Dominion Democracy Suite 5.10 Voting System Software Test Report for California Secretary of State

DOM-19002-CSTR-01

Vendor Name	*Dominion Voting Systems*
Vendor System	*Democracy Suite 5.10*

Prepared by:

SLI COMPLIANCE

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

Date	Release	Author	Revision Summary
6/27/2019	1.0	*M. Santos*	Initial Release
8/21/19	2.0	*M. Santos*	Updated for CASOS comments

Disclaimer

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

Trademarks

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

TABLE OF CONTENTS

INTRODUCTION **4**

SCOPE OF THE DOMINION DEMOCRACY SUITE 5.10 VOTING SYSTEM 4

REVIEW SPECIFICATIONS **5**

SOURCE CODE REVIEW 5

REVIEW RESULTS **7**

DISCREPANCIES 7

VULNERABILITIES 8

FINAL REPORT **9**

INTRODUCTION

This report outlines the test approach SLI Compliance (SLI) followed when performing Software Testing on the **Dominion Democracy Suite 5.10** voting system against the California Voting System Standards (CVSS).

Scope of the Dominion Democracy Suite 5.10 Voting System

This section provides a description of the scope of **Dominion Democracy Suite 5.10** Voting System components:

- Election Management System (EMS) Results Tally Reporting (RTR) application
- ImageCast Precinct 2 (ICP2) firmware/hardware
- ImageCast Evolution (ICE) firmware/hardware
- ImageCast X (ICX) firmware/hardware
- ImageCast Central (ICC) application

The **Dominion Democracy Suite 5.10** EMS represents a set of software applications (EMS, RTR, Adjudication) for pre-voting and post-voting election project activities that are applicable to jurisdictions of various sizes and geo-political complexities.

The ImageCast Precinct 2 is a precinct-based optical scan ballot tabulator that is used in conjunction with ImageCast compatible ballot storage boxes. The system is designed to scan marked paper ballots, interpret voter marks on the paper ballot, and safely store and tabulate each vote from each paper ballot.

The **Dominion Democracy Suite 5.10** ICE 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 **Dominion Democracy Suite 5.10** ICX ballot marking platform creates paper Electronic Mobile Ballots. These ballots are later scanned and tabulated by the ICC optical ballot counter and/or scanned, verified, and cast by the ICE.

The **Dominion Democracy Suite 5.10** ICC system consists of a central, high-speed, optical scan ballot counter (tabulator) called the ICC Ballot Counter and is used for processing absentee ballots (such as vote by mail). This ballot counter unit is based on commercial-off-the-shelf (COTS) hardware coupled with custom-made ballot processing application software. It is used for high-speed, accurate, and reliable centralized scanning and counting of paper ballots.

REVIEW SPECIFICATIONS

The following are the specifications for source code testing conducted on the **Dominion Democracy Suite 5.10** Voting System.

Source Code Review

The **Dominion Democracy Suite 5.10** Voting System includes proprietary software and firmware. The voting system code base was tested to the applicable CVSS requirements.

Review of the code included:

- Adherence to the applicable standards in sections 5 and 7 of the CVSS
- Adherence to other applicable coding format conventions and standards including best practices for the coding language used
- Analysis of the program logic and branching structure
- Evaluate whether the system is designed in a way that allows meaningful analysis, including:
  - Whether the architecture and code is amenable to an external review
  - Whether code analysis tools can be usefully applied
  - Whether the code complexity is at a level that obfuscates its logic

Security considerations reviewed against the code base included:

- Search for exposures to commonly exploited vulnerabilities
- Evaluate the use and correct implementation of cryptography and key management
- Analysis of error and exception handling
- Evaluate the likelihood of security failures being detected
  - Evaluate whether audit mechanisms are reliable and tamper resistant
  - Evaluate whether data that might be subject to tampering is properly validated and authenticated
- Evaluate the risk that a user can escalate his or her capabilities beyond those authorized
- Evaluate the design and implementation to ensure that sound, generally accepted engineering practices are followed, checking to verify that code is defensively written against:
  - Bad data
  - Errors in other modules
  - Changes in environment
  - User errors

- Other adverse conditions

- Evaluate for embedded, exploitable code (such as “Easter eggs”) that can be triggered to affect the system
- Evaluate the code for dynamic memory access features which would permit the replacement of certificated executable code or control data or insertion of exploitable code or data.
- Evaluate the code for use of runtime scripts, instructions, or other control data that can affect the operation of security relevant functions or the integrity of the data.

