Dominion Democracy Suite 5.2
Security and Telecommunications Test Report

CDV-306-STR-01

Prepared for:

Vendor Name	*Dominion Voting Systems*
Vendor System	*Democracy Suite 5.2*

Prepared by:

SLI Compliance[SM]
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

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

Revision History

Release	Author	Revision Summary
1.0	M. Santos	Initial Release

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

Overview

This test report provides results for the security testing of the **Dominion Democracy Suite 5.2** voting system.

Security and Telecommunications testing covered:

- Top-level system design and architecture
- System documentation and procedures
- Testing of relevant software and operating system configuration for pertinent vulnerabilities
- Testing of hardware, including examination of unused hardware ports and security measures applied to those ports
- Testing of system communications, including encryption of data as well as protocols and procedures for access authorization

Testing was implemented without any prior knowledge of the source code.

The testing was divided into three phases.

Phase I included review of all pertinent documents for appropriate processes and procedures for implementing a secure system. This included review of the system design and architecture.

Phase II included testing of relevant software, operating systems, and hardware configurations.

Phase III included testing of all telecommunications aspects of the system.

Phase I - Documentation Review

During Phase I testing, documentation was reviewed to verify and validate the following types of requirements:

- Top-level system design and architecture
- System documentation and procedures

During Phase I testing, documentation was reviewed to verify and validate the following requirements:

- 7.2.2 Access control identification
- 7.3.1 Polling place security
- 7.3.2 Central count location security
- 7.4.1 Software and firmware installation
- 7.4.2 Protections against malicious software
- 7.4.3 Software distribution and setup validation
- 7.4.4 Software Distribution
- 7.4.5 Software Reference Information
- 7.4.6 Software Setup Validation
- 7.8.1 Access control

See the applicable section below for more details on these requirements and the review results.

During Phase I testing, an issue log of any errors and omissions found in the documentation or anomalies encountered was maintained.

7.2.2 Access Control Identification

a. The voting system **shall** identify users and processes to which access is granted and the specific functions and data to which each entity holds authorized access.

b. Voting system equipment that implements role-based access control **shall** support the recommendations for Core RBAC in the ANSI INCITS 359-2004 American National Standard for Information Technology- Role Based Access Control document.

c. Voting system equipment **shall** allow the administrator group or role to configure the permissions and functionality for each identity, group, or role to include account and group/role creation, modification, and deletion.

Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

7.3.1 Polling Place Security

For polling place operations, manufacturers **shall** develop and provide detailed documentation of measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences.

The measures **shall** allow the immediate detection of tampering with vote casting devices and precinct ballot counters.

Review of the TDP validated that the requirement was satisfactorily covered.

7.3.2 Central Count Location Security

Manufacturers **shall** develop and document in detail the measures to be taken in a central counting environment. These measures **shall** include physical and procedural controls related to the handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.

Review of the TDP validated that the requirement was satisfactorily covered.

7.4.1 Software and Firmware Installation

The system **shall** meet the following requirements for installation of software, including hardware with embedded firmware.

a. Air Gap Architecture

   i. Every voting system **shall** be capable of being deployed in a segregated dual-installation architecture to protect against propagation of viruses. The architecture **shall** allow elections officials to use one or more, permanent server(s) and set of central-office voting devices, known to be running unaltered, certified software and firmware to create memory cards before each election and to use another, physically separate “sacrificial” server and set of voting devices after the election to tabulate results and generate reports. The architecture **shall** allow transfer of the election definition and tally database from the permanent server(s) to the sacrificial server using a write-once medium, such as a CD-R. The voting system architecture **shall** allow each installation to use its own Ethernet network, port server, and central-office vote-recording units, including any DRE and optical scan units, permitting the two installations to be segregated and air-gapped to ensure that there are no cross connections. An air gap is established by keeping two installations/networks physically separate and seeing that no device attached to the sacrificial installation/network is connected (directly or indirectly) to the first network, ensuring that data cannot flow from one installation/network to the other.

ii. The TDP for the voting system **shall** provide full procedures and instructions, to be incorporated into the Official Use Procedures for the voting system, to implement the segregated dual-installation architecture.

b. Voting and Tabulating Units

i. If software is resident in the system as firmware, the manufacturer **shall** require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations.

ii. To prevent alteration of executable code, no software **shall** be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.

iii. The voting system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote counting program, and its associated exception handlers.

iv. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.

v. After initiation of Election Day testing, no source code or compilers or assemblers **shall** be resident or accessible.

Review of the TDP validated that the requirement was satisfactorily covered.

