SECURITY ASSESSMENT SUMMARY REPORT
FOR
DOMINION VOTING SYSTEMS
DEMOCRACY SUITE 4.0

TABLE OF CONTENTS

Page No.

1.0 INTRODUCTION

1.1 Objective

The purpose of this security assessment was to investigate various possible technical, physical, and operational security issues with the voting system Equipment-Under-Test (EUT). This final report summarizes the testing performed and the noted results. The testing included, but was not limited to, document reviews, vulnerability scans, system audits, and Security Test & Evaluations (ST&E). This report is intended to help familiarize stakeholders with the system level technical, physical, and operational testing processes that were used to help check the confidentiality, integrity, and availability of the system and its components.

1.2 Scope

The following Dominion Voting Systems components were utilized during testing:

- Election Management System (EMS) – Election Event Designer (EED)
- Election Management System (EMS) – Results, Tally and Reporting (RTR)
- Election Management System (EMS) – Audio Studio (AS)
- ImageCast Evolution (ICE)
- ImageCast Precinct (ICP)
- Transport Media (TM)
- Audio Tactile Device (ATI)
- Ballot Box
- Technical Data Package (TDP) Documents

The following activities were within the scope of this project:

- Review of supplied documentation.
- Assessment of the physical security of the system components.
- Assessment of the configuration and security controls of the system components.
- Assessment of user access, roles, and permissions
- Penetration testing of system components and peripherals

The following activities were NOT part of this security assessment:

- Any Social Engineering techniques.
- Any testing that could irreparably harm the EUT.

1.3 References

The media listed below were utilized as part of this test:

- Parikh, Clay U., CEH, CHFI, CISSP. Email. PR List. July 26, 2011. Print.

- Parikh, Clay U., CEH, CHFI, CISSP. Email. RE: PR List. July 27, 2011. Print.
- Parikh, Clay U., CEH, CHFI, CISSP. Email. ICE Security Comments. December 10, 2011. Print.
- Wyle Laboratories. Compliance Testing of the Dominion Voting Systems Democracy Suite ICPA System, T-57381. July 29, 2011. Print.
- Dominion Voting Systems. "2.06 Democracy Suite System Security Specification, Version 1.1.0::293". N.p., March 16, 2012. Print.
- Dominion Voting Systems. "2.02 Democracy Suite System Overview, Version 1.2.0::225". N.p., March 16, 2012. Print.
- Dominion Voting Systems. "2.03 Democracy Suite EMS Functional Description, Version 1.1.0::209". N.p., March 20, 2012. Print.
- Dominion Voting Systems. "2.03 Democracy Suite ImageCast Evolution Functionality Description Functional Description, Version 1.2.0::58". N.p., March 21, 2012. Print.
- Dominion Voting Systems. "2.03 Democracy Suite ImageCast Central Functionality Description Functional Description, Version 1.0.0::48". N.p., March 20, 2012. Print.
- Dominion Voting Systems. "2.03 Democracy Suite ImageCast Precinct Functionality Description Functional Description, Version 1.1.0::100". N.p., March 16, 2012. Print.
- Dominion Voting Systems. "2.04 ImageCast Evolution Tabulator System Hardware Specifications, Version 1.2.0::77". N.p., March 16, 2012. Print.
- Dominion Voting Systems. "2.04 ImageCast Precinct Tabulator System Hardware Specifications, Version 1.1.0::67". N.p., March 16, 2012. Print.
- Dominion Voting Systems. "2.05 EMS Software Design and Specifications, Version 1.0.0::186". N.p., March 21, 2012. Print.
- Dominion Voting Systems. "2.05 ImageCast Evolution Software Design and Specification, Version 1.0.0::70". N.p., March 21, 2012. Print.
- Dominion Voting Systems. "2.05 ImageCast Precinct Software Design and Specification, Version 1.0.0::93". N.p., March 16, 2012. Print.
- Dominion Voting Systems. "2.05 ImageCast Central Software Design and Specification, Version 1.1.0::147". N.p., March 21, 2012. Print.
- Dominion Voting Systems. "2.08 ICE System Operations Procedures, Version 1.0.0::79". N.p., March 21, 2012. Print.
- Dominion Voting Systems. "2.08 EMS System Operations Procedures, Version 1.0.0::45". N.p., March 16, 2012. Print.
- Dominion Voting Systems. "2.08 ICP System Operations Procedures, Version 1.0.0::45". N.p., March 16, 2012. Print.
- Dominion Voting Systems. "2.08 ICE System Operations Procedures, Version 1.1.0::109". N.p., March 16, 2012. Print.
- Dominion Voting Systems. "2.09 EMS System Maintenance Manual". N.p., February 22, 2012. Print.

