Dominion Democracy Suite 5.2 Source Code Test Report for California

DOM-17002-CSTR-01

Prepared for:

Vendor Name	*Dominion Voting*
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
2.0	M. Santos	Updates for CVSS discrepancies

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

This report outlines the test approach SLI Compliance (SLI) followed when performing Software Testing on the ***Dominion Democracy Suite 5.2*** *voting system* against the California Voting System Standards (CVSS). The purpose of this document is to provide an understanding of the work SLI conducted.

Scope of the Dominion Democracy Suite 5.2 Voting System

This section provides a description of the scope of **Dominion Democracy Suite 5.2** voting system components:

- EMS – Result, Tally and Reporting (RTR) application
- ImageCast Central (ICC) application
- ImageCast Evolution (ICE) firmware/hardware
- ImageCast X (ICX) firmware/hardware

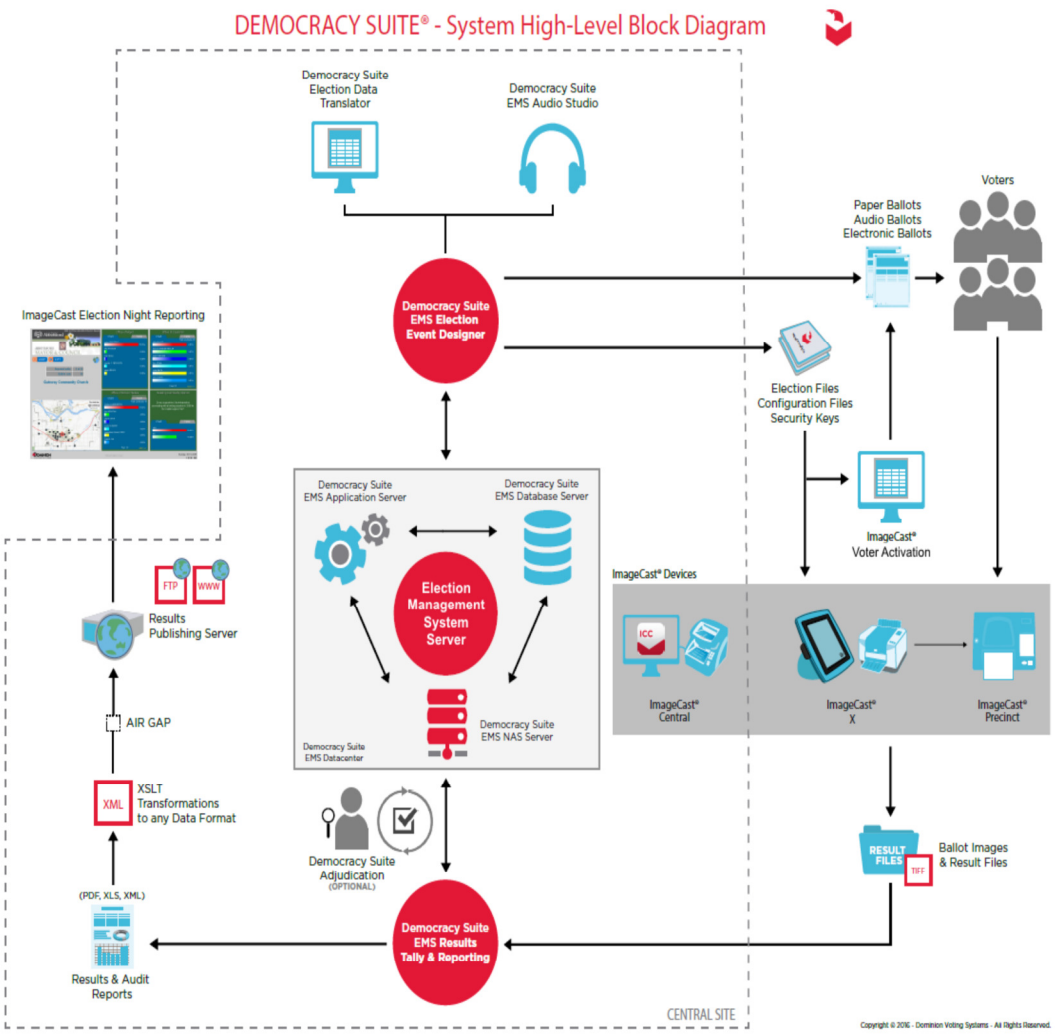
The **Dominion Democracy Suite 5.2** Election Management System (EMS) represents a set of N-Tier software applications (EMS, RTR, Adjudication) for pre-voting and post-voting election project activities that are applicable to jurisdictions of various sizes and geo-political complexities.

The **Dominion Democracy Suite 5.2** 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 centralized scanning and counting of paper ballots.

The **Dominion Democracy Suite 5.2** 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 5.2** ICX ballot marking platform is used for creation of 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.

System Topology Diagram



REVIEW SPECIFICATIONS

The following are the specifications for source code testing conducted on the **Dominion Democracy Suite 5.2 voting system**.

Source Code Review

The **Dominion Democracy Suite 5.2 voting system** includes proprietary software and firmware. The **Dominion Democracy Suite 5.2 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
- Evaluation of 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
- Analyze 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 Dominion’s applications are shown in Table 1.