7.4.2 Protection against Malicious Software

Voting systems **shall** deploy commercial-off-the-shelf (COTS) protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs.

Manufacturers **shall** develop and document the procedures to be followed to ensure that such protection is maintained in a current status. Virus and malware protection software and updates **shall** be installed using transportable portable media only and **shall not** be installed by download from the Internet.

Review of the TDP validated that the requirement was satisfactorily covered.

7.4.3 Software Distribution and Setup Validation

Subsections 7.4.4, 7.4.5 and 7.4.6 specify requirements for the distribution of voting system software and the setup validation performed on voting system equipment. These requirements are applicable to voting systems that have completed certification testing.

7.4.4 Software Distribution

The manufacturer **shall** document all software including voting system software, third party software (such as operating systems and drivers) to be installed on the certified voting system, and installation programs.

a. The documentation **shall** have a unique identifier (such as a serial number or part number) for the following set of information: documentation, software manufacturer name, product name, version, the certification application number of the voting system, file names and paths or other location information (such as storage addresses) of the software.

b. The documentation **shall** designate all software files as static, semi-static or dynamic.

Review of the TDP validated that the requirement was satisfactorily covered.

7.4.5 Software Reference Information

a. The manufacturer **shall** provide the NSRL, any California certified escrow facility, pursuant to Title 2, Division 7, Chapter 6 of the California Code of Regulation, and the Office of the Secretary of State with a copy of the software installation disk, including the executable binary images of all third party software. Further, the manufacturer **shall** deposit the source code, tools, and documentation, to allow the complete and successful compilation of a system in its production/operation environment.

   i. The manufacturer **shall** document that the process used to verify the software distributed on unalterable storage media is the certified software by using the reference information provided by the NSRL or other designated repository before installing the software.

c. The manufacturers **shall** document to whom they provide voting system software.

Review of the TDP validated that the requirement was satisfactorily covered.

7.4.6 Software Setup Validation

g. Setup validation methods **shall** verify the contents of all system storage locations (e.g., system registers, variables, files, etc.) containing election

specific information (e.g., ballot style, candidate registers, measure registers, etc.).

i. The manufacturer **shall** document the default values of all system storage locations that hold election specific information.

Review of the TDP validated that the requirement was satisfactorily covered.

7.8.1 Access Control

The accredited testing laboratory **shall** conduct tests of system capabilities and **review** the access control policies and procedures submitted by the manufacturer to identify and verify the access control features implemented as a function of the system.

Specific activities to be conducted by the S-ATA **shall** include:

a. A review of the manufacturer's access control policies, procedures and system capabilities to confirm that all requirements have been addressed completely.

Review of the TDP validated that the requirement was satisfactorily covered.

Phase II - Functional Security Testing

Phase II testing included:

- Testing of relevant software and operating system configuration, for pertinent vulnerabilities
- Testing of hardware, including examination of unused hardware ports, and security measures applied to those ports

During Phase II, functional tests were exercised in order to verify and validate the following requirements:

- 5.4.3 In-process Audit Records
- 7.2.1 General access control
- 7.2.2 Access control identification
- 7.2.3 Access control authentication
- 7.2.4 Access control authorization
- 7.3 Physical security measures
- 7.3.1 Polling place security
- 7.3.2 Central count location security
- 7.4.1 Software and firmware installation
- 7.4.2 Protection against malicious software
- 7.4.3 Software distribution and setup validation
- 7.4.5 Software Reference Information
- 7.4.6 Software Setup Validation
- 7.6 Telecommunications and data transmission
- 7.6.1 Maintaining Data Integrity
- 7.6.2 Election Returns
- 7.8.1 Access Control
- 7.8.2 Data Interception and Disruption

See the applicable section below for more details on these requirements and the test results.

An issue log of any errors, omissions, or anomalies found in the documentation was maintained.

5.4.3 In-process Audit Records

iv. Notification of system login or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing

Testing performed: As all other requirements were being tested, the audit log was reviewed to verify that appropriate records were recorded for the events occurring.

Applicable to: Election Management System (EMS), Adjudication (ADJ), ImageCast® Central (ICC), ImageCast® Evolution (ICE), ImageCast® X (ICX), and workstation/device environment.

Review of the requirement showed that the ICX device does not provide monitoring of physical security.

Additionally, the ICX does not provide hash values for exported log files, which allows for potential modification after export.

The EMS work stations did not provide information regarding invalid login attempts at the application level. Operating system level did provide log information.

