Dominion Democracy Suite ImageCast Remote 5.10 RAVBMS Software Test Report

DOM-19002-SCRTR-01

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

Prepared by:

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
July 22,2019	v1.0	M. Santos	Initial Release
August, 22, 2019	v2.0	M. Santos	Updates for CA comments
August, 23, 2019	V3.0	M. Santos	Updates for CA 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

The California Voting Systems Standards (CVSS) were written in such a way to be applicable to a wide variety of voting technology. Therefore, the relevant portions of the CVSS are reviewed as they relate to the Remote Accessible Vote By Mail System (RAVBMS) for the purposes of this report. The use of "voting system" shall apply to the RAVBMS.

This report outlines the testing SLI Compliance (SLI) followed when performing Software Testing on the **Dominion Democracy Suite ImageCast Remote 5.10 (RAVBMS)** (DS ICR 5.10 RAVBMS) against the California Voting System Standards (CVSS).

The **DS ICR 5.10 RAVBMS** enables voters to mark their ballots using a secure web-based interface and generate and download a PDF representation of their selections. Voters then print the ballot and return it to the clerk.

REVIEW SPECIFICATIONS

The following are the specifications for source code testing conducted on the **DS ICR 5.10 RAVBMS**.

Source Code Review

The **DS ICR 5.10 RAVBMS** includes proprietary software. The **DS ICR 5.10 RAVBMS** 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:

- Evaluation of potential vulnerabilities and related issues (code quality and standards compliance), considering that an exploitable issue in a component that is not in itself security relevant could be used to subvert more critical data.

- Search for exposures to commonly exploited vulnerabilities, including vulnerabilities that could be exploited to:
  - Alter the paper cast vote record
  - Alter vote results
  - Alter critical election data such as audit logs
  - Conduct a “denial of service” attack on the voting technology
- Evaluation of the use and correct implementation of cryptography and key management
- Analysis of error and exception handling
- Evaluation of the likelihood of security failures being detected
  - Evaluation of whether audit mechanisms are reliable and tamper resistant
  - Evaluation of whether data that might be subject to tampering is properly validated and authenticated
- Evaluation of the risk that a user can escalate his or her capabilities beyond those authorized
- Evaluation of 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
- Evaluation for embedded, exploitable code (such as “Easter eggs”) that can be triggered to affect the system
- Evaluation of 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.
- Evaluation of 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.

Languages involved in the **DS ICR 5.10 RAVBMS** are shown in Table 1.

Table 1 – Dominion DS ICR 5.10 RAVBMS components

Component	Language/s	Lines of Code	Standard
RAVBMS	JavaScript	19175	CVSS, dvs_javaCodingStandards.pdf
RAVBMS	C#	184143	CVSS, StyleCop Coding Standards
RAVBMS	Comment Lines	68546	CVSS, StyleCop Coding Standards

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 requirements
- Understand: a commercial application used to review code to 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.

RAVBM system source code review

There were no source code requirements found to be at issue within the RAVBMS source code base reviewed.

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.

RAVBMS source code vulnerability review

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

Final Report

There were no discrepancy findings within the **DS ICR 5.10 RAVBMS** code base.

No vulnerabilities were identified within the **DS ICR 5.10 RAVBMS** 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