vorbis Encoder	1.10.1	oggdecV1.10.1.zip
Prism Mvvm	1.1.1	prism.mvvm.1.1.1.nupkg
PDF Printing	2.9.5.2	PDFPrinting.zip
Entity Framework	6.1.3	entityframework.6.1.3.nupkg
WiX	3.10	Wix310.exe
Spreadsheet Light	3.4.3	spreadsheetlight.3.4.3.nupkg
Open XML SDK 2.0 for Microsoft Office	2.0	OpenXMLSDKv2.msi
Acrobat Reader	Acrobat DC	AcroRdrDC1501020060_en_US.exe
Arial Narrow Fonts	N/A	ArialNarrowFonts.zip
PdfToImage	1.2	ConvertPDF_source_1.2.zip

Table 1-14. Democracy Suite 5.0-A ICC Software Build Environment Component Descriptions

Firmware/Software	Version	Filename
NASM Assembler	2.09.07	nasm-2.09.07-win32.zip
OpenSSL	1.0.2K	openssl-1.0.2K.tar.gz
OpenSSL FIPS Object Module	2.0.10 (Cert 1747)	openssl-fips-2.0.10.tar.gz

Table 1-15. Democracy Suite 5.0-A EDM Software Build Environment Component Descriptions

Firmware/Software	Version	Filename
Ajax Control Toolkit	15.1.4	AjaxControlToolkit.Installer.15.1.4.0.exe
SQLite	1.0.98.0	sqlite-netFx451-binary-bundle-x64-2013-1.0.98.0.zip
Ionic	1.9.1.8	DotNetZipLib-DevKit-v1.9.zip
Google Text-to-speech Engine – Architecture arm	3.8.16	com.google.android.tts_3.8.16-210308160_minAPI15(armeabi-v7a)(nodpi).apk
Google Text-to-speech Engine – Architecture x86	3.8.16	com.google.android.ttscom.google.android.tts_3.8.16-210308163_minAPI15(x86)(nodpi).apk

Table 1-16. Democracy Suite 5.0-A Adjudication Software Build Environment Component Descriptions

Firmware/Software	Version	Filename
Microsoft Enterprise Library	5.0	Enterprise Library 5.0.msi
Microsoft Prism	4.0-November 2010	Prismv4.exe
Microsoft Identity Foundation SDK	4.0	WindowsIdentityFoundation-SDK-4.0.msi
Toggle Switch Control Library	1.1.1	ToggleSwitch 1.1.1.zip
Infragistics NetAdvantage Ultimate 2013.1	2013.1	NetAdvantage_dotNet_20131_With SamplesAndHelp.zip
iTextSharp	5.5.1	itextsharp-all-5.5.1.zip
CLR Security	June 2010	clrsecurity_june10.zip
OpenSSL	1.0.2K	openssl-1.0.2K.tar.gz
OpenSSL FIPS Object Module	2.0.10 (Cert 1747)	openssl-fips-2.0.10.tar.gz
Community MSI Extensions	1.4	msiext-1.4.zip
TreeViewEx	3.0.0.0	TreeViewEx.dll

Table 1-17. Democracy Suite 5.0-A ICP Election Firmware Compiler Descriptions

Firmware/Software	Version	Filename
g++ (GNU C++ compiler)	gcc3.4.0-20040603	m68k-uclinux-tools-c++-gcc3.4.0-20040603.sh

Table 1-18. Democracy Suite 5.0-A ICP Firmware Build Environment Component Descriptions

Firmware/Software	Version	Filename
Ubuntu 10.04 LTS – Long-term support	10.04	ubuntu-10.04.2-desktop-amd64.iso
Toolchain Installation Script	N/A	Toolchain.sh
m68k uClinux tools base gcc	3.4.0-20040603	m68k-uclinux-tools-base-gcc3.4.0-20040603.sh
m68k uClinux tools c++ gcc	3.4.0-20040603	m68k-uclinux-tools-c++-gcc3.4.0-20040603.sh
m68k uClinux tools gdb	20040603	m68k-uclinux-tools-gdb-20040603.sh
OpenSSL	1.0.2K	Openssl-1.0.2K.tar.gz
OpenSSL FIPS Object Module	2.0.10 (Cert 1747)	Openssl-fips-2.0.10.tar.gz

Table 1-19. Democracy Suite 5.0-A ICX Firmware Build Environment Component Descriptions

Firmware/Software	Version	Filename
Ubuntu 14.04.4	14.04.4	ubuntu-14.04.4-desktop-amd64.iso
OpenSSL	1.0.2K	openssl-1.0.2K.tar.gz
OpenSSL FIPS Object Module	2.0.10 (Cert 2473)	openssl-fips-2.0.10.tar.gz