Audit logs are located within the Election Event Designer (EED) but only deal with actions taken after the voting project has been opened (with credentials). Operating system logs provide detail at the operating system level.

The ADJ is controlled strictly by the windows login credentials and the Results Tally and Reporting (RTR) system. There are, however, no login prompts to launch or operate the ADJ functionality.

The ICC has audit logs that detail invalid logins and other systems functions but the audit log, as far as can be verified, only displays recent time and not date. This log also appears to be able to be cleared and does not contain multiple days of logs. There is no permanent log for the ICC scanning system. The ICC workstation operating system does provide log information at the operating system level.

Review of the requirement demonstrated that the requirement was partially covered.

7.2.1 General Access Control

a. Voting system equipment **shall** provide access control mechanisms designed to permit authorized access to the voting system and to prevent unauthorized access to the voting system.

i. Access control mechanisms on the EMS shall be capable of identifying and authenticating individuals permitted to perform operations on the EMS.

b. Voting system equipment shall provide controls that permit or deny access to the device's software and files.

c. The default access control permissions shall implement the minimum permissions needed for each role or group identified by a device.

d. The voting device shall prevent a lower-privileged process from modifying a higher-privileged process.

e. An administrator of voting system equipment shall authorize privileged operations.

f. Voting system equipment shall prevent modification to or tampering with software or firmware through any means other than the documented procedure for software upgrades.

Testing performed: Tests were performed on each user role within the voting system in order to verify that a user is allowed to perform all necessary tasks for their role, but is not allowed to perform any tasks not assigned to their role, nor are they able to modify a role to a higher level role activity.

Tests were performed to verify that all voting system equipment prevents modification of related software/firmware by any means other than the documented procedure for software upgrades. Tests were performed to verify that tampering is not allowed.

Applicable to: EMS, Adjudication, ICC, ICE, and ICX.

The only thing that was questionable, under (b) or (c), was that an under privileged user was able to get a full user listing of the EMS system, and while the user was not able to manipulate the accounts in any way, they had successfully acquired a full user list for the EED or RTR systems. At the operating system level, appropriate controls are in place to permit or deny access to users attempting to gain access to the environment.

Review of the requirement validated that the requirement was satisfactorily covered.

7.2.2 Access Control Identification

d. The voting system **shall** identify users and processes to which access is granted and the specific functions and data to which each entity holds authorized access.

e. Voting system equipment that implements role-based access control **shall** support the recommendations for Core RBAC in the ANSI INCITS 359-2004 American National Standard for Information Technology- Role Based Access Control document.

f. Voting system equipment **shall** allow the administrator group or role to configure the permissions and functionality for each identity, group, or role to include account and group/role creation, modification, and deletion.

Testing performed: Tests were performed on each user role within the voting system in order to verify that a user is allowed to perform all necessary tasks for their role and are appropriately identified by the system.

Applicable to: EMS, Adjudication, ICC, ICE, ICX, and workstation/device environment.

Review of the requirement validated that the requirement was satisfactorily covered.

7.2.3 Access Control Authentication

The following authentication requirements apply to all voting system equipment.

a. Voting system equipment **shall** authenticate users prior to granting them access to system functions or data.

b. When private or secret authentication data is stored in voting system equipment, the data **shall** be protected to ensure that the confidentiality and integrity of the data is not violated.

c. Voting system equipment **shall** allow the administrator group or role to set and change passwords, pass phrases, and keys.

d. Voting system equipment **shall** allow privileged groups or roles to be disabled and allow new individual privileged groups or roles to be created.

e. Voting system equipment **shall** lock out groups, roles, or individuals after a specified number of consecutive failed authentication attempts within a predefined time period.

f. Voting systems **shall** allow the administrator group or role to configure the account lock out policy, including the time period within which failed attempts must occur, the number of consecutive failed access attempts allowed before lock out, and the length of time the account is locked out.

g. If the voting system uses a user name and password authentication method, the voting system **shall** allow the administrator to enforce password strength, histories, and expiration.

h. The voting system **shall** allow the administrator group or role to specify password strength for all accounts, including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters.

i. The voting system **shall** enforce password histories, and allow the administrator to configure the history length.

j. Voting system equipment **shall** ensure that the username is not used in the password.

k. Voting systems **shall** provide a means to automatically expire passwords in accordance with the voting jurisdiction's policies.

Testing performed: Tests were performed to verify that the administrator group or role is able to perform all the functions listed in the requirements above. Tests were performed that verify that users are authenticated properly prior to being allowed access, and that all private access data is secured properly. Tests were performed to verify that usernames are not allowed to be part of the password.

