



Report:

Testing Oversight of Clear Ballot ClearVote 2.4 Public Report v1

Prepared for:



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

7/13/2023



For Public Release

ACRONYMS AND TERMS	
ATI	Audio Tactile Interface
BMD	Ballot Marking Device
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off-the-Shelf
EAC	Election Assistance Commission
EMS	Election Management Software
FIPS	Federal Information Processing Standards
GPO	Group Policy Objects
IoT	Internet of Things
LTSC	Long-Term Servicing Channel
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

1	INTRODUCTION.....	4
2	EXECUTIVE SUMMARY	4
	2.1 Retests of ClearCount 2.2 Issues.....	5
	2.2 NYSTEC Recommendations.....	5
	2.3 Components in the ClearVote 2.4 System	5
3	SLI TESTING	6
	3.1 Documentation Review.....	6
	3.1.1 Review of Prior Work.....	6
	3.1.2 Technical Data Package (TDP) Review.....	6
	3.1.3 Requirements Matrix.....	6
	3.2 Test Plans and Reports.....	7
	3.2.1 Master Test Plan and Report.....	7
	3.2.2 Functional Testing	7
	3.3 Source Code Reviews	8
	3.3.1 Source Code Review Test Plans.....	8
	3.3.2 Source Code Review Reports	8
4	DISCREPANCIES.....	10
	4.1 SLI Findings.....	10
	4.2 Open Discrepancies.....	11
5	NYSTEC ACTIVITIES.....	11
6	DOCUMENTS REFERENCED	12
7	ATTACHMENTS	14

List of Tables

Table 1, Count of All Discrepancies Reported by SLI	11
Table 2, Documents Referenced	12

1 Introduction

The New York State Board of Elections (NYSBOE) asked NYSTEC, as a security expert, to perform an independent review of work conducted by SLI Compliance (SLI) for their testing of the ClearVote 2.4 electronic voting system. ClearVote 2.4 was developed by Clear Ballot for certification and use in New York State elections. NYSTEC was tasked with reviewing all deliverables produced by SLI, including functional, source code, and security test plans 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 system source code testing.

ClearVote 2.3 is U.S. Election Assistance Commission (EAC) certified. All modifications included in the ClearVote 2.4 system were fully tested against all VVSG and New York State requirements. Because the entire voting system would 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.
- A breakdown of the work performed.

2 Executive Summary

SLI tested the functionality, security, and system documentation of the ClearVote 2.4 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 ClearVote 2.4 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), Volume 1 and 2 requirements, per the NYSBOE-approved testing approach for the ClearVote 2.4 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 Retests of ClearCount 2.2 Issues

Two issues found during the certification of ClearCount 2.2, a component of ClearVote 2.4 that was certified in a previous testing event and being tracked, were shown in this testing event to be resolved by Clear Ballot. Additionally, the software validation process in ClearCount 2.2 has been resolved.

2.2 NYSTEC Recommendations

NYSTEC has the following recommendations:

- Several issues were found by SLI during its review of the source code. 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 Clear Ballot review these issues in their code and remediate, if necessary, in a future build. NYSBOE should keep track of these issues to ensure that they are resolved in any future versions brought to them for certification.
- The one open functional discrepancy (JIRA) should be tracked and shown to be fixed in a future version.

2.3 Components in the ClearVote 2.4 System

According to the SLI report, *“The ClearVote 2.4 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:

ClearDesign 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.

ClearMark – A standalone precinct level ballot marking device (BMD) that includes an audio tactile interface (ATI).

ClearCast – A scan precinct ballot counter (tabulator) that is used in conjunction with an external ballot box.

ClearCount – A high-speed, central ballot scanning system used for the high-volume processing of ballots.

3 SLI Testing

This section reviews the testing SLI performed on the ClearVote 2.4 system.

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 would 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 indicated “shall” was accepted without evaluating test cases. NYSTEC reviewed SLI’s assessment of prior work for the ClearVote 2.4 system and resolved with SLI all our questions. NYSTEC’s final review, including all comments, is included in this report as Attachment A.