Table 1-20. Voting System Equipment

Component	Serial Number
Proprietary Hardware	
ImageCast Precinct Optical Scanner PCOS-320C	AAFAJFM0061, AAFAJFN0030, AAFAJGI6764, AAFAJEL0352
ImageCast Precinct Optical Scanner PCOS-320A	AANAGCP0347, AANAGCP0002
ICP Ballot Box BOX-330A	AAUCCFX0083, AAUCCGI0011
ICX Samsung Tablet	[DVS-Samsung ICX-001], RF2GB01W0GD, RF2GB01V4HF, RF2GB01V5RL
ICX Inline EMI Filter	[DVS-EMIFILTER-001] thru [DVS-EMIFILTER-003]
COTS Hardware	
ICX aValue 15” Tablet (SID-15V)	0E14AF00014, B03G005400006, B033G00540008, 9E274118, 1D274118
ICX aValue 21” Tablet (SID-21V)	0E14AF00027, B03G005500019, 03G005500009, 0039BZ2D, 0039B209
Dell OptiPlex 7440 All In One	HVNRFB2, HVNQFB2, HVNPFB2
Dell PowerEdge R630	4Z07T52
Canon imageFormula DR-G1130 Scanner	GF301092, GF304418
Dell Precision T3420 PC	HS0VFB2, HS0TFB2, HS0RFB2, HS0SFB2
HP LaserJet Pro Printer M402dn	PHBQF20342, PHBQF20345, PHBQC12619, PHBQC19613, PHBQC12519, PHBQD18790, PHBQC12616
Dell OptiPlex 9030 All-In-One	CF73S52
Dell Ultrasharp 24” Monitor U2414H	1PVZ152, 62VZ152

Table 1-21. Voting System Support Equipment

Component	Serial Number
Dell Monitor KM632	FYNTY12, CKX6Y12, CN-0524N3-72461-59H-6U5U
Dell Monitor P2414Hb	CN-0524N3-74261-5AH-2DNU, CN-0524N3-74261-5AH-2DAU
ABLENET Jelly Bean Twist 10033400	[DVS-ablenet-001] thru [DVS-ablenet-014]
Tecla ShieldDos KDL-02001	[DVS-Tecla-001] thru [DVS-Tecla-006]

Table 1-21. Voting System Support Equipment *(continued)*

Component	Serial Number
Brother Laser Printer HL-L2300D	U63878K5N281729
Dell DVD Multi Recorder GP60NB60	[DVS-Dell-001]
Dell Latitude E7450 Laptop	30GFH72, 369FH72
Maxim iButton Programmer DS9490R# with DS1402	[DVS-Maxim-001] thru [DVS-Maxim-005]
APC Smart-UPS SMT1500	3S1536X06436, 3S1536X06475, 3S1536X06461, 3S1536X06485, 3S1536X06272, 3S1536X06201, 3S1536X07305, 3S1504X00395, 3S1504X00396
Dell X1008 Network Switch	4R8XX42, 26SXX42, 63SXX42
Dell X1018 Network Switch	6TN7Y42
Dell X1026 Network Switch	83D9Y42
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-005]
4-Way Joystick Controller S26	PME QC 1550 12, [DVS-JOY-001], [DVS-JOY-002]
Enablemart # 88906 Rocker (Paddle) Switch	[DVS-paddle-001]
Dell PowerConnect 2808 Network Switch	3S2P0Z1
IOGEAR SDHC/microSDHC 0U51USC410 Card Reader	8632, 8633
Lexar USB 3.0 Dual-Slot Reader	24020845007435
Hoodman Steel USB 3.0 UDMA Reader 102015	[DVS-hoodman-001]
ATI Handset	98862010101-035, 98862010103-075, 00659010100-046, 98862010100-232
ATI-USB Handset	02440010100-011, [DVS-ATIUSB-001], [DVS-ATIUSB-002]
ACS PC-Linked Smart Card Reader ACR39U	RR374-006272, RR374-010356, RR374-010365
Lexar Professional CF Card Reader Workflow CFR1	24050361400108, 24050361401994, 24050361401991, 24050361401990
CORCOM Filter P/N#: 15EMC1	[DVS-CorcomEMIFilter-001]
Delta Filter P/N#: 16PDCG5C	[DVS-DeltaEMIFILTER-001]

The materials required for testing of the D-Suite 5.0-A System included all materials to enable the test campaign to occur. This included the applicable hardware and software as well as the TDP, test support materials, and deliverable materials as identified by Dominion Voting Systems.

1.2 References

- Election Assistance Commission 2005 Voluntary Voting System Guidelines (VVSG) Version 1.0, Volume I, "Voting System Performance Guidelines", and Volume II, "National Certification Testing Guidelines"
- Election Assistance Commission Testing and Certification Program Manual, Version 2.0
- Election Assistance Commission Voting System Test Laboratory Program Manual, Version 2.0
- National Voluntary Laboratory Accreditation Program NIST Handbook 150-2016, "NVLAP Procedures and General Requirements (NIST Handbook 150-2016)", dated July 2006
- National Voluntary Laboratory Accreditation Program NIST Handbook 150-22, 2008 Edition, "Voting System Testing (NIST Handbook 150-22)", dated May 2008
- 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, Revision 7.0
- Election Assistance Commission "Approval of Voting System Testing Application Package" letter dated May 6, 2016
- EAC Requests for Interpretation (RFI) (listed on www.eac.gov)
- EAC Notices of Clarification (NOC) (listed on www.eac.gov)
- Dominion Voting Systems Technical Data Package *(A listing of the Democracy Suite 5.0-A documents submitted for this test campaign is listed in Section 3.1 of this Test Report)*

1.3 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

"CM" – Configuration Management

"COTS" – Commercial Off-The-Shelf

"DRE" – Direct Record Electronic

"EAC" – United States Election Assistance Commission

"EMS" – Election Management System

"FCA" – Functional Configuration Audit

"HAVA" – Help America Vote Act

"ICC" – ImageCast Central

"ICP" – ImageCast Precinct

"ICX" – ImageCast X

"ISO" – International Organization for Standardization

"NOC" – Notice of Clarification

"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

2.0 CERTIFICATION TEST BACKGROUND

2.1 Revision History

The Dominion Democracy Suite 5.0-A Voting System is a modified voting system configuration that introduces updated OpenSSL FIPS 140-2 validated cryptographic modules to the certified Democracy Suite 5.0 system configuration. The list below includes changes between this system and the baseline of the Democracy Suite 5.0 Voting System:

EMS

• Updated OpenSSL FIPS 140-2 validated cryptographic modules

ADJ

• Updated OpenSSL FIPS 140-2 validated cryptographic modules

ICC

• Updated OpenSSL FIPS 140-2 validated cryptographic modules

ICX

• Updated OpenSSL FIPS 140-2 validated cryptographic modules

ICP

• Updated OpenSSL FIPS 140-2 validated cryptographic modules

2.2 Scope of Testing

Testing from the previous test campaign was used to establish the baseline. The focus of this test campaign was on the introduction of the updated OpenSSL FIPS 140-2 validated modules. The following tasks were performed required to verify compliance of the modifications:

- Source Code Review, Compliance Build, Trusted Build, and Build Document Review

  To verify that no source code was changed to implement the updated FIPS modules/libraries, which are called upon in the build process and included in the compile, Pro V&V performed a comparison on the submitted source code.

- System Level Testing (System Integration Testing and Limited FCA)

  The system integration tests were performed to insure the D-Suite 5.0-A functioned as a complete system. The FCA for this test campaign included an assessment of the submitted modifications and included inputs of both normal and abnormal data during test performance. This evaluation utilized baseline test cases as well as specifically designed test cases and included predefined election definitions for the input data.

- Limited Technical Documentation Package (TDP) Review

  A limited TDP Review was performed to ensure that all submitted modifications were accurately documented and that the documents met the requirements of the EAC 2005 VVSG.

2.2.1 Modification Overview

The system modifications were limited to the introduction of the updated OpenSSL FIPS 140-2 validated cryptographic modules to the certified Democracy Suite 5.0 system configuration.

2.2.1.1 Detailed List of Changes

The introduction of the updated OpenSSL FIPS 140-2 validated cryptographic modules resulted in the following system changes:

Table 2.1. OpenSSL FIPS 140-2 Certification Information

Component	D-Suite 5.0 System	D-Suite 5.0-A System
EMS	OpenSSL 1.2	OpenSSL FIPS Object Module 2.0.10 (Cert 1747) OpenSSL 1.0.2k
Adjudication	OpenSSL 1.0.2e	OpenSSL FIPS Object Module 2.0.10 (Cert 1747) OpenSSL 1.0.2k
ICC	OpenSSL 1.2.3	OpenSSL FIPS Object Module 2.0.10 (Cert 1747) OpenSSL 1.0.2k
ICX	N/A	OpenSSL FIPS Object Module 2.0.10 (Cert 2473) OpenSSL 1.0.2k
ICP	OpenSSL 1.1.2	OpenSSL FIPS Object Module 2.0.10 (Cert 1747) OpenSSL 1.0.2k

