Report:

Testing Oversight of ES&S Express Vote (EVS) 6.3.0.1

Public Report v1

Prepared for:

NEW YORK STATE | Board of Elections

Amy Hild, Director of Election Operations
Thomas Connolly, Deputy Executive Director
Brendan Lovullo, Deputy Executive Director
New York State Board of Elections
40 North Pearl St.
Albany, NY 12207

5/31/2023

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

ACRONYMS AND TERMS	
ATI	Audio Tactile Interface
BMD	Ballot Marking Device
COTS	Commercial Off-the-Shelf
EAC	Election Assistance Commission
EMS	Election Management Software
EVS 6.3.0.1	Express Vote 6.3.0.1
NYSBOE	New York State Board of Elections
PDF	Portable Document Format
QA	Quality Assurance
SCA	Software Composition Analysis
SLI	SLI Compliance, a Division of Gaming Laboratories International, LLC
TDP	Technical Data Package
VVSG	Voluntary Voting System Guidelines

Table of Contents

List of Tables

1 Introduction

The New York State Board of Elections (NYSBOE) has asked NYSTEC, as a security expert, to perform an independent review of work conducted by SLI Compliance (SLI) for testing the Express Vote 6.3.0.1 (EVS 6.3.0.1) electronic voting system that was developed by ES&S Voting System Corporation for certification and use in New York State elections. Specifically, NYSTEC was tasked with reviewing all deliverables produced by SLI, including the functional test plans, source code test plans, and security test plans that SLI created based on the federal 2005 Voluntary Voting System Guidelines (VVSG) and 2021 New York State voting laws and regulations. NYSTEC enlisted the services of Cyber Castellum, a security consulting firm, to review the testing that deals with the system's source code.

EVS 6.3.0.0 is U.S. Election Assistance Commission (EAC) certified. All modifications included in the EVS 6.3.0.1 system were fully tested against all VVSG and New York State requirements. As the entire voting system will be used in New York State if certified, the testing scope included all devices and components of the system.

This report includes:

- A list of SLI deliverables reviewed by NYSTEC.
- A breakdown of the work performed by NYSTEC.

2 Executive Summary

SLI tested the functionality, security, and system documentation of the EVS 6.3.0.1 system, based on VVSG version 1.0 (2005) and New York State voting laws and regulations (2021). NYSTEC reviewed SLI's requirements mapping, test plans, discrepancies (referred to as JIRAs by SLI), and reports, as well as the code review report from Cyber Castellum. Based on those reviews, NYSTEC believes that SLI adequately tested the functionality and security of the system.

The scope of testing performed by SLI to evaluate the EVS 6.3.0.1 system included:

- All applicable 2021 New York State election laws.
- Section 6209 of Subtitle V of Title 9 of the Official Compilation of Codes, Rules, and Regulations of the State of New York.
- The EAC 2005 VVSG 1.0 (2005), Volumes 1 and 2 requirements, per the NYSBOE-approved testing approach for the EVS 6.3.0.1 certification event.

All 2005 VVSG requirements that indicated "shall" (rather than "should") were previously tested for EAC certification and, therefore, were accepted and not repeated. NYSTEC did not review any

testing conducted during EAC certification. As part of this testing, all 2005 VVSG requirements that indicated "should" were tested as if the "should" read as "shall."

2.1 NYSTEC Recommendations

NYSTEC has the following recommendation:

- Several issues were found by SLI during their review of the source code. However, it remains that the risk associated with these issues is being mitigated through controls present on the devices where the code is installed. As a best practice in software development, code should not rely on external environmental controls for security, therefore, NYSTEC recommends that ES&S remediate these issues in their code, along with the list of issues they agreed to address, in a future build. NYSBOE should keep track of these issues to ensure they are resolved in any future versions brought to them for certification.

2.2 Components in the EVS 6.3.0.1 System

According to the SLI report, "*The EVS 6.3.0.1 system represents a set of software applications for pre- voting, voting, and post-voting election project activities for jurisdictions of various sizes and political division complexities.*"

System components include:

Election Management Software (EMS) – A set of applications that are responsible for all pre-voting and post-voting groups of activities in the process of defining and managing elections.

DS200 v1.2, DS200 v1.3, DS200 v1.3.13, DS300 – Scan precinct ballot counters (tabulators) that are used in conjunction with an external ballot box.

DS450, DS850, DS950 – High-speed, central digital ballot scanning systems used for high-volume processing of ballots (such as vote by mail).

ExpressVote XL - A standalone precinct level ballot marking device (BMD) which also includes an audio tactile interface (ATI), which allows voters who cannot complete a paper ballot to generate a machine-readable and human-readable paper ballot, based on vote selections made, using the ATI.

3 SLI Testing

This section reviews the testing performed on the EVS 6.3.0.1 system by SLI.