Applicable to: EMS, Adjudication, ICC, ICE, ICX and workstation/device environment.

Review of requirement 7.2.3.e showed that there is no ability to configure lockout, password history, or expiration in the voting specific software for EMS passwords. The ICX allows expiration dates for ICX smart cards during programming. However, testing of the feature determined that the expiration date did not work. Per the Dominion representative, the expiration date is not active in this version of the software; however, it will be in later versions.

The Windows Operating System has lockout and password policies in effect.

Review of requirement 7.2.3.f showed that for the EMS there is no lockout, password history, or expiration in the voting specific software. The Windows Operating System has lockout and password policies in effect.

Review of requirement 7.2.3.g showed that there is no lockout, password history, or expiration in the voting specific software. The Windows Operating System has lockout and password policies in effect.

There is the ability to set ibutton and smartcard passcode length to between four and eight characters. However, there are no histories or expirations for ibuttons or smartcards. There is a smartcard expiration date field with a date, but currently the functionality is not implemented.

The EMS system EED and RTR currently are forced to have ten-character complex passwords; however, there are no easily distinguished ways to set expiration of accounts, nor are there ways to set a password history.

Review of requirement 7.2.3.h showed that EMS specifications state that EED/RTR user account password complexity can be changed; however, it was determined that the password complexity functionality is not implemented. Windows based operating systems have password policy requirements specified for OS login.

The ICX passcode length field on the ICX is limited to eight characters.

Review of requirement 7.2.3.i determined that password history functionality is not implemented in election system specific systems. Operating system specific password policies are in effect, including password history.

Review of requirement 7.2.3.j showed that SLI could enable random generation of ibutton and smartcard pin numbers of between four and eight characters. In the EED and RTR user accounts, SLI was able to create user accounts with passwords that contained usernames. All windows based authentication credentials prohibited username as part of the password.

In review of requirement 7.2.3.k, it was determined the ability to expire passwords/passcodes or user accounts for any of the **Dominion Democracy Suite 5.2** products is not implemented. Operating System specific functionality provides the ability to expire passwords/passcodes or user accounts.

Review of the requirement demonstrated that the requirement was partially covered.

7.2.4 Access Control Authorization

a. Voting systems **shall** ensure that only authorized roles, groups, or individuals have access to election data.

b. Voting systems **shall** explicitly authorize subject's access based on access control lists or policies.

c. Voting systems **shall** explicitly deny subject's access based on access control lists or policies.

Testing performed: Tests were performed on each user role within the voting system in order to verify that only authorized users, roles, or groups are allowed access to election data, based on pertinent access control lists or policies.

Applicable to: Adjudication, ICC, ICE and workstation/device environment.

Review of the requirement validated that the requirement was satisfactorily covered.

7.3 Physical Security Measures

a) Any unauthorized physical access **shall** leave physical evidence that an unauthorized event has taken place.

b) Voting systems **shall** only have physical ports and access points that are essential to voting operations and to voting system testing and auditing.

c) An event log entry that identifies the name of the affected device **shall** be generated if a component connected to a piece of voting system equipment is disconnected while polls are open.

d) Ports disabled while polls are open **shall** only be re-enabled by authorized administrators.

e) Access points, such as covers and panels, **shall** be secured by locks or tamper evident seals or tamper resistant countermeasures **shall** be implemented so that system owners can monitor access to voting system components through these points.

f) Ballot boxes **shall** be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.

Testing performed: Tests were performed to verify that unauthorized physical access leaves physical evidence of the intrusion. Tests were performed to verify that only ports and access points essential to voting operations, testing, and auditing are present. In addition, tests were performed to verify that event log entries adequately identify affected devices. Tests were also performed to verify ports disabled during the open polls period can only be re-enabled by an authorized administrator. Tests were performed to verify that all access points and ballot boxes are secured and provide adequate tamper evidence as well as tamper resistant countermeasures.

Applicable to: EMS, Adjudication, ICC, ICE, and ICX.

Review of requirement 7.3.d showed that for the ICX, all ports are enabled on the system; however, physical access to these ports is restricted.

Review of the requirement demonstrated that the requirement was partially covered.

7.3.1 Polling Place Security

For polling place operations, manufacturers **shall** develop and provide detailed documentation of measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences.

The measures **shall** allow the immediate detection of tampering with vote casting devices and precinct ballot counters.

Testing performed: Tests were performed to verify that the documented measures provide adequate polling place security.

Applicable to: ICE and ICX.

Review of the requirement validated that the requirement was satisfactorily covered.