2.2.2 Block Diagram

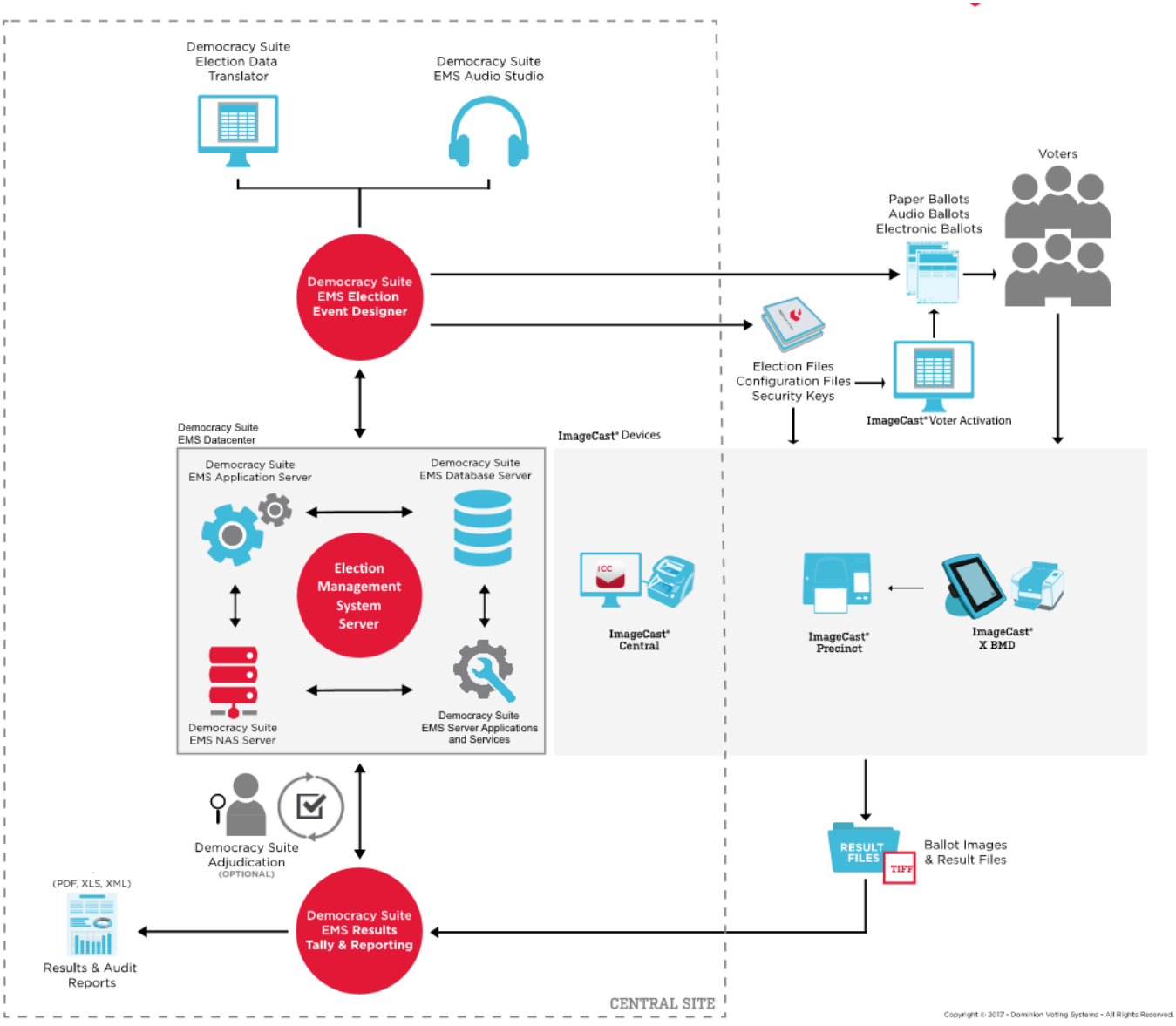

Figure 1-1. D-Suite 5.0-A System Overview

2.2.3 Supported Languages

The submitted voting system supports:

- Bengali
- Chinese
- English
- French
- Hindi
- Japanese
- Korean
- Spanish
- Thai

Due to the limited scope of testing, only English and Spanish language ballots were cast during the performance of functional testing.

2.2.4 VVSG

The D-Suite 5.0-A Voting System was evaluated against the relevant requirements contained in the EAC 2005 VVSG, Version 1.0.

2.2.5 RFIs

There are no RFIs released by the EAC as of the date of test completion that pertained to this test campaign that were not in effect at the time of the baseline system certification.

2.2.6 NOCs

There are no NOCs released by the EAC as of the date of test completion that pertained to this test campaign that were not in effect at the time of the baseline system certification.

3.0 TEST FINDINGS AND RECOMMENDATION

The D-Suite 5.0-A Voting System was evaluated against the relevant requirements contained in the EAC 2005 VVSG, Volumes I and II. The focus of this test campaign was on the introduction of the updated OpenSSL FIPS 140-2 validated cryptographic modules, as detailed in Section 2.2 of this Test Report. The summary findings and recommendations for each area of testing are provided in the following sections.

3.1 Summary Findings and Recommendations

Summary findings for the System Level Testing (System Integration Testing and Limited FCA), Security Testing, and Source Code Review are detailed in the relevant sections of this report. In addition to these areas of testing, a Limited TDP Review was performed, as described below.

Limited Technical Documentation Package (TDP) Review

A limited TDP Review was performed to ensure that all submitted modifications were accurately documented and that the documents met the requirements of the EAC 2005 VVSG. This review focused on TDP documents that had been modified since the certification of the baseline system. Any revised documents during the TDP review process were compared with the previous document revision to determine changes made, and the document was re-reviewed to determine whether subject requirements had been met.

A listing of all documents contained in the D-Suite 5.0-A TDP is provided in Table 3-1.

Table 3-1. TDP Documents

Document Number	Description	Version
Adjudication Documents		
2.05	Democracy Suite Adjudication Software Design and Specification	5.0-A::79
2.08	Democracy Suite Adjudication System Operation Procedures	5.0-A::123
2.09	Democracy Suite Adjudication System Maintenance Manual	5.0-A::62
D-Suite Documents		
2.02	Democracy Suite System Overview	5.0-A::101
2.06	Democracy Suite System Security Specification	5.0-A::488
2.07	Democracy Suite System Test and Verification	5.0-A::148
2.10	Democracy Suite Personnel Deployment and Training Requirements	5.0-A::90
2.11	Democracy Suite Configuration Management Process	5.0-A::303
2.12	Democracy Suite Quality Assurance Program	5.0-A::117
2.13	Democracy Suite System Change Notes	5.0-A::54
EMS Documents		
2.03	Democracy Suite EMS Functional Description	5.0-A::323
2.05	Democracy Suite EMS Software Design and Specification	5.0-A::274
2.08	Democracy Suite EMS System Operations Procedures	5.0-A::678
2.09	Democracy Suite EMS System Maintenance Manual	5.0-A::104
---	Democracy Suite EMS System Installation and Configuration Procedure	5.0-A::135
ImageCast Central Documents		
2.03	Democracy Suite ImageCast Central Functionality Description	5.0-A::138
2.05	Democracy Suite ImageCast Central Software Design and Specification	5.0-A::81
2.08	Democracy Suite ImageCast Central System Operation Procedures	5.0-A::170
---	Democracy Suite ImageCast Central Installation and Configuration Procedure	5.0-A::88