3.1 Documentation Review

3.1.1 Review of Prior Work

Prior work documentation lists the last certification date for each component of the system to demonstrate which versions will need to be reviewed during the current testing event. This aided SLI in determining the scope of testing. NYSBOE's policy is to leverage all EAC testing for New York State such that any VVSG 1.0 (2005) requirement that indicates "shall" was accepted without evaluating test cases. NYSTEC reviewed SLI's assessment of prior work for the EVS 6.3.0.1 system. NYSTEC resolved all our questions with SLI, and no outstanding issues remain. NYSTEC's final review, including all comments, is included in this report as Attachment A.

3.1.2 Technical Data Package (TDP) Review

The technical data package (TDP) review assesses the technical documentation submitted to NYS for this certification testing event. SLI worked with the vendor throughout the testing process to ensure that any updates needed — due to changes required to remediate issues found during testing — were included in the technical documentation. NYSTEC reviewed the final TDP submission and found no issues. NYSTEC's final review, including all comments, is included in this report as Attachment B.

3.1.3 Requirements Matrix

The requirements matrix is the foundation for this certification testing event, as it evaluates all VVSG 1.0 (2005) and New York State requirements against any modifications or prior work. This high-level assessment is then directly mapped to the master test plan, individual test plans, and — at the lowest level — test cases. NYSTEC's final reviews, including all comments, are included in this report as Attachment C.

3.2 Test Plans and Reports

3.2.1 Master Test Plan and Report

The master test plan created by SLI used the determinations for planned testing from the requirements matrix (See Section 3.1.3 Requirements Matrix) to organize the requirements by type (e.g., functional, security, or source code). NYSTEC reviewed the master test plan with SLI over several rounds of discussion, and all issues and questions were resolved. NYSTEC's final review, including all comments, is included in this report as Attachment D.

Results from the testing prescribed by the master test plan were reviewed, and there are no outstanding issues with the master test report. NYSTEC's final review, including all comments, is included in this report as Attachment E.

3.2.2 Functional Testing

Functional testing aims to validate the system against requirements. Functional testing for this project was divided into two test plans, the functional test plan, and the security functional test plan. SLI evaluated the EVS 6.3.0.1 system against all applicable New York State 2021 election law, §6209 Voting System Standards, and VVSG 1.0 (2005) requirements, per the testing approach approved by NYSBOE.

NYSTEC reviewed the functional test plan and agreed with all SLI assessments for that testing. All questions were resolved. NYSTEC's final review of the functional test plan, including all comments, is included in this report as Attachment F.

NYSTEC reviewed the functional test report and agreed with all SLI assessments for that testing. Questions were raised and all questions were resolved. NYSTEC's final review of the functional test report is included as Attachment G.

NYSTEC reviewed the security functional test plan and agreed with all SLI assessments for that testing. Any testing plans that were too high-level were verified in the test cases for clarification. All questions were resolved. NYSTEC's final review, including all comments, is included in this report as Attachment H.

NYSTEC reviewed the security functional test report and agreed with all SLI assessments for that testing. Questions were raised regarding test cases and all questions were resolved. NYSTEC's final review of the security functional test report, including all comments, is included in this report as Attachment I.

NYSTEC also reviewed the security functional test cases. All questions were resolved. NYSTEC's final review, including all comments, is included in this report as Attachment J.

3.3 Source Code Reviews

3.3.1 Source Code Review Test Plans

Cyber Castellum was contracted to complete a quality assurance (QA) review of SLI's source code review and security source code review test plans that evaluate the code base against New York State requirements.

3.3.2 Source Code Review Reports

Cyber Castellum completed a QA review of SLI's source code review report and security source code review report, and the resulting Cyber Castellum report is included in this report as Attachment M. SLI used an automated code scanning software, Checkmarx, that can quickly review large software packages with a customized configuration to check for coding standards and known security vulnerabilities. SLI properly selected all pertinent scans for the EVS 6.3.0.1 code base.

In total, 43,218 potential vulnerabilities were identified by Checkmarx, but approximately 94% of findings were marked as "Not Exploitable." The other findings were put into a list of 430 potential vulnerabilities. SLI has classified the "Exploit Potential" of these 430 potential vulnerabilities to require "Extensive knowledge of the system or a Vendor Insider".

No JIRAs were created for those findings as many were false positives and the others, when examined within the context of the physical environment and implemented security controls, did not pose a significant threat to the EVS 6.3.0.1 system.

Cyber Castellum noted the following shortcomings in the code review plans and reports delivered by SLI:

- Items marked by SLI as "Not Exploitable."
- Dependency checks.
- Quality of source code.

These shortcomings noted by Cyber Castellum were due to the distributed nature of the SLI testing process and the fact that Cyber Castellum did not see other parts of the overall testing performed by SLI.

