Report:

Testing Oversight of Hart Verity Voting 2.7

Final Report v1

Prepared for:

NEW YORK STATE Board of Elections

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

November 16, 2022

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

ACRONYMS AND TERMS	
CVE	Common Vulnerabilities and Exposures
EAC	Election Assistance Commission
NYS	New York State
QA	Quality Assurance
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 Verity Voting 2.7 electronic voting system that was developed by Hart InterCivic for certification and use in New York State (NYS) 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 NYS 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.

Verity Voting 2.7 is U.S. Election Assistance Commission (EAC) certified, with the exception of Verity Reader. Verity Reader was not included in the EAC testing because it is a component specifically used in NYS. Verity Reader was tested for all VVSG requirements, in addition to NYS-specific testing. In addition, because SLI was the voting system testing laboratory (VSTL) that conducted the EAC testing for the Verity Voting 2.7 system, NYSTEC contracted with Cyber Castellum to complete a review of 10% of the source code base, SLI's source code and security source code test plans, and the results of SLI's source code testing, in addition to completing a gap analysis, to ensure a thorough security review. As the entire voting system will be used in NYS 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 list of discrepancies found by SLI and Cyber Castellum during testing.
- A description of open discrepancies.
- A breakdown of the work performed by NYSTEC.

2 Executive Summary

SLI tested the functionality, security, and system documentation of the Verity Voting 2.7 system, based on VVSG version 1.0 (2005) and NYS voting laws and regulations (2021). NYSTEC reviewed SLI's requirement mapping, test plans, discrepancies (JIRAs), 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 Verity Voting 2.7 system included:

- All applicable 2021 NYS 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 Verity Voting 2.7 certification event.

With the exception of Verity Reader, all 2005 VVSG requirements that indicate "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 NYS testing, all 2005 VVSG requirements that indicate "should" were tested as if the "should" reads as "shall." Verity Reader was fully tested for all VVSG requirements.

2.1 NYSTEC Recommendations

NYSTEC has the following recommendation:

- Several issues were found by Cyber Castellum during their independent review of 10% of the code base which do not pose a threat to the current voting system as tested. 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 Hart 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. See Section 4.2 "Cyber Castellum Findings" for more details.

2.2 Components in the Verity Voting 2.7 System

According to the SLI report, "The Verity Voting 2.7 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:

Verity Scan — A digital scan precinct ballot counter (tabulator) that is used in conjunction with an external ballot box.

Verity Print — An on-demand ballot production device for unmarked paper ballots.

Verity Reader — A polling place device that allows voters to scan and see the ballot they have voted.

Verity Election Management — Allows administrators to import and manage election definitions.

Verity User Manager — Enables users with the correct role and permissions to create and manage user accounts.

Verity Desktop — Enables users to set the workstations' date and time, gather Verity application hash codes, and access the Windows desktop.

Verity Data — Provides users with controls for entering and proofing data and audio.

Verity Build — Begins the election event to proof data, view reports, and print ballots, and allows for configuring and programming Verity Scan, Verity Touch Writer, and Verity Print, as well as producing the election definition and auditing reports.

Verity Central — A high-speed, central digital ballot scanning system.

Verity Count — An application that tabulates election results and generates reports.

3 SLI Testing

This section reviews the testing performed on the Verity Voting 2.7 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 what versions will need to be reviewed during this testing event. This aids SLI in determining the scope of testing. NYSBOE's policy is to leverage all EAC testing for NYS such that any VVSG 1.0 (2005) requirement that indicates "shall" will be accepted without evaluating test cases. NYSTEC reviewed SLI's assessment of prior work for the Verity Voting 2.7 system. NYSTEC resolved all of 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 TDP review assesses the technical documentation submitted to NYS for this certification testing event. SLI works with the vendor throughout the testing process to ensure that any updates needed — due to changes required to remediate issues found during testing — are 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 NYS 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. Two requirements' matrices were created for this testing effort, one for Verity Reader and the other for the entire system. NYSTEC reviewed both, and all questions were resolved. NYSTEC's final reviews, including all comments, are included in this report for the Verity Reader as Attachment C and the entire system as Attachment D.