- Dominion Voting Systems. "2.09 ImageCast Evolution System Maintenance Manual, Version 1.1.0:109". N.p., March 16, 2012. Print.
- Wyle Laboratories. VP-1 Photographs, T-56849. 2010. JPGs
- United States Election Assistance Commission. 2005 Voluntary Voting System Guidelines, Volume I, Version 1.0. New York, Washington D.C., 2005, Print
- United States Election Assistance Commission. 2005 Voluntary Voting System Guidelines, Volume II, Version 1.0. New York, Washington D.C., 2005. Print
- United States Election Assistance Commission. Testing and Certification Program Manual, Version 1.0. New York, Washington, January 1, 2007. Print
- United States Election Assistance Commission. Voting System Test Laboratory Program Manual, Version 1.0, New York, Washington, effective date July 2008. Print
- United States Department of Commerce, National Institute of Standards and Technology. National Voluntary Laboratory Accreditation Program, NIST Handbook 150, 2006 Edition, NVLAP, Washington, February 2006. Print
- United States Department of Commerce, National Institute of Standards and Technology. National Voluntary Laboratory Accreditation Program, NIST Handbook 150-22, 2008 Edition, NVLAP, Washington, May 2008. Print
- Help America Vote Act (HAVA) of 2002, Pub. L. no. 107-252. October 2002. Web
- Wyle Laboratories. Quality Assurance Program Manual, Revision 4. Print
- ANSI/NCSL Z540-3, Calibration Laboratories and Measuring and Test Equipment, General Requirements. Web
- International Standards Organization. ISO 10012-1:2003(E), Measurement Management Systems, Requirements for Measurement Processes and Measuring Equipment, April 15, 2003. Print
- United States Election Assistance Commission. Notices of Clarification. Web, EAC.gov
- United States Election Assistance Commission. Requests for Interpretation. Web, EAC.gov
- Panko, Raymond R. "Corporate Computer and Network Security". Boston: Prentice Hall, 2010. Print
- Tipton, Harold F, CISSP and Micki Krause, CISSP. Information Security Management Handbook. Boca Raton, Fl: CRC Press, 2010. CD-ROM
- NIST Standards for Security Categorization of Federal Information and Information Systems, FIPS PUB 199, February 2004

1.4 Terms and Abbreviations

Table 1-1 Terms and Abbreviations

Term	Abbreviation	Definition
Audio Studio	AS	Democracy Suite EMS Audio Studio client application represents an end-user helper application used to record audio files for a given election project. As such, it is utilized during the pre-voting phase of the election cycle.
Audio Tactile Interface	ATI	The Audio Tactile Interface is a handheld device used by a voter during an accessible voting session to navigate through, and make selections to, their ballot.
United States Election Assistance Commission	EAC	Commission created per the Help America Vote Act of 2002, assigned the responsibility for setting voting system standards and providing for the voluntary testing and certification of voting systems.
Election Manager System	EMS	The Democracy Suite Election Management System (EMS) set of applications are responsible for all pre-voting and post-voting groups of activities in the process of defining and managing elections. The complete EMS software platform consists of client (end-user) and server (back-end) applications.
Election Event Designer	EED	Democracy Suite EMS Election Event Designer client application integrates election definition functionality and represents a main pre-voting phase end-user application.
Equipment Under Test	EUT	Dominion Voting Systems Democracy Suite Comments and Peripherals
ImageCast Central	ICC	ICC is a central location ballot counters
ImageCast Evolution	ICE	ICE is a polling place election day ballot counters with optional ballot marking
ImageCast Precinct	ICP	ICP is a polling place election day ballot counters
Personal Computer	PC	The EMS Windows 2007 Operating System (OS) desktop computer and peripherals.
Results, Tally, and Reporting	RTR	Democracy Suite EMS Results Tally and Reporting client application integrates election results acquisition, validation, tabulation, reporting and publishing capabilities and represents a main post-voting phase end-user application.
Technical Data Package	TDP	The documents necessary to define the product and its method of operation; to provide technical and test data supporting the vendor's claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance.
Transport Media	TM	CF Cards used by the system to transport election data.
Voluntary Voting System Guidelines	VVSG	Technical Data Package TDP A set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility and security capabilities required to ensure the integrity of voting systems.