3.1.2 Technical Data Package (TDP) Review

The 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 (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 identified no outstanding issues. 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 ClearVote 2.4 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 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 were resolved. NYSTEC’s final review of the security functional test report, including all comments, is included in this report as Attachment I.

NYSTEC 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 completed 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, which 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 ClearVote 2.4 code base.

Checkmarx identified 617 potential vulnerabilities, but approximately 82% of findings were marked as “Not Exploitable.” The remaining findings were added to a list of 109 potential vulnerabilities. SLI classified the exploit potential of those 109 potential vulnerabilities to require “extensive knowledge of the system or a vendor insider.”

No JIRAs were created for those potential vulnerabilities, as many were judged to be false positives. The others — when examined within the context of the physical environment, implemented security controls, and knowledge required to exploit the issue — were assessed by SLI to not pose a significant threat to the ClearVote 2.4 system.

Cyber Castellum noted the shortcomings related to the following items as identified 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. For an explanation of each shortcoming, see Sections [3.3.2.1](#), [3.3.2.2](#), and [3.3.2.3](#).

SLI did not use the Checkmarx software to scan installed commercial off-the-shelf (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.”

“SLI has conducted triage of all vulnerabilities identified by Checkmarx. According to the triage conducted, over 82% are false positive, Not Exploitable. Thus, as a result, none of the vulnerabilities triaged were confirmed to be an issue. This is highly unlikely, as out of the 617 vulnerabilities triaged, not even a single vulnerability is confirmed.”

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

*“**Not Exploitable** – confirmed to be a false positive. Either compensating controls exist which the scanner missed or misinterpreted the context.”*

Thus, the 508 (617 findings minus 109 potential vulnerabilities) findings are not necessarily false positives. SLI believes there are countermeasures in place to keep the vulnerabilities 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, Clear Ballot 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:

“There is no methodology or process documented in the SLI plans and/or reports for the identification of vulnerabilities in software dependencies. It was confirmed during a call with SLI that they do not have the rights to Checkmarx SCA and no other tool is utilized for the identification of vulnerabilities in software dependencies. The SLI reports do not include any vulnerabilities associated with dependency checks. However, a list of vulnerabilities associated with platform and libraries have been provided. Due to the lack of understanding of the methodology and process Cyber Castellum cannot validate the completeness of the list.”

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 four informational discrepancies, all due to code indentation the same as the function. No other code quality issues have been identified.”

Most of the source code quality issues relate to 2005 VVSG requirements, which were tested in the ClearVote 2.3 EAC Certification. As such, SLI performed a manual review of only higher risk VVSG requirements, which explains the low number of code quality findings.

4 Discrepancies

4.1 SLI Findings

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	66	4	109	179
Open discrepancies	1	4	109	114

4.2 Open Discrepancies

As of the conclusion of this testing effort, there is one open functional discrepancy.

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. NYSTEC reviewed the following SLI deliverables:
 - 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. Cyber Castellum reviewed the following SLI deliverables:
 - 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 Clear Ballot to resolve any discrepancies.
- NYSTEC reviewed all final reports from SLI:
 - Master test report.
 - Functional test report.
 - Security functional test report.