Table 3-1. TDP Documents *(continued)*

Document Number	Description	Version
ImageCast Precinct Documents		
2.03	Democracy Suite ImageCast Precinct Functionality Description	5.0-A::153
2.04	Democracy Suite ImageCast Precinct System Hardware Specification	5.0-A::121
2.04.1	Democracy suite ImageCast Precinct System Hardware Characteristics	5.0-A::72
2.05	Democracy Suite ImageCast Precinct Software Design and Specification	5.0-A::129
2.08	Democracy Suite ImageCast Precinct System Operation Procedures	5.0-A::248
2.09	Democracy Suite ImageCast Precinct System Maintenance Manual	5.0-A::102
ImageCast X Documents		
2.03	Democracy Suite ImageCast X Functionality Description	5.0-A::35
2.05	Democracy Suite ImageCast X Software Design and Specification	5.0-A::53
2.08	Democracy Suite ImageCast X System Operation Procedures	5.0-A::98
2.09	Democracy Suite ImageCast X System Maintenance Manual	5.0-A::39
---	Democracy Suite ImageCast X Installation and Configuration Procedure	5.0-A::25
User Guides		
---	Democracy Suite ImageCast Adjudication User Guide	5.0-A::111
---	Canon imageFORMULA DR-G1130 DR-G1100 User Manual	---
---	Democracy Suite Election Device Management User Guide	5.0-A::13
---	Democracy Suite EMS Audio Studio User Guide	5.0-A::66
---	Democracy Suite EMS Election Data Translator User Guide	5.0-A::70
---	Democracy Suite EMS Election Event Designer User Guide	5.0-A::159
---	Democracy Suite EMS Mobile Ballot Production User Guide	5.0-A::38
---	Democracy Suite EMS Results Tally and Reporting User Guide	5.0-A::90
---	Democracy Suite ImageCast Central User Guide	5.0-A::97
---	Democracy Suite ImageCast Precinct User Guide	5.0-A::48
---	Democracy Suite ImageCast Voter Activation User Guide	5.0-A::38
---	ImageCast X Ballot Marking Device User Guide	5.0-A::65
---	Dell Latitude E7450 Owner's Manual	---
---	SID-15V-Z37-A1R User Manual	Rev. 1.0
---	SID-21V-Z37-A1R User Manual	Rev. 1.0
---	Samsung GALAXY Note PRO Android Tablet User Manual	---

Table 3-1. TDP Documents *(continued)*

Document Number	Description	Version
---	Samsung GALAXY Tab PRO Android Tablet User Manual	---
Supplementary Documents		
---	AT4 Wireless Test Report No. (NIE) 39698RSE.001 (Tecla Shield)	---
---	Cyber Acoustics ACM-70B Stereo Headphones Product Sheet	---
---	Democracy Suite ImageCast C++ Coding Standard	5.0-A::25
---	Democracy Suite C# Automated Code Review Process	5.0-A::20
---	Dell Latitude E7450/Latitude 7450 Regulatory Compliance Sheet	---
---	Dell OptiPlex 9020 AIO Regulatory Compliance Sheet	---
---	Dell OptiPlex 9030 AIO Regulatory Compliance Sheet	---
---	Dell Networking X-Series Specification Sheet	Ver. 1.9
---	Dell OptiPlex 9020 All-in-One Technical Specification Sheet	---
---	Dell OptiPlex 9030 All-in-One Technical Specification Sheet	---
---	Dell B2360d and B2360dn Brochure	---
---	Dominion Voting Systems Java Coding Standards	1.0
---	Dominion Voting Systems JavaScript Coding Standards	1.0
---	Google Java Style Dominion .xml	---
---	Democracy Suite ImageCast Device Configuration Files	5.0-A::67
---	Democracy Suite ImageCast Printing and Finishing Specification	5.0-A::58
---	Democracy Suite ImageCast Total Results File Format	5.0-A::28
---	Democracy Suite ImageCast Precinct Election Definition Files	5.0-A::39
---	Democracy Suite ImageCast Precinct Extracting Firmware Contents	5.0-A::18
---	Democracy Suite ImageCast Precinct Firmware Update Procedure	5.0-A::29
---	Democracy Suite ImageCast Precinct Level One (L1) Maintenance Manual	5.0-A::43
---	Democracy Suite ImageCast Precinct Technical Guide	5.0-A::27
---	Canon imageCLASS LNP6230dw Technical Specification Sheet	---
---	YEDU.E95462 Uninterruptible Power-supply Equipment Sheet	---
---	Dell Latitude E7440 Regulatory Compliance Sheet	Rev. A09
---	Dell PowerEdge R630 Regulatory Compliance Sheet	Rev. A10
---	Dell Precision T1700 MT Regulatory Compliance Sheet	Rev. A09
---	Dell PowerConnect 2808 Product Safety. EMC, and Environmental DataSheet	---

Table 3-1. TDP Documents *(continued)*

Document Number	Description	Version
---	Dell PowerConnect 2816 Product Safety. EMC, and Environmental DataSheet	---
---	LAVA STS Product Family User Manual	Rev. A01
---	APC Smart-UPS 230V Product Information Sheet	---
---	SAMSUNG Android Tablet Health and Safety and Warranty Guide	---
Build Documents		
---	Democracy Suite EMS Software Build Document	2.3.1::10
---	Democracy Suite ImageCast Precinct Firmware Build and Install	5.0-A::53
---	ImageCast X Build	5.0.11

Additionally, the requirements for the QA and CM system review were evaluated throughout the test campaign, as described below:

QA and CM System Review

This testing utilized the TDP Review in conjunction with the PCA to determine compliance to the EAC 2005 VVSG requirements and the requirements stated in the Dominion technical documentation. The review of the Quality Assurance and Configuration Management documentation focused on Dominion's adherence to its stated QA and CM processes. No discrepancies were noted during the reviews.

3.1.1 Source Code Review, Compliance Build, Trusted Build, and Build Document Review

Pro V&V reviewed the submitted source code to the EAC 2005 VVSG 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.