Components and coding languages involved in the voting system applications are shown in Table 1.

Table 1 – Democracy Suite 5.10 Components

Component	Language/s	Lines of Code	Standard
EMS	C#	1,682,875	Csharp_AutomatedCodeReview-5.10-CA.pdf
ICP2	C/C++	473,991	CPlusPlus_CodingStandard-5.10-CA.pdf
ICX	Java	166,547	dvs_JavaCodingStandards.pdf
ICE	C/C++	822,346	CPlusPlus_CodingStandard-5.10-CA.pdf
ICC	C/C++	234,812	CPlusPlus_CodingStandard-5.10-CA.pdf
ADJ	C#	189,280	Csharp_AutomatedCodeReview-5.10-CA.pdf

Source Code Review Tools utilized by SLI included:

- Module Finder: an SLI proprietary application used to parse module names from C/C++, Java and VB code and populate the identified module names into the review documents
- StyleCop: a commercial application used to review code to stated requirements
- Understand: a commercial application used to review code to stated requirements

REVIEW RESULTS

Discrepancies

Discrepancies are reported such that the California Secretary of State is provided with a basis for evaluating the extent to which the source code meets applicable standards.

EMS source code review

No source code requirements were found to be an issue within the EMS source code base reviewed; as a result, no discrepancies were written against the code base.

ICP2 source code review

No source code requirements were found to be an issue within the ICP source code base reviewed; as a result, no discrepancies were written against the code base.

ICX source code review

No source code requirements were found to be an issue within the ICX source code base reviewed; as a result, no discrepancies were written against the code base.

ICE source code review

No source code requirements were found to be at issue within the ICE source code base reviewed; as a result, no discrepancies were written against the code base.

ICC source code review

No source code requirements were found to be at issue within the ICC source code base reviewed; as a result, no discrepancies were written against the code base.

ADJ source code review

No source code requirements were found to be at issue within the ADJ source code base reviewed; as a result, no discrepancies were written against the code base.

Vulnerabilities

For any vulnerabilities discovered, SLI was tasked with identifying the particular standards applicable to each vulnerability.

To the extent possible, reported vulnerabilities include an indication of whether the exploitation of the vulnerability would require access by:

- Voter: Usually has low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine(s) for less than an hour.
- Poll worker: Usually has low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine(s) for up to one week, but all physical security has been put into place before the machines are received.
- Elections official insider: Wide range of knowledge of the voting machine design and configuration. May have unrestricted access to the machine for long periods of time. Their designated activities include:
  - Set up and pre-election procedures;
  - Election operation;
  - Post-election processing of results; and
  - Archiving and storage operations.
- Vendor insider: Great knowledge of the voting machine design and configuration. They have unlimited access to the machine before it is delivered to the purchaser and, thereafter, may have unrestricted access when performing warranty and maintenance service, and when providing election administration services.

SLI will not verify or demonstrate exploitability of the vulnerability but the report of the vulnerability will identify factors involved in the exploitation.

Any vulnerability theories developed by the source code review team members shall, to the extent possible, be referred to the Secretary of State staff.

EMS source code vulnerability review

No vulnerabilities were found within the EMS source code base reviewed; as a result, no findings were written against the code base.

ICP2 source code vulnerability review

No vulnerabilities were found within the ICP source code base reviewed; as a result, no findings were written against the code base.

ICX source code vulnerability review

No vulnerabilities were found within the ICX source code base reviewed; as a result, no findings were written against the code base.

ICE source code vulnerability review

No vulnerabilities were found within the ICE source code base reviewed; as a result, no findings were written against the code base

ICC source code vulnerability review

No vulnerabilities were found within the ICC source code base reviewed; as a result, no findings were written against the code base.

ADJ source code vulnerability review

No vulnerabilities were found within the ADJ source code base reviewed; as a result, no findings were written against the code base.

FINAL REPORT

No discrepancy findings were located within the **Dominion Democracy Suite 5.10** code base.

No potential vulnerabilities were identified within the **Dominion Democracy Suite 5.10** code base

As directed by the California Secretary of State, this software testing report does not include any recommendation as to whether or not the system should be approved.

End of Software Test Report