Table 1 – Democracy Suite 5.2 Components

Component	Language/s	Lines of Code	Standard
ICC	C/C++	234,812	CPlusPlus_CodingStandard-5.2-CA.pdf
ICX	Java	166,547	dvs_JavaCodingStandards.pdf
ICE	C/C++	822,346	CPlusPlus_CodingStandard-5.2-CA.pdf
ADJ	C#	189,280	Csharp_AutomatedCodeReview-5.2-CA.pdf
EMS	C#	1,682,875	Csharp_AutomatedCodeReview-5.2-CA.pdf

Source Code Review Tools utilized by SLI included:

- Module Finder: an SLI proprietary application used to parse module names from C/C++ and VB code and populate the identified module names into the review documents
- 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 to provide the California Secretary of State a basis for evaluating the extent to which the source code meets applicable standards.

ADJ source code review

Four violations of the “single exit point” requirement were found in the ADJ source code base reviewed. As a result, four discrepancies were written against the code base.

EMS source code review

There were fifty violations of the “single exit point” and one function found to be longer than 240 lines in the EMS source code base reviewed. As a result, fifty-one discrepancies were written against the code base.

ICC source code review

There were nine instances of unchecked pointers and one instance of case statement without a break found in the ICC source code base reviewed. As a result, ten discrepancies were written against the code base.

ICE source code review

There were four instances of unchecked pointers found in the ICE source code base reviewed. As a result, four discrepancies were written against the code base.

ICX source code review

No source code requirements were found to be at issue within the ICX source code base reviewed and 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:
        - Setup and pre-election procedures;
        - Election operation;
        - Post-election processing of results; and
        - Archiving and storage operations.
- Vendor insider: Possesses 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.

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.

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.

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.

ICE source code vulnerability review

The following potential vulnerabilities were found within the ICE source code base:

SQL Statements

Five instances of SQL statements that hold the possibility of code being injected into them were observed within the ICE source code base. It was noted, however, that these statements are inside private functions and can only be accessed by appropriate function calls.

As a result of the placement of the SQL statements in question, the level of access required to take advantage of this potential vulnerability would be that of a vendor insider – someone with great knowledge of, and access to, the voting machine design and configuration.

strcopy

It was noted that forty-four instances of the “strcopy” function are being used. It is recommended not to use strcopy as it does not protect against out of bounds issues.

The strings being acted on are normally bounds-checked either on entry into or before being passed by the receiving or calling function.

For the “strcopy” statements in question, the level of access required to take advantage of this potential vulnerability would be that of a vendor insider – someone with great knowledge of, and access to, the voting machine design and configuration.

memcpy

It was noted that six instances of the “memcpy” function are being used. Code using the memcpy function is prone to buffer overflow.

The data being acted on is normally bounds-checked on entry into or before being passed by the receiving or calling function.

For the “memcpy” statements in question, the level of access required to take advantage of this potential vulnerability would be that of a vendor insider – someone with great knowledge of, and access to, the voting machine design and configuration.

strcmp

It was noted that one instance of the “strcmp” function is being used. Code using the “strcmp” function is prone to buffer overflow.

Values being passed into the strcmp function are bounds-checked before being passed to the strcmp function. For the “strcmp” statements in question, the level of access required to take advantage of this potential vulnerability would be that of a vendor insider – someone with great knowledge of, and access to, the voting machine design and configuration.

ICX source code vulnerability review

One potential vulnerability was found within the ICX source code base reviewed. Potentially, whenever a USB drive is inserted into the ICX machine it is automatically loaded, without a security check of the contents. This could mean that regardless of what is on that thumb drive it will be read and if an “.exe” file exists, it will be run. This potential vulnerability will be further investigated during Security testing.

For the vulnerability in question, the level of access required to take advantage of this potential vulnerability would be inclusive of the following actors:

- Voter, who could potentially gain access to the USB port and cause a reboot of the device.
- Poll worker, who does have access to the USB port as well as the ability to reboot the device.
- Elections official insider, who does have access to the USB port as well as the ability to reboot the device.
- Vendor insider, who does have access to the USB port as well as the ability to reboot the device.

Final Report

Sixty-nine discrepancies were identified within the **Dominion Democracy Suite 5.2** code base.

Several potential vulnerabilities were identified within the **Dominion Democracy Suite 5.2** code base, within either the ICE code base or the ICX code base.

Within the **Dominion Democracy Suite 5.2** ICE code base, all findings were low risk vulnerabilities that would require an in-depth knowledge of the ICE code base and how it operates to be able to successfully subvert the system. To exploit them successfully would require modifying the code before any build.

Within the **Dominion Democracy Suite 5.2** ICX code base, one potential vulnerability was discovered and the level of access required to take advantage of this potential vulnerability would be open to a variety of actors including a voter, a poll worker, an election official insider, and a vendor insider. This possible

vulnerability has a more widespread potential. Polling place procedures are one method of mitigating this issue, with poll workers actively verifying that the USB ports are sealed and no one has access.

As per the direction given 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 Test Report