Summary Findings

Automated Source Code Review: An Automated Source Code Review was performed on the Election Management source code, ICX source code and the ICP source code. All components of the Election Management source code were revised to reflect the use of the updated FIPS modules; however, the proprietary source code itself was not modified. These revisions are reflected in Table 1-1. Additionally, due to the updated FIP modules, the ICX source code changed from 5.0.6149.28963 to ICX 5.0-A.6366.20007. The ICP source code changed from 5.0.1-US to 5.0.2-US. No source code issues were found during the Automated Source Code review. *Note: The source code version was incremented due to the release of the source code with the updated FIPS modules.*

Manual Source Code Review: The Manual Source Code review was performed prior to the Compliance and Trusted Builds. The Manual Source Code was a comparison between the previously certified source code and the source code submitted for this test campaign.

Compliance Build: The compliance build was performed following the compliance review. Once the compliance review was performed and the source was deemed stable enough to proceed with testing, the source code and all additional packages were compiled into a Compliance Build.

Trusted Build: The trusted build consisted of inspecting customer submitted source code, COTS, and Third Party software products and combining them to create the executable code. This inspection followed the documented process from the "United States Election Assistance Commission Voting System Test Laboratory Program Manual" Section 5.5 – 5.7. *Performance of the trusted build includes the build documentation review*

3.1.2 System Level Testing

System Level Testing included the Limited Functional Configuration Audit (FCA) and the System Integration Tests. System Level testing was implemented to evaluate the complete system. This testing included all proprietary components and COTS components (software, hardware, and peripherals) in both the EMS Standard and EMS Express system configurations. For software system tests, the tests were designed according to the stated design objective without consideration of its functional specification. The system level hardware and software test cases were prepared independently to assess the response of the hardware and software to a range of conditions.

The FCA for this test campaign included an assessment of the submitted modifications and included inputs of both normal and abnormal data during test performance. For example if the system field requires numeric characters normal inputs would be numeric characters only. To verify this is true abnormal inputs would be entered into the fields using alpha numeric characters. The results would be verified and validated to verify the system will only accept the normal data input which would be numeric characters only and a failure would occur if alpha numeric characters were accepted. This evaluation utilized baseline test cases as well as specifically designed test cases and included predefined election definitions for the input data. The System Integration Tests were performed to verify the D-Suite 5.0-A functioned as a complete system.

The Democracy Suite Election Management System (EMS) consists of a set of applications responsible for all pre-voting and post-voting activities used in election definition and management process. The Democracy Suite EMS applications are as follows:

- EMS Election Event Designer
- EMS Results Tally and Reporting
- EMS Audio Studio
- EMS Adjudication

- EMS Adjudication Services
- EMS File System Service
- EMS Election Data Translator
- Smart Card Helper Service
- ImageCast Voter Activation
- EMS Data Center Manager
- EMS Application Server*
- EMS Database Server*
- EMS NAS Server
- EMS Election Device Management

*This application is installed when the EMS Data Center Manager application is run on the EMS Server or EMS Express PC. Unlike the other EMS Applications, it is not installed using an application installer file.

The Democracy Suite 5.0-A Voting System is a paper-based optical scan voting system with a hybrid paper/DRE option consisting of the following major components: The Election Management System (EMS), the ImageCast Central (ICC), the ImageCast Precinct (ICP), and the ImageCast X (ICX).

Summary Findings

The FCA was completed successfully with no anomalies or deficiencies noted. All system integration tests were successfully executed. System Integration was performed on the entire Democracy Suite 5.0-A system. The following elections were ran from end-to-end:

- Three general elections with the following breakdowns:
  - General Election held in four precincts (one of which was a split precinct)
  - General Election held in three precincts. This election contained fifteen contests compiled into three ballot styles.
  - General Election 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:
  - Open Primary Election in two precincts. This election contained thirty contests compiled into five ballot styles.

- Primary Election held in two precincts. This election contained thirteen contests compiled into three ballot styles. One contest is in all three ballot styles; all other contests are independent.
- Primary Election designed to functionally test the handling of multiple ballot styles, support for at least three languages including a Ideographic based language, support for common voting variations, and audio support for at least three languages and a ADA binary input device.

3.1.2.1 Software Module and Functional Testing

Pro V&V reviewed the manufacturer's program analysis, documentation, and module test case design and evaluated the test cases for each module with respect to flow control parameters and entry/exit data.

Component Level Testing was implemented during the FCA for each component and subcomponent. During the source code review, compliance builds, and security testing, Pro V&V utilized limited structural-based techniques (white-box testing). Additionally, specification-based techniques (black-box testing) were utilized for the individual software components.

Pro V&V defined the expected result for each test and the ACCEPT/REJECT criteria for certification. If the system performed as expected, the results were accepted. If the system did not perform as expected, an analysis was performed to determine the cause. If needed, the test was repeated in an attempt to reproduce the results. If the failure could be reproduced and the expected results were not met, the system was determined to have failed the test. If the results could not be reproduced, the test continued. All errors encountered were documented and tracked through resolution.

Summary Findings

All software module and functional testing was completed successfully with no anomalies or deficiencies noted. This testing was integrated into the FCA and System Level Testing.

3.1.3 Security Testing

The system security functions for the modification remain unchanged from the previously certified system; however, additional review was performed on the implementation of the FIPS cryptographic module in order to:

- Confirm the module (model and version) that is used and implemented was present on the NIST CMVP validated products list.
- Confirm the module in all five instances is configured and used per the NIST published security policy for that module.

Summary Findings

Security Testing was completed successfully with no anomalies or deficiencies noted. It was confirmed that the modules used were present on the NIST CMVP validated products list and in all instances were configured and used per the NIST published security policy for that module.

No other security testing will be performed.