7.3.2 Central Count Location Security

Manufacturers **shall** develop and document in detail the measures to be taken in a central counting environment. These measures **shall** include physical and

procedural controls related to the handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.

Testing performed: Tests were performed to verify that the documented measures provide adequate central count location security.

Applicable to: ICC, Adjudication, and EMS.

Review of the requirement validated that the requirement was satisfactorily covered.

7.4.1 Software and Firmware Installation

The system **shall** meet the following requirements for installation of software, including hardware with embedded firmware.

b. Voting and Tabulating Units

i. To prevent alteration of executable code, no software **shall** be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.

ii. The voting system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote counting program, and its associated exception handlers.

iii. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.

iv. After initiation of Election Day testing, no source code or compilers or assemblers **shall** be resident or accessible.

Testing performed: Tests were performed to verify that if any software or firmware is installed, unless the documentation details how to protect it, it is inaccessible to activation or control by anything other than authorized means. Tests were performed to verify that no source code or compilers or assemblers are resident or accessible, after election day testing.

Applicable to: EMS, Adjudication, ICC, ICE, ICX and workstation/device environment.

Review of the requirement validated that the requirement was satisfactorily covered.

7.4.2 Protection against Malicious Software

Voting systems **shall** deploy commercial-off-the-shelf (COTS) protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs.

Manufacturers **shall** develop and document the procedures to be followed to ensure that such protection is maintained in a current status. Virus and malware protection software and updates **shall** be installed using transportable portable media only and **shall not** be installed by download from the Internet.

Testing performed: Tests were performed to verify that COTS products are implemented to protect against malicious software, as described in voting system manufacturer documentation.

Applicable to: EMS, Adjudication, ICC, ICE, ICX and workstation/device environment.

Review of requirement 7.4.2 showed that on the EMS Server, the AVAST Antivirus (AV) File Shield (the real time AV monitor) was only able to detect and clean one of the four European Institute for Computer Antivirus Research (EICAR) files which potentially leaves the system open to zipped and double zipped viruses as well as infection strings in plain text.

The ICX system is currently an Android tablet device and contains no form of AV protection.

The ICE system is a proprietary system that utilizes firmware and compact flash cards to run, load, and store election based software. This system contains no AV protection.

Review of the requirement demonstrated that the requirement was partially covered.

7.4.3 Software Distribution and Setup Validation

Subsections 7.4.4, 7.4.5 and 7.4.6 specify requirements for the distribution of voting system software and the setup validation performed on voting system equipment. These requirements are applicable to voting systems that have completed certification testing.

Testing performed: This requirement is met by successful validation of 7.4.4, 7.4.5, and 7.4.6.

Applicable to: EMS, Adjudication, ICC, ICE, ICX and workstation/device environment.

Review of the requirement validated that the requirement was satisfactorily covered.

Software Reference Information

a. The voting system equipment **shall** be designed to allow the voting system administrator to verify that the software is the certified software by comparing it to reference information produced by the NSRL or other designated repository.

Testing performed: Tests were performed to verify that the software can be verified to meet the National Software Reference Library (NSRL) reference information.

Applicable to: EMS, Adjudication, ICC, ICE, ICX and workstation/device environment.

Review of the requirement validated that the requirement was satisfactorily covered.

7.4.6 Software Setup Validation

a. Setup validation methods **shall** verify that only authorized software is present on the voting equipment. Authorized software is COTS software components needed to run the voting system and voting software components identified by the manufacturer as authorized.

b. The manufacturer **shall** provide a method to comprehensively list all software files that are installed on voting systems.

   i. This method **shall** list version names and numbers for all application software on the voting system.

   ii. This method should list of the date of installation for all application software on the voting system.

c. Setup validation methods **shall** include a software verification method that ensures that the voting system software has not been modified illegitimately.

   i. The voting systems **shall** include any supporting software and hardware necessary to conduct the software verification method.

   ii. The manufacturer **shall** document the process used to conduct the software verification method.

   iii. The software verification method **shall** not modify the voting system software on the voting system.

d. Voting systems **shall** include a software verification method that either verifies software prior to installation or a method that verifies software using an external interface. Voting systems may include both software verification methods. Voting systems may provide ancillary setup validation methods, including methods for verifying or identifying installed software, other than those described in this section. There are no specific requirements for ancillary setup validation methods. However, any method intended to serve

as the voting system software verification method must meet the requirements outlined in this section.

e. Voting systems which implement a software verification method that verifies software prior to installation **shall** meet the following requirements.

   i. The voting system **shall** contain no more than one method for installing, updating, or removing software on a system.