1.5 Tested System Description

As per the *Democracy Suite System Overview*, "the Democracy Suite platform consists of four main system components:

- The Democracy Suite Election Management System (EMS) software platform,
- The Democracy Suite ImageCast Precinct (ICP) optical ballot counter,
- The Democracy Suite ImageCast Evolution (ICE) optical ballot counter,
- The Democracy Suite ImageCast Central (ICC) optical ballot counter.

The Dominion Democracy Suite Election Management System (EMS) represents a set of N-Tier software applications for pre-voting and post-voting election project activities that are applicable to jurisdictions of various sizes and geo-political complexities. The Democracy Suite EMS platform is available in three hardware configurations ranging from a single PC/laptop configuration, to single server and dual server hardware configurations.

The ImageCast Precinct system is a precinct optical scan ballot tabulator that is used in conjunction with an external ballot storage box. The unit is designed to scan marked paper ballots, interpret voter marks on the paper ballot, and communicate these interpretations back to the voter either visually through the integrated LCD display or via the AVS interface. Upon acceptance of the voter, the unit securely deposits the ballots into the secure ballot box. AVS requirements can be met using an integrated Audio Tactile Interface (ATI) that is tethered to the ImageCast. This provides the voter with the ability to create a machine and human readable marked paper ballot entirely through an AVS interface.

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

The Dominion Democracy Suite ICC Ballot Counter system 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. Central scanning system hardware consists of a combination of two COTS devices used together to provide the required ballot scanning processing functionality.

Further, According to the *System Security Specification* Document, "The ICE, ICP and ICC are logically and physically connected to the EMS platform through the use of memory cards and administrative security keys."

Table 1-2 Security Scan Equipment

Equipment	Manufacturer / Model	Hardware Specifications	Service Tag
Dell Precision Desktop	T1500	Processor: Intel Core i7-860 2.8 GHz, Memory: 4x 1GB 1333MHz DDR3, Hard Drive Capacity: 500 GB	61VNNM1
Dell Precision Desktop	T1500	Processor: Intel Core i7-860 2.8 GHz, Memory: 4x 1GB 1333MHz DDR3, Hard Drive Capacity: 500 GB	61TPNM1
Dell Precision Desktop	T1500	Processor: Intel Core i7-860 2.8 GHz, Memory: 4x 1GB 1333MHz DDR3, Hard Drive Capacity: 500 GB	61YMNM1
Dell Workstation	Inspiron One 2305	Processor: AMD Athlon II X2 240e 2.8 GHz, Memory: 8GB Dual Channel 1333MHz DDR3, Hard Drive Capacity: 1 TB	564C3P1
ICP	Dominion	Precinct-level optical scanner and tabulator with audio voting capabilities	WLDAFBH0023
ICP	Dominion	Precinct-level optical scanner and tabulator with audio voting capabilities	WLDAFBH0002
ICP	Dominion	Precinct-level optical scanner and tabulator with audio voting capabilities	WLDAFBH0005
ICE	Dominion	Precinct-level optical scanner, ballot marker, and tabulator with audio voting	ICE2P1008
ICE	Dominion	Precinct-level optical scanner, ballot marker, and tabulator with audio voting	ICE2P1015
ICE	Dominion	Precinct-level optical scanner, ballot marker, and tabulator with audio voting	ICE2P1007
ICC	Dominion	High-speed central ballot scan tabulator	ED300874
Ballot Box	Dominion	Externally secure ballot box	57381-007
Ballot Box	Dominion	Externally secure ballot box	57381-015
Ballot Box	Dominion	Externally secure ballot box	57381-008
Ballot Box	Dominion	Externally secure ballot box	57381-014
Ballot Box	Dominion	Externally secure ballot box	57381-012
Ballot Box	Dominion	Externally secure ballot box	57381-013

2.0 SUMMARIES OF COMPONENT SECURITY ASSESSMENTS

2.1 EMS SECURITY ASSESSMENT

The EMS (Express) was located on a Dell Precision T1500 with Rocsecure Commander 2UE external hard drive. The EMS was subjected to two main rounds of security evaluations. The first was during evaluations of the ICP and its components and the second was during of the ICE and its components.
In both instances all of the WoP6 evaluations were performed. These included in part examining the BIOS, boot sequence, Windows User Accounts, EMS User Accounts, residing software, command-line interpreter, system and log audits, physical security concerns, user credentialing, and system settings. These evaluations were performed manually or with the aid of scripts.

The below EMS security concerns were observed and communicated to the manufacture.