SLI did not use the Checkmarx software to scan installed COTS software code or libraries for known vulnerabilities, as that was out of scope. NYSTEC verified that SLI manually investigated for any known vulnerabilities for installed COTS software.

3.3.2.1 Items Marked by SLI as "Not Exploitable"

In its report, Cyber Castellum remarks about the number of findings that SLI labeled as "Not Exploitable."

> *"Cyber Castellum requested the Checkmarx reports in PDF format and analyzed the triage results. Over 99 percent (43,211 out of 43,218) of the Checkmarx vulnerabilities were identified as false positive and not exploitable. It is interesting that none of them have been confirmed as true positive. Cyber Castellum has not experienced such a high false positive rate with such tools as Checkmarx."*

Cyber Castellum is interpreting the Checkmarx label "Not Exploitable" as being a true false positive. However, SLI defines "Not Exploitable" as:

> *"A potential vulnerability is considered 'Not Exploitable' if it is found to be a false positive, or sufficient counter measures exist to prevent exploitation from causing interruption or failure of the system."*

Thus, the 43,211 findings are not necessarily false positive; rather, SLI believes that there are countermeasures in place to keep the vulnerability from being exploited by an attacker. NYSTEC agrees with Cyber Castellum's conclusion, that even though SLI believes the potential vulnerabilities are mitigated via external controls, ES&S should review the findings and update the code as warranted.

3.3.2.2 Dependency Checks

In its report, Cyber Castellum discusses that tools to find publicly disclosed vulnerabilities of code were not used.

> *"Furthermore, Checkmarx Software Composition Analysis (SCA) was not used to identify publicly disclosed vulnerabilities in libraries and components that the software depends on."*

SLI did not perform a known vulnerability review during source code testing but did during functional security testing. SLI's Security Functional Test Report v2.0 states:

> "*The known vulnerability database identifies all documented software libraries present within the TDP and provides results regarding known relevant vulnerabilities related to each software library. Some libraries may have dependencies upon others; however, each piece of software was individually investigated."*

Cyber Castellum was only given the source code review and security source code review reports and did not have access to the information on the known vulnerability testing by SLI. NYSTEC believes the known vulnerability approach taken by SLI is adequate. In addition, NYSTEC verified that SLI manually investigated for any known vulnerabilities for installed COTS software.

3.3.2.3 *Quality of Source Code*

In its report, Cyber Castellum outlined the quality of the source code:

> *"The report that focused on the quality of the source code only identified 20 errors, all of which are exceeding the line length of 120 characters. No other code quality issues have been identified."*

Most of the source code quality issues are 2005 VVSG requirements, and SLI performed a manual review to only higher risk VVSG requirements, which explains the low number of code quality findings.

4 Discrepancies

4.1 SLI Findings

SLI reports a discrepancy found during testing as a "JIRA." In a code review, a discrepancy occurs when the source code does not meet defined requirements or specifications, does not function as intended, or allows a security breach. In all other testing, a discrepancy occurs when an element of the voting system does not meet defined functional or security requirements. The final count of open discrepancies reflects issues that were not addressed during the certification process and that remain in violation of requirements.

TABLE 1, COUNT OF ALL DISCREPANCIES REPORTED BY SLI

	REPORTED TEST ISSUES (JIRAS)	SOURCE CODE	SECURITY SOURCE CODE (POTENTIAL VULNERABILITIES)	TOTAL
Discrepancies found during testing	34	20	430	**484**
Open discrepancies	0	20	430	**450**

4.2 Open Discrepancies

As of the conclusion of this testing effort, there are no open functional discrepancies.

5 NYSTEC Activities

NYSTEC performed the following oversight activities for the testing conducted by SLI:

- Reviewed all deliverables supplied by SLI for this certification testing event. After review and consultation with the NYSBOE Operations Unit, NYSTEC sent comments and questions to SLI. SLI responded, and there were several iterations and discussions until all issues were resolved. The following is a list of the SLI deliverables that were reviewed:
  - Requirements matrix.
  - Review of prior work.
  - TDP.
  - Master test plan.
  - Functional test plan.
  - Security functional test plan.
- NYSTEC brought in a subcontractor, Cyber Castellum, to perform a security QA review of the code review performed by SLI. The following is a list of the SLI deliverables that were reviewed.
  - Source code review test plan.
  - Security source code review test plan.
  - Security source code review test cases.
  - Source code review test report.
  - Security source code review test report.
- NYSTEC reviewed the security functional test cases, and it appears that SLI sufficiently tested the system. Any issues found were discussed with SLI and resolved. SLI updated all corresponding deliverables.
- NYSTEC reviewed discrepancy reports from SLI as they were received and then worked with the NYSBOE Operations Unit, SLI, and ES&S to resolve any discrepancies.
- NYSTEC reviewed all final reports from SLI:
  - Master test report.
  - Functional test report.
  - Security functional test report.