      - Voting system equipment **shall** prevent processes from installing software except for the one specific software installation process identified by the manufacturer.
      - The voting system manufacturer **shall** document the procedures for installing, updating, and removing voting system software, configuration files, and data files.
      - Voting system equipment **shall** prevent processes from installing, updating or removing software while the polls are open.
      - Voting system equipment **shall** prevent the execution of software not installed using the specified software installation process.

   ii. The voting system **shall** only allow authenticated administrators to install software on voting equipment. The voting system **shall** present the administrator with a description of the software change being performed, including:

      - A list of all applications and/or file names being updated.
      - The type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file)

   iii. Voting system equipment **shall** store the current version identification of all software installed on the voting system equipment.

      - The current version identification **shall** be included as part of reports created by the voting system equipment.
      - The current version identification **shall** be displayed as part of the voting system equipment start up process.

   iv. The process for installing, updating and removing software **shall** make software changes based on information contained in software update packages. Software update packages **shall** minimally contain the following information:

      - A unique identifier for the software update package.
      - Names of the applications or files modified during the update process.

- Version numbers of the applications or files modified during the update process.
- Any software prerequisites or dependencies for the software involved in the update.
- A description of the type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file).
- The binary data of any new or updated files involved in the update process.

v. The software update package **shall** be formatted in a non-restrictive, publicly-available format. Manufacturers **shall** provide a specification describing how they have implemented the format with respect to the manufacturer's specific voting devices and data, including such items as descriptions of elements, attributes, constraints, extensions, syntax and semantics of the format, and definitions for data fields and schemas.

vi. vi. Software update packages **shall** be digitally signed by using a NIST approved algorithm with a security strength of at least 112 bits. vii. The software installation process **shall** verify digital signatures, software version identification, software prerequisites and dependencies, and manufacturer specific authorization information associated with the software before the software is installed. The software installation process **shall** not install software with invalid digital signatures, version numbers, or manufacturer specific authorization information, and **shall** not install software on systems that do not meet the update requisites.

vii. The voting system **shall** have the capability to prevent the installation of previous versions of applications or files.

viii. The software installation process **shall** result in information being stored in the voting system equipment's log such that altering or deleting log entries or the log was detected.

ix. The minimum information to be included in the voting system equipment log **shall** be:

- Success or failure of the software installation process;
- Cause of a failed software installation (such as invalid version identification, digital signature, etc.);
- Application or file name(s), and version number(s);
- A description of the type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file);

- A cryptographic hash of the software update package using FIPS 1402 level 1 or higher validated cryptographic module.

f. If software is verified after being installed on the voting system equipment, the voting system equipment **shall** provide an external interface to the location of the voting system software for software verification purposes.

   i. The external interface:

      - **Shall** be protected using tamper evident techniques,
      - **Shall** have a physical indicator showing when the interface is enabled and disabled
      - **Shall** be disabled during voting
      - Should provide a direct read-only access to the location of the voting system software without the use of installed software ii. The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system manufacturer.
      - If the process uses hashes or digital signatures, then the verification software **shall** use a FIPS 140-2 level 1 or higher validated cryptographic module.
      - The verification process **shall** either (a) use reference information on unalterable storage media received from the repository or (b) verify the digital signature of the reference information on any other media.

g. Setup validation methods **shall** verify the contents of all system storage locations (e.g., system registers, variables, files, etc.) containing election specific information (e.g., ballot style, candidate registers, measure registers, etc.).

   i. The manufacturer should provide a method to query the voting system to determine the value contained in all system storage locations containing election specific information.

Testing performed: Tests were performed to verify that the installation process for each system component is robust and maintains the integrity of the voting system.

Applicable to: EMS, Adjudication, ICC, ICE, ICX and workstation/device environment.

Review of requirement 7.4.6.b.i shows that Dominion specifies what is required to complete software validation but does not specifically supply the required software or hardware to do so. In the case of the ICX third party, Android developer tools were required to pull packages from the ICX device for hashing.

Review of requirement 7.4.6.c.i shows that Dominion specifies what is required to complete software validation but does not specifically supply the required software

or hardware to do so. In the case of the ICX third party, Android developer tools were required to pull packages from the ICX device for hashing.

Review of requirement 7.4.6.e.i.4 shows that the ICX hardware is set to not allow unsigned Android Package Kits (APK) from being installed; however, with the Tech Card there is nothing voting system specific that prevents additional package files from being installed.