- The ***Local Security Policy*** account lockout threshold was set to 0.
- The ***Password Policy*** complexity was disabled.

- The Administrator and Guest accounts had not been disabled or renamed.
- The access of ***Global System Objects*** was disabled.
- The ***Backup and Restore Privilege*** was disabled.
- The ***Auto Shutdown System if Unable to Log Security Audits*** was disabled.
- The ***Clear Virtual Memory Pagefile*** was disabled.
- The ***Do Not Display Last User Name*** was disabled.
- The ***Use FIPS Compliant Algorithms for Encryption Hashing and Signing*** was disabled.
- The ***Network Access Remotely Accessible Registry Paths*** setting had registry listings. Although network setup was not analyzed for this system it is a best practice to restrict network access to the registry.
- The ***Everyone Group*** was listed in ***Bypass Traverse Checking and Access This Computer from the Network***. It is a best practice to always restrict network access, and although the ***Bypass Traverse Checking*** does not allow the user to list the contents of a directory, only to traverse directories, the ***Everyone Group*** should be removed.
- An ***Audit Events Have Been Dropped by the Transport 0*** was observed. This error can happen for several reasons but almost always involves the system freezing or rebooting. This is of note because the EMS system resides on a Windows 7 OS and dependent upon it.
- In several instances EMS user accounts, especially Language User, were found able to perform outside their defined roles.
- Sections of the TDP were inconsistent with observed normal system operations.
- There were concerns surrounding the FTP used with the library file "DVS.Utilities.PlainFTP.dll.
- The logging of administrative actions with respect to user account activation and deactivation was considered to be deficient.
- There were noted differences between the defined accounts and noted password policies

2.2 ICP SECURITY ASSESSMENT

The Democracy Suite was subjected to Security Testing in accordance with the requirements of Section 7 of Volume I and Section 6.4 of Volume II of the VVSG. The purpose of the Security Test was to verify that security technologies implemented in the Democracy Suite to secure the hardware, software, and storage media during pre-voting, voting, and post-voting activities perform as documented in the Dominion-supplied technical documentation and that it meets the requirements of the VVSG.

The Security Test was performed by running a security test suite to provide verification of the access controls and the physical controls documented by Dominion and to gather the necessary information. The information gathered was provided to a certified security professional for analysis.

2.3 ICE SECURITY ASSESSMENT

All external I/O connections appeared to perform as stated in the TDP.

- USB ports were checked during boot up process and during operation. They appeared to be disabled as stated in the TDP.
- The RJ45 connections on the side of the system were checked. The rearmost connector only allows for operation of the ATI device. The forward connector (network) does give a physical connection (link light) but is disabled. No communication was made with the system and no information was gleaned from the system through this connector.
- The rear RJ11 connector is for the lighting system as stated in the TDP.

In conjunction with and during an unrelated ICE usability test that included ATIs, an ICE unit was also set up in accordance with WoP6b to test if "physical security elements worked as specified by the vendor in their TDP." Another ICE unit being used in the usability test was employed as a control and reference. Utilizing the usability test allowed for the physical security elements to be evaluated while the unit was being use (i.e. was physical security impacted by the need to use actually use an ATI, change printer paper, etc.). During this test three physical security concerns were noted and communicated to the manufacturer. These included the below. The manufacture has since addressed these concerns.

- A hole was found in the ballot box large enough to insert ballots.
- Following the TDP no tamper indicators were placed on the ballot box locks.
- Following the TDP no tamper indicators were placed on the rear printer panel.

Except for the above mentioned concerns, all physical access points appeared to be locked and/or sealed with tamper resistant bands, seals, or indicators. The touchscreen performs as expected and did not appear to contain any Admin/Tech backdoors. The boot order process could not be manipulated.

In *2.03, ICE Functional Description, Section 4.1.2, Paper-based System requirements*: *Opening the Poll* it states, "authenticate the software version (in Technician menu SHA256 can be calculated for every component in the system. The calculated values should be compared with certified values that are given from the certification laboratory)." The manufacture does the initial build process and these values should be generated by them (the origin). They can be verified by the lab but should originally come from the vendor. Labs do have to keep a record and should Hash/serialize the software but this is for record purposes and should not be confused with what a technician should be doing during normal maintenance operations.

2.4 ICC SECURITY ASSESSMENT

The ICC is a central scanning system that utilizes two COTS devices. This system is intended to be physically isolated by the controlling jurisdiction through properly implemented physical access controls. The system documentation was reviewed to evaluate the vendor security recommendations and risk assessments.