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 4.1.3, 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 E.

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 F.

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 Verity Voting 2.7 system against all applicable NYS 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 G, and our review of the functional test report is included as Attachment H.

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 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. A complete review of all JIRAs created during testing is included in this report as Attachment K.

Questions that arose during the review of the security functional test report centered around gaining clarity on what devices were tested against which requirements. SLI provided explanations for their testing decisions and provided additional information to demonstrate that all devices were tested. All remaining questions were resolved. NYSTEC's final review of the security functional test report, including all comments, is included in this report as Attachment L.

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 NYS requirements. Cyber Castellum completed a review of SLI's source code test plans and comments are included in this report as Attachment M.

3.3.2 Source Code Review Reports

Cyber Castellum also completed a QA review of both source code review reports resulting from SLI's testing. 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 Verity Voting 2.7 code base. A list was produced that showed 68 high, 57 medium, and 2,235 low severity findings, which were discussed with SLI and NYSBOE. No JIRAs were created for those findings as many were false positives and because, when examined within the context of the physical environment and implemented security controls, they did not pose a significant threat to the Verity Voting 2.7 system.

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.

Cyber Castellum investigated, at NYSBOE's request, the many issues found by the Checkmarx automated scan performed by SLI and concluded the review in agreement with SLI's assessment of the findings. All questions were answered, and no additional work was requested of SLI.

The remaining issues pertaining to the source code that are detailed in section 4.2 and in Cyber Castellum's final report refer to issues found during their independent review of 10% of the code base and are included in this report as Attachment N.

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.

There are two issues that NYSTEC specifically looks closely at due to past difficulty with compliance. The first is the software integrity or 'hash check' requirement (VVSG 7.4.6). The second is the digital signature requirement (6209.2.F.12 and 6209.2.F.13.ii). The software integrity protocol provided by Hart and the results of SLIs investigation were found to be satisfactory. No additional work is needed for compliance. The results of the investigation into the use of digital signatures for Verity Voting 2.7 provided enough information that NYSTEC believes this security requirement was implemented correctly and no additional work needs to be completed for compliance.

TABLE 1, COUNT OF ALL DISCREPANCIES REPORTED BY SLI

	FUNCTIONAL	SECURITY FUNCTIONAL	SOURCE CODE	TOTAL
Discrepancies found during testing	12	0	0	12
Open discrepancies	1	0	0	1

4.2 Cyber Castellum Findings

A review of the source code to verify compliance with EAC requirements was initially completed by SLI as the VSTL earlier this year. As a part of the NYS certification effort, a 10% check of the code base must be completed. Because SLI was the VSTL for the EAC testing, NYSTEC contracted Cyber Castellum to complete this 10% check. NYSTEC reviewed the report created by Cyber Castellum for their QA review and security gap analysis of 10% of the Verity Voting 2.7 code base, included as attachment N. Table 2 shows a synopsis of each discrepancy found by Cyber Castellum during their independent QA review and gap analysis, as well as NYSTEC's comments on each issue listed.

TABLE 2, CYBER CASTELLUM FINDINGS

FINDING	DESCRIPTION *(From the Cyber Castellum Report)*	HART RESPONSE	
Single Exit Point	“Regular expressions were used to identify instances of multiple return statements within a given function/methods.”	The files listed are automatically generated during the product compilation by Microsoft Visual Studio. They are neither created nor modified by Hart. As such, they are not required to conform to Hart's coding standard. There is no security threat associated with this finding.	NYSTEC agrees that this is a compliance finding and that any risk is minimal.
Line Length	“Line lengths should be no greater than 132 characters. Line lengths greater than 120 must be justified.”	Hart does acknowledge this finding and will address the line length issue (exceeds 150) in a future version as it does not represent a security threat.	NYSTEC agrees that this is a compliance finding and that any risk is minimal. This finding will be tracked for review in a future release.
SecureString Data Type	“…in some instances, it fails to consistently use the SecureString across the application”	One finding is a false positive, the other two will be addressed in a future release to ensure that validation and functionality can be maintained.	These findings will be tracked for review in a future release.
Dangerous Functions	“Use of banned functions that are more like to produce vulnerabilities. All	… the Microsoft “banned” functions list only triggers additional scrutiny and care by Microsoft engineers when using these functions in certain situations. Although they suggest	NYSTEC agrees that the risk is acceptable due to the other controls in the operating environment of the software. However,