Review of requirement 7.4.6.e.v shows that SLI was able to replace digitally signed application installers with renamed executables without the installation package failing.

SLI was able to modify election specific installers utilizing a hex editor to change minor things including mouse over text and digital signature names.

SLI was able to take installers from previous versions of the installation package and use them to install older versions of the software from the Democracy Suite installation.

SLI believes it would be possible to inject more lethal payloads into the installers given the opportunity.

Review of requirement 7.4.6.e.vi shows that SLI was able to install the newer version of the ICX software without having to uninstall the older version. SLI was able to update the ICE without having to uninstall the older version.

Review of requirement 7.4.6.e.viii.1 shows that SLI review of system logs on ICE, ICX, and EMS systems did not locate entries that dealt with a failed or successful installation of software. Operating System level logs did provide information on installation of software.

Review of requirement 7.4.6.e.viii.2 shows that SLI review of system logs on ICE, ICX, and EMS systems did not locate entries that dealt with cause of a failed installation of software. Operating System level logs did provide information on failed installation of software.

Review of requirement 7.4.6.e.viii.4 shows that SLI review of system logs on ICE, ICX, and EMS systems did not verify these specific details because there was no visual representation of the actions performed; not every application had these specific details provided. Operating System level logs did provide information.

Review of requirement 7.4.6.f.i.2 determined that the ICX does not have visual indicators showing if the port is enabled or disabled. This requirement is considered to be failed.

Review of requirement 7.4.6.f.i.3 determined that the ICX does not have visual indicators showing that the port is disabled during voting. This requirement is considered to be failed.

Review of requirement 7.4.6.f.i.3 determined that there is not a specific method to be able to verify or determine exactly all contents on the system. This requirement is considered to be failed.

Review of the requirement demonstrated that the requirement was partially covered, with fails on some of the sub-requirements.

7.6 Telecommunications and Data Transmission

There are four areas that must be addressed by telecommunications and data transmission security capabilities: access control, data integrity, detection and prevention of data interception, and protection against external threats.

7.6.1 Maintaining Data Integrity

Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function.

a. Voting systems that use electrical or optical transmission of data **shall** ensure the receipt of valid vote records is verified at the receiving station. This should include standard transmission error detection and correction methods such as checksums or message digest hashes. Verification of correct transmission **shall** occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.

    i. Cryptography used to verify the receipt of vote records **shall** use NIST approved algorithms with security strength of at least 112 bits. Message Authentication Code (MAC) keys **shall** have a security strength of at least 112 bits.

Testing performed: Tests were performed to verify that data is properly encrypted and that receipt is verified.

Applicable to: EMS, Adjudication, and ICC

Individual public facing voting components are not networked, nor do they transmit individual voting results. This includes the ICE and the ICX Ballot Marking Device (BMD). The only telecommunications that are in use are an isolated closed network to link the EMS/ADJ/ICC devices together at a central count location. Operating system level transmissions provided appropriate encryption and receipt validation.

Review of the requirement validated that the requirement was satisfactorily covered.

7.6.2 Election Returns

If the voting system provides access to election returns or interactive inquiries, the system **shall**:

a. Allow authorized administrators the ability to disable or restrict access to election returns (for equipment that operates in a central counting environment). This requirement applies as well to polling place equipment that contains a removable memory module or that may be removed in its entirety to a central place for the consolidation of polling place returns

b. Design voting system software and its security environment such that data accessible to interactive queries resides in an external file or database created and maintained by the elections software under the restrictions applying to any other output report:

   i. The output file or database has no provision for write access back to the system

   ii. Persons whose only authorized access is to the file or database are denied write access, both to the file or database, and to the system

Testing performed: Tests were performed to determine that if the system provides access to election returns or interactive queries, then the authorized administrators can disable or restrict access, and that the data resides in an external file or database governed by the voting system.

Applicable to: EMS and Adjudication

Review of the requirement validated that the requirement was satisfactorily covered.

7.8.1 Access Control

For those access control features built in as components of the voting system, the S-ATA **shall design tests to confirm that these security elements work as specified**.

Specific activities to be conducted by the S-ATA **shall** include:

b. Specific tests designed by the S-ATA to verify the correct operation of all documented access control procedures and capabilities, including tests designed to circumvent controls provided by the manufacturer. These tests **shall** include:

   i. Performing the activities that the jurisdiction will perform in specific accordance with the manufacturer's access control policy and procedures to create a secure system, including procedures for software and firmware installation

ii. Performing tests intended to bypass or otherwise defeat the resulting security environment. These tests **shall** include simulation of attempts to physically destroy components of the voting system in order to validate the correct operation of system redundancy and backup capabilities

This review applies to the full scope of system functionality. It includes functionality for defining the ballot and other pre-voting functions, as well as functions for casting and storing votes, vote canvassing, vote reporting, and maintenance of the system's audit trail.