Per the Dominion TDP Documentation, "security of the central count location is not the responsibility of Dominion Voting Systems. The official environment of the central count location is under the control of

the jurisdiction, which determines its own physical security requirements for their central count facility." (Dominion, 2.06, System Security Specifications)

2.5 TESTING NOTES: In many instances security related issues were also re-examined at different time intervals during the testing campaign performed by Wyle (e.g. functional examination of EMS User Roles). In such instances any security concerns discovered were addressed as part of those efforts. Also security issues were reported to Dominion Voting System as they become known. Since that time Dominion Voting Systems has updated their documentation, hardware, and applications to address these concerns.

The security testing executed on the Dominion system was completed by the Wyle staff with execution of the WoP's and a third party security consultant. The third party security contractor ran a number of tests and scans on the Dominion system in order to verify they meet the requirements within the 2005 VVSG. Execution of the security checks were not performed by the use of standard Wyle test cases, but were tested by a security expert to the VVSG standards under Wyle supervision.

Table 2-1 Dominion Security Test Matrix

"x" = to be tested **= not to be tested**

Tests	To be Tested				Results			
TESTS	**ICE**	**EMS**	**ICP**	**ICC**	**ICE**	**EMS**	**ICP**	**ICC**
Ports, Protocols, Services Scan	X		X		Pass		Pass	
Vulnerability Scan	X	X	X		Pass	Pass	Pass	
File permission checks on critical files/apps/directories	X	X	X	X	Pass	Pass	Pass	Pass
Account checks (*privileges, password*)	X	X	X	X	Pass	Pass	Pass	Pass
Test Verification Process	X	X	X	X	Pass	Pass	Pass	Pass
Attacks from key - TM	X	X	X	X	Pass	Pass	Pass	Pass
TDP Review	X	X	X	X	Pass	Pass	Pass	Pass
File Manipulation	X	X	X	X	Pass	Pass	Pass	Pass
Operating System Tests								
BIOS - order change, backdoor, potential mbr attack on crypto	X	X	X	X	Pass	Pass	Pass	Pass

Xwindows - bypass/short cut desktop		X				Pass		
Password policy enforcement	X	X	X	X	Pass	Pass	Pass	Pass
Hardware connections (USB,LAN)	X	X	X	X	Pass	Pass	Pass	Pass
Event Log	X	X	X	X	Pass	Pass	Pass	Pass
Application Tests								
Check installed software	X	X	X	X	Pass	Pass	Pass	Pass
Check "timeout"	X	X	X	X	Pass	Pass	Pass	Pass
Password Aging	X	X	X	X	Pass	Pass	Pass	Pass
Verify user name and password	X	X	X	X	Pass	Pass	Pass	Pass
Verify user roles	X	X	X	X	Pass	Pass	Pass	Pass
Transport Media Tests								
Dominion Approved Compact Flash	X	X	X	X	Pass	Pass	Pass	Pass
Compact Flash Clean or Cleared	X	X	X	X	Pass	Pass	Pass	Pass
Physical Security								
Machine disposables can be replaced without gaining access to internal components.	X	X	X	X	Pass	Pass	Pass	Pass
Verify that ballot counter cannot be reset except by authorized persons	X		X	X	Pass		Pass	Pass
Tamper evident tape and seals	X		X		Pass		Pass	
Bypass or defeat security environment	X	X	X	X	Pass	Pass	Pass	Pass
Ballot storage device is secure	X		X		Pass		Pass	
TDP Review	X	X	X	X	Pass	Pass	Pass	Pass
Verify software and firmware on unit reflects the TDP	X	X	X	X	Pass	Pass	Pass	Pass

3.0 CONCLUSION

Wyle Laboratories security tests were performed in parallel with efforts by the manufacture to update and improve their voting system. As security test results were realized they were communicated to the manufacture in a timely qualified manner. This dialog allowed the manufacture to address concerns and recommendations by updating their system and/or documentation while the test campaign proceeded. This interchange not only allowed for an in-depth testing of the system as originally presented but also allowed for the testing of revisions made by the manufacture. As such the final test results do not simply reflect the eventual test findings but also represent reiterated testing.

The security threat and risk assessments for these tests were based upon the initial ***Test Case Procedure Specification*** and the relevant VVSG requirements. Ultimately it was determined that all security test concerns were adequately addressed by the manufacture.

Wyle has therefore determined that the Democracy Suite 4.0 is compliant with the security requirements of the EAC 2005 VVSG.