6 Documents Referenced

SLI TEST PLANS, TEST CASES, AND REQUIREMENTS MAPPING
Evaluation of Prior Work for ES&S EVS 6301 v1.0.pdf
TDP Review for ES&S EVS 6301.pdf • Attachment A – NYS ES&S EVS 6.3.0.1 TDP List • Attachment B – NYS ES&S EVS 6.3.0.1 TDP Issues (Confidential)
ES&S EVS 6301 NYS Requirements Matrix.xls
NYSBOE ES&S EVS6301 Master Test Plan v2.0.pdf
NYSBOE ESS EVS 6.3.0.1 Functional Test Plan v1.0.pdf
NYSBOE ESS EVS 6301 Security Functional Test Plan v2.0.pdf
ES&S EVS 6301 Security Test Cases • NY ES&S EVS 6301 Security Test Suite.pdf
NYSBOE ESS EVS 6.3.0.1 Source Code Review Test Plan v2.0.pdf NYSBOE ESS EVS 6301 Security Source Code Review Test Plan v2.0 • Attachment A – NYS ES&S EVS 6301 Requirements Matrix • Attachment B – SLI Testing Approach ES&S EVS6301 – Finalized 08292022 • Attachment C – ES&S Declared Coding Standards
SLI TEST REPORTS
NYSBOE ESS EVS 6.3.0.1 Functional Test Report v2.0.pdf • Attachment A – ES&S EVS 6301 NYS Requirements Matrix w Test Cases.xls • Attachment B – NYS ES&S EVS 6.3.0.1 As Run Test Cases (Confidential) • Attachment C – NYS ES&S EVS 6.3.0.1 Functional JIRAs (Confidential).pdf
NYSBOE ES&S EVS 6.3.0.1 Functional Security Test Report v2.0.pdf • Attachment A – NYS ES&S EVS 6.3.0.1 Requirements Matrix w Test Cases.xls • Attachment B – NYS ES&S EVS 6301 Security Test Cases (Confidential) • Attachment C – NYS ES&S EVS 6.3.0.1 Security JIRA Issues (Confidential).pdf • Attachment D – NYS ES&S 6.3.0.1 Security Test Artifacts (Confidential) • Attachment E – NYS ES&S EVS 6.3.0.1 Security Test Notebook (Confidential)
NY ESS EVS 6.3.0.1 Master Test Report v3.0.pdf • Attachment A – ES&S EVS 6301 NYS Requirements Matrix w Test Cases.xls • Attachment B – SLI Testing Approach ES&S EVS6301 - Finalized 08292022.pdf

• Attachment C – NYS ES&S EVS 6.3.0.1 Master JIRAs (Confidential).pdf
NYSBOE ESS EVS 6301 Source Code Review Test Report v2.0 • Attachment A – New York Requirements Matrix EVS 6.3.0.1.xlsx • Attachment B – EVS 6.3.0.1 List of Source Code Reviewed (Confidential) • Attachment C – Source Code Review Form Spreadsheets (Confidential) • Attachment D – Source Code Review Discrepancy Review Forms (Confidential) • Attachment E – Source Code Review Test Cases.pdf • Attachment F – ES&S Declared Standards
REPORTS FROM NYSTEC SUBCONTRACTOR CYBER CASTELLUM
NY ESS EVS 6.3.0.1 Code Review Test Plan Feedback v1.0.pdf
Evaluation of SLI ESS 6.3.0.1 Code Review Report 05.21.23.pdf

7 Attachments

A. ES&S – Prior Work – NYSTEC Comments.pdf
B. ES&S – TDP Review – NYSTEC Comments.pdf
C. ES&S – NYS Requirements Matrix – NYSTEC Comments.pdf
D. ES&S – Master Test Plan – NYSTEC Comments.pdf
E. ES&S – Master Test Report – NYSTEC Comments.pdf
F. ES&S – Functional Test Plan – NYSTEC Comments.pdf
G. ES&S – Functional Test Report – NYSTEC Comments.pdf
H. ES&S – Security Functional Test Plan – NYSTEC Comments.pdf
I. ES&S – Security Functional Test Report – NYSTEC Comments.pdf
J. ES&S – Security Functional Test CASES – NYSTEC Comments.pdf

Phone: (888) 969-7832
Email: nystec@nystec.com
Website: www.nystec.com

ROME
99 Otis Street, 2nd Floor
901
Rome, NY 13441

ALBANY
540 Broadway, 3rd Floor

Albany, NY 12207

NEW YORK CITY
27 West 24th St., Suite

New York, NY 10010