Testing performed: Tests were performed to verify the documented procedures as well as attempts to defeat the implemented access control security on each system component.

Applicable to: EMS, Adjudication, ICC, ICE, ICX and workstation/device environment.

Review of the requirement validated that the requirement was satisfactorily covered.

7.8.2 Data Interception and Disruption

For systems that use telecommunications, as provided for in section 6 of the Standards and consistent with California law, to transmit official voting data, the S-ATA **shall** review, and conduct tests of, the data interception and prevention safeguards specified by the manufacturer in its TDP. The S-ATA **shall** evaluate safeguards provided by the manufacturer to ensure their proper operation, including the proper response to the detection of efforts to monitor data or otherwise compromise the system.

Testing performed: Testing was performed to verify appropriate encryption, receipt validation and data integrity against any attempts to compromise the system.

Applicable to: EMS, Adjudication, ICC, ICE, ICX and workstation/device environment.

Individual public facing voting components are not networked nor do they transmit individual voting results. This includes the ICE and the ICX BMD. The only telecommunications that are in use are an isolated closed network to link the EMS/ADJ/ICC devices together at a central count location. Operating system level transmissions provided appropriate encryption, receipt validation, and data integrity.

Review of the requirement validated that the requirement was satisfactorily covered.

Phase III – Telecommunications and Data Transmission Testing

During Phase III, tests were conducted in order to verify and validate the following requirements:

- Testing of system communications, including encryption of data, as well as protocols and procedures for access authorization

In this phase, tests were exercised in order to verify and validate the following requirements:

- 6.1.2 Data Transmission
- 6.2.1 Confirmation

See the applicable section below for more details on these requirements and the test results.

An issue log of any errors, omissions, or anomalies found in the documentation was maintained.

6.1.2 Data Transmission

These requirements apply to the use of telecommunications to transmit data for the preparation of the system for an election, the execution of an election, and the preservation of the system data and audit trails during and following an election. While this section does not assume a specific model of voting system operations and does not assume a specific model for the use of telecommunications to support such operations, it does address the following types of data, where applicable:

Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmits votes individually

Ballot Definition: Information that describes to a voting machine the content and appearance of the ballots to be used in an election

Vote Count: Information representing the tabulation of votes at any level within the control of the jurisdiction, such as the polling place, precinct or central count

List of Voters: A listing of the individual voters who have cast ballots in a specific election

Additional data transmissions used to operate a voting system in the conduct of an election, but not explicitly listed above, are also subject to the requirements of this section.

Testing performed: Testing was performed to verify appropriate encryption, receipt validation, and data integrity.

Applicable to: EMS, Adjudication, ICC, ICE, ICX and workstation/device environment.

Nessus vulnerability scans were conducted on all devices that were connected to the private EMS network. These included the EMS Server, EMS work Station, Adjudication workstation, and ICC system. Operating system level transmissions provided appropriate encryption, receipt validation, and data integrity.

Review of the requirement validated that the requirement was satisfactorily covered.

6.2.1 Confirmation

Confirmation occurs when the system notifies the user of the successful or unsuccessful completion of the data transmission, where successful completion is defined as accurate receipt of the transmitted data. To provide confirmation, the telecommunications components of a voting system shall notify the user of the successful or unsuccessful completion of the data transmission. In the event of unsuccessful transmission the user shall be notified of the action to be taken.

Testing performed: Testing was performed to verify appropriate confirmation of data transmission to the user and actions to be taken, if any.

Applicable to: EMS, Adjudication, ICC and workstation/device environment.

Nessus vulnerability scans were conducted on all devices that were connected to the private EMS network. These included the EMS Server, EMS workstation, Adjudication workstation, and ICC system. Operating system level transmissions provided confirmation.

Review of the requirement validated that the requirement was satisfactorily covered.

Final Report

Within the **Dominion Democracy Suite 5.2,** issues were noted related to Audit logging, passwords, anti-virus, and installation aspects of the voting system at the DS 5.2 application level. Audit logging, installation and password aspects were deemed sufficient at the operating system level. None of these issues directly affect the functioning of the voting systems and could potentially be alleviated with manual processes.

As per the direction given by the California Secretary of State, this Security and Telecommunications testing report does not include any recommendation as to whether or not the system should be approved.

End of Test Report