3.2 Anomalies and Resolutions

When a result is encountered during test performance that deviates from what is standard or expected, a root cause analysis is performed. Pro V&V considers it an anomaly if no root cause can be determined. In instances in which a root cause is established, the results are then considered deficiencies. No anomalies occurred during the testing of the D-Suite 5.0-A System.

3.3 Correction of Deficiencies

Any violation of the specified requirement or a result is encountered during test performance that deviates from what is standard or expected in which a root cause is established is considered to be a deficiency. Upon occurrence, deficiencies are logged throughout the test campaign for disposition and resolution. No deficiencies were encountered during testing of the D-Suite 5.0-A Voting System.

4.0 RECOMMENDATION FOR CERTIFICATION

The D-Suite 5.0-A Voting System, as presented for testing, successfully met the requirements set forth for voting systems in the U.S. Election Assistance Commission (EAC) 2005 Voluntary Voting System Guidelines (VVSG), Version 1.0. Additionally, Pro V&V, Inc. has determined that the D-Suite 5.0-A functioned as a complete system during System Integration Testing. Based on the test findings, Pro V&V recommends the EAC grant the D-Suite 5.0-A certification to the EAC 2005 VVSG.

ATTACHMENT A

Trusted Build

EMS Version 5.0.16.1 – The EMS trusted build was performed using the "Democracy Suite EMS Software Build Environment Install Document for EMS Suite" document Version 2.3.1_10, provided by Dominion Voting Systems. The EMS build included the following source code components:

- EMS Election Event Designer (EED) 5.0.16.1
- EMS Results Tally and Reporting (RTR) 5.0.16.1
- EMS Application Server 5.0.16.1
- EMS File System Service (FSS) 5.0.16.1
- EMS Audio Studio (AS) 5.0.16.1
- EMS Data Center Manager (DCM) 5.0.16.1
- EMS Election Data Translator (EDT) 5.0.16.1
- ImageCast Voter Activation (ICVA) 5.0.16.1
- EMS Adjudication (Adj) 5.0.0.44402
- EMS Adjudication Service 5.0.0.44402
- EMS Election Data Manager (EDM) 5.0.6366.25253
- Smart Card Helper Service 5.0.6366.25232

The trusted build yielded the following output files and their associated Hash Values:

- **Democracy_Suite_5.0.16.1.iso**

SHA256 -AC74C36ADA7F1A1772253F42629A0F9187B4E4C0CBE5FD9F567D5651E9B7FD14

  - Adjudication**DVS Adjudication Services Setup.msi**
    SHA256 - 98fa8d8416ca68cc5692061b3fc6931d46e4351219fa8576fe040aee82c048bf
  - Adjudication**DVS ImageCast Adjudication Client Setup.msi**
    SHA256 - ccc2df4ad8f700f8a977a522d9ddb7ed0859f7994d4e34c34a120d3fc6297974
  - Adjudication**InstallWithLogging.bat**
    SHA256 - 027ad0e8e4d35181b54988dfd38b9d69fcfb4b365e8300b134714171f5784bcb
  - EdmAdmin**EdmInstaller.msi**
    SHA256 - dc7c72d8cac07339761506466a45e40c8c639f870a7ddae924656c451f01995d
  - EdmAdmin**setup.exe**
    SHA256 - 9ce8595f59c6f15ae616d615cbdfb42bc3197d50ddf50854b455ff27283cd39c
  - EMSAPPS\x64**APPS_FED_CERT_Setup_x64.msi**
    SHA256 - a8a7a579ea1a9e3a541ffe90c1095d2603090bdffd0be9339085f348deba89c5
  - EMSAPPS\x64**setup.exe**
    SHA256 - 1018ee1798cc19a25371e8dc575d9bff49bb7ba23c6bddd63b97f7bf3d78a5b9
  - EMSAS\x32**EMSAudioStudioSetup.msi**
    SHA256 - 7ead21a40f05483b414f00f253df7178de7d491cd531aa50a0a0d1e5c907e1e4
  - EMSAS\x32**setup.exe**
    SHA256 - 3139eafb12f385f55f28271f65c1ae178497c23d4e0cbfe9ac3a969c51716d96
  - EMSDCM\x32**DemocracySuiteEMS_DCM.exe**
    SHA256 - 5ee38d771e57802470537db711fad3cbf929c95500a482d99dc1cc531b1ad66c
  - EMSDCM\x32**DemocracySuiteEMS_DCM.exe.config**

