



NYSBOE Dominion Upgrade Source Code Review Findings

1.0 Introduction

In previous certification efforts for NYSBOE, SLI verified all source code modules provided to the state were compliant with the best practices and coding requirements defined in the following standards:

- VVSG 2005, (Volume I and Volume II)
- 2011NYElectionLaw.pdf
- 6210Regulations09052008.pdf
- BMD Requirements.pdf
- Ciber_COTStandard.pdf
- NYS_voting_systems_standards-4-20(6209).pdf
- havalaw.pdf
- Table of known vulnerabilities
- Democracy Suite EMS Coding Standards.docx

This included a secure source code review to ensure protection against all known and identified vulnerabilities reported within prior ITA reports, voting system tests, or risk assessment final reports, and other comparable examinations performed by independent testing organizations.

All source code submitted for certification was compiled and reviewed at the SLI Compliance Testing Facility by SLI staff. The build scripts, vendor source code, and any modified Commercial Off-the-Shelf (COTS) code was reviewed for format, structure, and functionality. All code delivered was also reviewed using both automated and manual methods for malicious code, Trojans, and viruses.

Since the initial certification effort, Dominion has added the Ballot Marking Device (BMD) to their system configuration and the BMD code has been reviewed for conformance against the VVSG 2005, and NY State Voting System requirements by SLI. As directed by NYSBOE, SLI conducted a full source code review of the BMD code against the VVSG 2005 and NY State requirements.



2.0 Scope of Review and Methodology

The main objective of the source code review was to analyze the BMD source code and confirm that the code complies with the criteria set forth by the state of New York.

List of Methodology Criteria

Review all the BMD device's software and firmware for security access controls, and determine any vulnerabilities.

Determine the effectiveness of the security access controls for the BMD device's software.

Review the BMD device's software source code to determine the presence of vulnerabilities, or if the software can be executed outside the intended manner and outside of normal conditions.

Where non-catastrophic failure of the device may be related to programming, exception handling routines were examined for data handling logic employed.

Review BMD device's software source code to verify data validation routines.

Verify Telecommunications capabilities, which are not allowed in NY elections systems, are not employed.

Verify there are no exploitable vulnerabilities that could affect warnings, alerts, error messages or logging.

Verify the inclusion of logic related to real time audit logging as stated in the voting standards.

Any other direct violations of the aforementioned standards were noted in discrepancy reports. Discrepancy reports were provided to the system vendor for their review and remediation.



3.0 Overview of Findings

Items found to be non-compliant during the review were described in discrepancy reports that were then provided to the vendor. Items described as non-compliant included:

- 1) Dead, unused, or unreachable code
- 2) Lack of logic to log certain events
- 3) The absence of parameter range and value validation logic Occurences of multiple exit points in modules
- 4) The presence of code intended for jurisdictions other than the State of New York
- 5) incomplete exception handling
- 6) Improper dispositions of system resources such as file handles and allocated memory
- 7) Nested Ternary operations, which is a violation under VVSG rules
- 8) Certain cognitive issues were also described, such as improperly written English language user messages.

Note: All findings are described in the accompanying SC Review summary report.

4.0 Conclusion

A number of items were cited by SLI as being non-compliant with the 2005 Voluntary Voting Systems Guilelines. Additional items were noted as not conforming with one or more of the other standards as mentioned above.

Through a succession of source code submissions and reviews, all cited non-compliant items have been resolved. There are no remaining open items against the BMD source code.

Based on the reviews conducted against the submitted DVS BMD source code, SLI recommends the following source code versions for certification:

BMD 4.9.6