FINDING	DESCRIPTION *(From the Cyber Castellum Report)*	HART RESPONSE	
	these functions have secure alternatives.”	alternatives with built-in validations when available, Microsoft still actively uses these functions when appropriate. It should be noted that holistic security mitigations, penetration testing activities, and multiple certification events have not identified an exploit within the Verity environment due to this finding.	relying on assumptions of the environment the code will run can create risks in the future if the configuration of the environment changes. Therefore, NYSTEC recommends that this code be revised for future releases.
New() without Delete()	“The application dynamically allocates memory but fails to release the memory as expected.”	No response received by report release date.	Using new without delete in this case is not going to result in a memory leak.
Use of Realloc()	“Use of realloc() can expose residual memory contents or render existing buffers impossible to securely erase.”	No response received by report release date.	It is commonly recommended that dynamic memory allocation should not be used in "high integrity" embedded systems. Reasons include potential memory leaks and undefined or unspecified behavior with associated functions.
Insecure Loading of Library	“The function searches several paths for a library if called with a filename, but no path. This can allow trojan DLLs to be deployed, regardless of the presence of the correct DLL. Ensure that a full path is specified.”	… it is unproven that an exploit exists in the Verity environment.	NYSTEC agrees that the risk is acceptable due to the other controls in the operating environment of the software. However, relying on assumptions of the environment the code will run can create risks in the future if the configuration of the environment changes. Therefore, NYSTEC recommends that this code be reviewed for future releases.
SQL Injection	“… a function takes input from a ‘query’ parameter which is not sanitized that may allow a SQL Injection to occur.”	… it is unproven that an exploit exists in the Verity environment.	NYSTEC agrees that the risk is acceptable due to the other controls in the operating environment of the software. However, relying on assumptions of the environment the code will run can create risks in the future if the configuration of the environment changes. Therefore, NYSTEC

FINDING	DESCRIPTION *(From the Cyber Castellum Report)*	HART RESPONSE	
			recommends that this code be reviewed for future releases.
Suspicious Comment	"The code contains comments that suggest the presence of bugs, incomplete functionality, or weaknesses."	… finding should have been resolved in an earlier release as it is no longer relevant. Hart will remove it in a future release.	This finding will be tracked for review in a future release.
Vulnerabilities in Dependencies	"These vulnerabilities are identified by a Common Vulnerabilities and Exposures (CVEs) number that comes from the National Vulnerability Database (NVD). Additionally, each of the CVEs relates to a Common Weakness Enumeration (CWE) that describes the weakness."	CVEs evaluated by Cyber Castellum are N/A for their system.	NYSTEC agrees with Hart's assessment that the CVEs identified by Cyber Castellum are not applicable

TABLE 3, COUNT OF ALL DISCREPENCIES REPORTED BY CYBER CASTELLUM

	INDEPENDENT SOURCE CODE
Discrepancies found during testing	10

4.3 Open Discrepancies

As of the conclusion of this testing effort, there is only one (1) open discrepancy from SLI and three (3) open discrepancies from Cyber Castellum that will be tracked for remediation in a future release. As mentioned above, a full review of all SLIs JIRAs can be found in Attachment K.

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 review.
    - 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, an independent review of 10% of the Verity Voting 2.7 code base, and a security gap analysis. Cyber Castellum conducted their reviews in parallel with 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 Hart to resolve any discrepancies.
- NYSTEC reviewed all final reports from SLI:
    - Master test plan report
    - Functional test report