SHA256 - 8c1b006dbd52069dd23b864a5bbcb2a125340b80857185eb5ef2501c47173a4c

- EMSDCM\x32**DVS.Utilities.Common.dll**
  SHA256 - 437cf123d25619360b4bccc9b899743b2b4e05d3faf980feba25a420278adedb
- EMSDCM\x32**DVS.Utilities.MSWinManager.dll**
  SHA256 - 22d16ea6dd33efcacbf2ec71f4322b0645c2e4f072d781d8be1ba6d7f4030935
- EMSDCM\x32**NLog.config**
  SHA256 - 1cf182c4496852131d5d85b68b3a14636dd487dbe446711a0c3a712a3b0d971a
- EMSDCM\x32**NLog.dll**
  SHA256 - e17aac589bd48a623857de7f8113bcae6f72e4fe4652ca615ffa1028353b246d
- EMSDCM\x32**Static.zip**
  SHA256 - 52ce17b3342201360f5a9ecb0586a949616ed6e58858e0d50901bc1ae2584bd3
- EMSEDT\x32**EDTSetup_x86.msi**
  SHA256 - da7f6dcf55492be87fa0b0c623fda3a79fcf8390b0bc8d17100ee8442b477da7
- EMSEDT\x32**setup.exe**
  SHA256 - c263194f55a920ea17c4179104cd5d91890e74cd95297ddf12b19f4fa156a310
- EMSEDT\x64**EDTSetup_x64.msi**
  SHA256 - d4dce79cf9d2a22056023effa74122a8dfad53060b7ea02a77da28893c63b2f0
- EMSEDT\x64**setup.exe**
  SHA256 - 01b65ed106fc301d75ac5eacf98dc6d826de080fed58d1d194b56d994db94b82
- EMSEED\x64**EED_FED_CERT_Setup_x64.msi**
  SHA256 - 1032adfefa802425db21946de96f6580042daf87b78a1811c055335331b33c36
- EMSEED\x64**setup.exe**
  SHA256 - 82145930f18dada43943cc0c2cd246454e8732abaf9c7ff07ff11e06b46a9367
- EMSFSS\x32**FSSSetup.msi**
  SHA256 - 315e8a9baa2a4b89d95874bd17e68491fc8016c4a7e1b4146d3d7a4acef44a0f
- EMSFSS\x32**setup.exe**
  SHA256 - 98086648dc146277a3038305bb3da942224346bb2efe88d20fdebe60c9b6113f
- EMSICVA\x64**ICVASetup.msi**
  SHA256 - 2e95db255c6020e8a0eaa69fc5e6bb37e97592e0693021c9f655a1879adda567
- EMSICVA\x64**setup.exe**
  SHA256 - 73f261e9c5de9ab6ebdf1bb592bd39b032db367deaecdd6c635b690a498ae48b
- EMSRTR\x64**RTR_FED_CERT_Setup_x64.msi**
  SHA256 be3be126fc1423f8668f5bf2383649dad7979539a104406ac454a3d9dfff23a3
- EMSRTR\x64**setup.exe**
  SHA256 - ee74ac3aa112b7f4149be5164476b1fc901eaa5a9c2e4cc1a5449c76450d7c78
- ICC_INSTALL**ICCSetup_v5.0.1.0.exe**
  SHA256 - 0dd31362c1116a349123d4ebb2700cbefd1746b60422760f847cf9fef8bcdc24
- SmartCardService**setup.exe**
  SHA256 - 0919c093db67edc2ec5e1feae12f7c835e3fb96d0cf035ab760a58cce8eb40a7
- SmartCardService**SmartCardServiceSetup.msi**
  SHA256 - 213fcb70f035e46f257c26db9df3e325e9e5609a124c0deafe58abd56c8bd0b0

ICP Version 5.0.2-US – The ICP trusted build was performed using the "ICP Firmware Build and Install" document Version 5.0-A::53, dated March 16, 2016, provided by Dominion Voting Systems. The ICP build included the following source code components:

- Election Firmware 5.0.2-US
- Firmware Updater 5.0.2-US
- Firmware Extractor 5.0.2-US
- Kernel (uClinux) 5.0.2-US
- Boot Loader (COLILO) 20040221
- Asymmetric Key Generator 5.0.2-US
- Asymmetric Key Exchange Utility 5.0.2-US
- Firmware Extractor (Uses Technician Key) 5.0.2-US

The trusted build yielded the following output files and their associated Hash Values:

- ApplUpdateCard**cf2xx.sig**

SHA 256 - 662717CDA06959285E2C893B3408A23339F9824299E5F772F800B38322B4F7A4

- ApplUpdateCard**colilo.bin**

SHA 256 -
24104A477672CC20D37E0910AB27D715E7D87B0DAD5D24C7A26ABA3EA5FA4A30

- ApplUpdateCard**firmUp.enc**

SHA 256 -
0B7C2674D6F19B52EA32B8FCD38387A3432924EAC2214DE8A8C73EE9D6A11924

- ApplUpdateCard**image.bin.gz**

SHA256 -
445EAF066A5A0B7CDCD3A85B84F6847F11BD1384978E1FC0DCB8D0EC3FA25C82

- Utilities**FirmwareExtract.enc**

SHA 256 -
3F2D98223CD61654A76AA219DC190020576BFAA01627F7732DBCA6E8FA01B4DB

- Utilities**KeyExchange.enc**

SHA 256 -
D9E4F27266A4E0B84A1E6AAA0AFA4C0F6C17727DDE247C43BA9F2017AD16ECF6

- Utilities**keyGen.enc**

SHA 256 -
D9E4F27266A4E0B84A1E6AAA0AFA4C0F6C17727DDE247C43BA9F2017AD16ECF6

- Utilities**TechExtract.enc**

SHA256 -
3F2D98223CD61654A76AA219DC190020576BFAA01627F7732DBCA6E8FA01B4DB

ICX Version 5.0-A.6366.2007– The ICX trusted build was performed using the "ImageCast X Build" document Version 5.0.12, dated 03/22/2016, provided by Dominion Voting Systems. The ICX build included the following source code components:

- ICX Application 5.0-A.6366.2007
- ICX Security Certificate N/A
- ICX Security Certificate Password N/A

The trusted build yielded the following output files and their associated Hash Values:

- **ICX.apk**

SHA 256 -
99F9212971109829B1DB3197DA9EA2A1A470E6C4624C3A61B5B772145E9FC642

- **icx_pkcs12.pfx**

SHA 256 - 18033D4F01217E5795575F9275BAEF7BC5C0387ADB1346F928E123629D273749

- **icx_pfx.pwd**

SHA 256 -
3F4C5B694B92DDC7DB0D23DBC38334FF41598862270198E9F70D62A15442132F

ATTACHMENT B

(As-Run Test Plan)