



NYSBOE ES&S Upgrade Source Code Review Findings DS200 2.9.0.1I

1.0 Introduction

Voting system certification efforts for the New York State Board of Elections by SLI Global Solutions included the verification that all of the source code modules that comprise the subject ES&S voting system were compliant with the best practices and coding requirements as described in the following documents and standards:

- VVSG 2005, (Volume I and Volume II)
- 2011NYElectionLaw.pdf
- 6210Regulations09052008.pdf
- Ciber_COTSSstandard.pdf
- NYS_voting_systems_standards-4-20(6209).pdf
- havalaw.pdf
- Table of known vulnerabilities

SLI's testing efforts performed for the State of New York included a secure source code review to evaluate and ensure protection against all vulnerabilities identified and described within prior ITA reports, voting system tests, risk assessment final reports, and other comparable examinations.

All source code submitted for certification was reviewed by SLI personnel at SLI Global Solutions' Compliance Testing Facility in Denver, Colorado. The vendor source code was reviewed for format, structure, and functionality. All delivered code was reviewed for the presence of malicious code, Trojan horses, and viruses by use of both automated and manual review methods. A build of the reviewed source code was completed at Wyle Labs' facility in Huntsville, Alabama.

The upgraded ES&S DS200 source code was initially reviewed for compliance with the 2005 Voluntary Voting Systems Guidelines (VVSG) by Wyle Labs as part of the Federal review process. As directed by NYSBOE, SLI performed a complete review of changes made to the source code for compliance with requirements of voting system source code as described in New York State regulations. In the course of performing its review, SLI also evaluated the current states of previously described and outstanding discrepancies cited against prior submissions of the source code. The evaluation of previously described



non-compliant items included reviews of items that had previously been revealed through usages of security and other automated source code review tools.

2.0 Review Scope and Criteria

The scope of the latest source code review effort performed for the State of New York was comprised of only those lines of project source code that had been added or edited since the last previous review, and their surrounding contexts. The review of edited source code lines was conducted to analyze changes made by the vendor to the software, and to assure the source code's continued compliance with criteria as set forth by the State of New York. The criteria against which the source code was reviewed for compliance included the following aspects:

- 1) The availability of the system audit log, and the inclusion of logic related to real time audit logging,
- 2) Cognitive issues related to system and user warnings, alerts, and error messages, and the appropriateness of both their placements and content,
- 3) Verification of the presence of data validation logic,
- 4) The presence of process controls to assure that the system cannot be executed outside of its intended manner,
- 5) Usage of certified software where cryptographic and hashing methods are employed,
- 6) Password management security, and access controls,
- 7) Appropriateness of exception handling routines in the event of the non-catastrophic failure of a device,
- 8) Confirmation of the absence of telecommunications capabilities within the system.

Any discovered violations of either the listed review criteria, or of the aforementioned standards, were noted in discrepancy reports. Discrepancy reports were provided to the system vendor for their review and remediation. No new discrepancies were cited by SLI during its review.

3.0 Overview of Findings

Items found to be non-compliant during this and prior reviews were described in discrepancy reports that were then provided to the vendor for their consideration and remediation. Items described as non-compliant have included:

- 1) Declared and un-used variables
- 2) Lack of logic to log certain conditions and events



- 3) Improper dispositions of system file handles
- 4) Usages of hard-coded numeric constants without explanatory comments
- 5) Ambiguous database transaction terminations

4.0 Conclusion

While several items within the source code were initially cited by SLI as being non-compliant with the 2005 Voluntary Voting Systems Guidelines and New York state regulations, after a succession of source code submissions and reviews, the last of which was performed on a code set received by SLI on March 14, 2014, only one item within the DS200 component's source code that was cited as being non-conforming remains open. That one item that remains open is not seen by SLI as posing a risk to the operation of the DS200 scanner.

Based on the review performed on the last submitted ES&S source code package, SLI recommends the following source code version for certification as part of the ES&S voting system:

DS200 v. 2.9.0.1l
PowerManagementMsp430 v. 1.2.8.0a
ScannerC8051 v. 3.1.0.0a