6 Documents Referenced

TABLE 2, DOCUMENTS REFERENCED

SLI TEST PLANS, TEST CASES, AND REQUIREMENTS MAPPING
Evaluation of Prior Work for Clear Ballot ClearVote 2.4 v2.0.pdf.
TDP Review for Clear Ballot ClearVote 2.4.pdf: <ul style="list-style-type: none"> • Attachment A – NYS Clear Ballot ClearVote 2.4 TDP List.pdf. • Attachment B – NYS Clear Ballot ClearVote 2.4 TDP JIRAs (Confidential).pdf.
NYS ClearVote 2.4 Requirements Matrix v2.0.xlsx.
NYSBOE Clear Ballot ClearVote 24 Master Test Plan v1.0.pdf.
NYSBOE Clear Ballot ClearVote 2.4 Functional Test Plan v2.0.pdf.
NYSBOE Clear Ballot ClearVote 2.4 Security Functional Test Plan v2.0.pdf.
NY Clear Ballot ClearVote 2.4 Security Test Cases.xlsx.
NYSBOE Clear Ballot ClearVote 2.4 Source Code Review Test Plan v1.0.pdf.
NYSBOE Clear Ballot ClearVote 2.4 Security Source Code Review Test Plan v1.0.pdf.
SLI TEST REPORTS
NYSBOE Clear Ballot ClearVote 2.4 Functional Test Report v3.0.pdf: <ul style="list-style-type: none"> • Attachment A – NYS Clear Ballot ClearVote 2.4 Requirements w Test Cases.xlsx. • Attachment B – NYS Clear Ballot ClearVote 2.4 As Run Test Cases (Confidential).

<ul style="list-style-type: none"> Attachment C – NYS Clear Ballot ClearVote 2.4 Functional JIRAs (Confidential).pdf.
<p>NYSBOE Clear Ballot ClearVote 2.4 Functional Security Test Report v3.0.pdf:</p> <ul style="list-style-type: none"> Attachment A – NYS Clear Ballot ClearVote 2.4 Requirements w Test Cases.xlsx. Attachment B - NYS Clear Ballot ClearVote 2.4 Security Test Cases (Confidential). Attachment C - NYS Clear Ballot ClearVote 2.4 Security Jira Issues (Confidential).pdf. Attachment D - NYS Clear Ballot ClearVote 2.4 Security Test Artifacts (Confidential). Attachment E - NYS Clear Ballot ClearVote 2.4 Security Test Notebook (Confidential).pdf.
<p>NY Clear Ballot ClearVote 2.4 Master Test Report v2.0.pdf:</p> <ul style="list-style-type: none"> Attachment A – Clear Ballot ClearVote 2.4 NYS Voting Systems Requirements.xlsx. Attachment B - SLI Testing Approach for Clear Ballot ClearVote 2.4 - Finalized 12132022.pdf. Attachment C – NYS Clear Ballot ClearVote 2.4 Master JIRAs (Confidential).pdf.
<p>NYSBOE Clear Ballot ClearVote 2.4 Source Code Review Test Report v2.0.pdf:</p> <ul style="list-style-type: none"> Attachment A – Clear Ballot ClearVote 2.4 NYS Voting Systems Requirements.xlsx. Attachment B - ClearVote 2.4 List of Source code Reviewed (Confidential). Attachment C - Source Code Review Form Spreadsheets (Confidential). Attachment D - Source code Review Discrepancy Report Forms (Confidential). Attachment E - Source Code Review Test Cases.pdf. Attachment F - Clear Ballot Declared Standards. <p>NYSBOE Clear Ballot ClearVote 2.4 Security Source Code Review Test Report v2.0.pdf:</p> <ul style="list-style-type: none"> Attachment A – Clear Ballot ClearVote 2.4 NYS Voting Systems Requirements.xlsx. Attachment B - ClearVote 2.4 List of Source code Reviewed (Confidential). Attachment C - Checkmarx Final Results (Confidential). Attachment D - Checkmarx Software Audit - Clear Ballot Responses (Confidential). Attachment E - Checkmarx Queries List. Attachment F - Checkmarx Informational Results (Confidential).
<p>REPORTS FROM NYSTEC SUBCONTRACTOR CYBER CASTELLUM</p>
<p>ClearVote 2.4 Code Review Test Plan Comments - Final Draft v1.0.pdf.</p>
<p>Evaluation of SLI Clear Ballot Code Review Report.pdf.</p>

7 Attachments

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



YOUR INDEPENDENT TECHNOLOGY ADVISOR

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

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

ALBANY
540 Broadway, 3rd Floor
Albany, NY 12207

NEW YORK CITY
27 West 24th St., Suite 901
New York, NY 10010