- Security functional test report

6 Documents Referenced

SLI TEST PLANS, TEST CASES, AND REQUIREMENTS MAPPING
Evaluation of Prior Work for Hart Verity Voting 2.7 v2.0.pdf
TDP Review for Hart InterCivic Verity Voting 2.7.pdf • Attachment A - NYS Hart InterCivic Verity Voting 2.7 TDP List.pdf • Attachment B - NYS Hart InterCivic Verity Voting 2.7 TDP Issues.pdf
Hart Verity 2.7 Reader NY Req Matrix v1.0.xls
Hart Verity Voting 2.7 NY Req Matrix v1.0.xls
NYSBOE Hart InterCivic Verity Voting 2.7 Master Test Plan v2.0.pdf
NYSBOE Hart InterCivic Verity Voting 2.7 Functional Test Plan v2.0.pdf
NYSBOE Hart InterCivic Verity Voting 2.7 Security Functional Test Plan v2.0.pdf
Verity Voting 2.7 Security Functional Test Cases • NY Verity 2.7 Security Test Suite.pdf • NY Hart Verity 2.7 Security test suite AsRun.pdf
NYSBOE Hart Verity 2.7 Source Code Review Test Plan v1.0.pdf • Attachment A1 - Hart InterCivic Verity Voting 2.7 NYS Voting Systems Requirements Matrix • Attachment A2 - Hart InterCivic Verity Voting 2.7 Reader NYS Req Matrix • Attachment B - SLI Testing Approach Verity 2.7 - 2.25.2022 Final • Attachment C - A Microsoft All-in-One-Code-Framework Coding Standards
SLI TEST REPORTS
NYSBOE Hart InterCivic Verity Voting 2.7 Functional Test Report v1.0.pdf • Attachment A1 - Hart InterCivic Verity Voting 2.7 NYS System Requirements Matrix w Test Cases v1.0.pdf • Attachment A2 - Hart InterCivic Verity Voting 2.7 Reader NYS Requirements Matrix w Test Cases v1.0.pdf • Attachment B - NYS Hart InterCivic Verity Voting 2.7 As Run Test Cases (Confidential).pdf • Attachment C - NYS Hart InterCivic Verity Voting 2.7 JIRAs (Confidential).pdf
NYSBOE Hart InterCivic Verity Voting 2.7 Security Functional Test Report v1.0.pdf • Attachment A1 - Hart InterCivic Verity Voting 2.7 NYS System Requirements Matrix w Test Cases v1.0.xlsx • Attachment A2 - Hart InterCivic Verity Voting 2.7 Reader NYS Requirements Matrix w Test Cases v2.0.xlsx • Attachment B - SLI Testing Approach Verity 2.7 - 2.25.2022 Final.pdf • Attachment C - NYS Hart InterCivic Verity Voting 2.7 JIRAs (Confidential).pdf
NY Hart InterCivic Verity Voting 2.7 Master Test Report v1.0.pdf

REPORTS FROM NYSTEC SUBCONTRACTOR CYBER CASTELLUM
Code Review Test Plans Review - Cyber Castellum
Static Code Analysis Report v1.0 - Cyber Castellum

7 Attachments

A. Verity Voting 2.7 - Prior Work - NYSTEC Comments.pdf
B. Verity Voting 2.7 - TDP Review - NYSTEC Comments.pdf
C. Verity Reader - NYS Requirements Matrix - NYSTEC Comments.pdf
D. Verity Voting 2.7 - NYS Requirements Matrix - NYSTEC Comments.pdf
E. Verity Voting 2.7 - Master Test Plan - NYSTEC Comments.pdf
F. Verity Voting 2.7 - Master Test Report - NYSTEC Comments.pdf
G. Verity Voting 2.7 - Functional Test Plan - NYSTEC Comments.pdf
H. Verity Voting 2.7 - Functional Test Report - NYSTEC Comments.pdf
I. Verity Voting 2.7 - Security Functional Test Plan - NYSTEC Comments.pdf
J. Verity Voting 2.7 – Security Functional Test Cases – NYSTEC Comments.pdf
K. Verity Voting 2.7 – JIRA Report 10.18.22 – NYSTEC Comments.pdf
L. Verity Voting 2.7 - Security Functional Test Report – NYSTEC Comments.pdf
M. Verity Voting 2.7 - Code Review Test Plans Review - Cyber Castellum.pdf
N. Verity Voting 2.7 - Static Code Analysis Report v1.0 - Cyber Castellum.pdf

NYSTEC
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