Report:

Testing Oversight of Dominion Democracy Suite (D-Suite) 5.16

Public Report v1.0

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

May 17, 2023

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

ACRONYMS AND TERMS	
ATI	Audio Tactile Interface
CISA	Cybersecurity & Infrastructure Security Agency
COTS	Commercial Off-the-Shelf
EAC	Election Assistance Commission
EMS	Election Management Software
ICC	ImageCast Central
ICE	ImageCast Evolution Ballot Counter
ICP	ImageCast Precinct Ballot Counter
ICP2	ImageCast Precinct Ballot Counter 2
ICX-BMD	ImageCast Ballot Marking Device
NYS	New York State
NYSBOE	New York State Board of Elections
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 to perform an independent review of work conducted by SLI Compliance (SLI) for testing the Democracy Suite 5.16 (D-Suite) electronic voting system developed by Dominion Voting Systems 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 of the system's source code.

Democracy Suite versions 5.0, 5.5, 5.5-A, 5.5-B, 5.5-C, and 5.5-D are U.S. Election Assistance Commission (EAC) certified. D-Suite v5.15 — which was used as the code base for the updates included in v5.16, which is being presented for certification — shares its code base with v5.5-D. 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 breakdown of the work performed by NYSTEC.

2 Executive Summary

SLI tested the functionality, security, and system documentation of the D-Suite 5.16 system based on 2005 VVSG 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 D-Suite 5.16 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 2005 VVSG, Volume 1 and 2 requirements, per the NYSBOE-approved testing approach for the D-Suite 5.16 certification event.

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” read as “shall.”

2.1 Additional Testing

NYSBOE requested that a known potential voter privacy issue with this system be tested. The issue was that certain generated reports contain a randomized ID number. Those randomized IDs can be un-randomized, leaving the potential to determine the order in which voting records were created and, thus, possibly the order of the voters. The compensating control is to delete this column of IDs if the report is generated. NYSTEC notes that if these numbers remain in the internal database, there is a risk that they can be accessed.

On 6/3/2022, the United States Cybersecurity & Infrastructure Security Agency (CISA) created an advisory for one of the components in the Dominion system being certified. The findings in that advisory were specifically tested by SLI and they determined the following. (From the SLI “Dominion Democracy Suite 5.16 Security Functional Test Report v5.0”):

> *“The ICS Advisory (ICSA-22-154-01) notes several potential vulnerabilities discovered in an investigation prior to and independent of the SLI Compliance Functional Security testing of the Dominion Democracy Suite 5.16 voting system. The vulnerabilities described are specific to the ImageCast X (ICX) device. The advisory was incorporated during functional security testing and the ICX was reviewed for potential security weaknesses. The results of security testing concluded that the voting system documentation employed sufficient physical and procedural controls over the system such that the effort and resources required of an adversary to effectively exploit the device were infeasible within the constraints of a production environment.”*

2.2 NYSTEC Recommendations

NYSTEC has the following recommendation:

- Numerous issues were found by SLI during their review of the Dominion 5.16 source code. However, 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 Dominion remediate these issues in their code 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 two open discrepancies should be addressed in the next iteration of the system.

2.3 Components in the D-Suite 5.16 System

According to the SLI report, "The DVS 5.16 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 responsible for all pre-voting and post-voting groups of activities in the process of defining and managing elections.

ImageCast Precinct Ballot Counter (ICP) — A digital scan precinct ballot counter (tabulator) that is used in conjunction with an external ballot box.

ImageCast Precinct Ballot Counter 2 (ICP2) — A digital scan precinct ballot counter (tabulator) that is used in conjunction with an external ballot box.

ImageCast Evolution Ballot Counter (ICE) — A digital scan precinct ballot counter (tabulator) that is used in conjunction with an external ballot box.

ImageCast Central (ICC) — A high-speed, central digital ballot scanning system used for the high-volume processing of ballots (such as vote by mail).

ImageCast X (ICX-BMD) — A standalone precinct level ballot marking device (BMD) that includes an audio Tactile interface (ATI).

3 SLI Testing

This section reviews the testing SLI performed on the D-Suite 5.16 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 component versions (if any) required full 2005 VVSG review 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 2005 VVSG requirement that indicates "shall" will be accepted without evaluating test cases. NYSTEC reviewed SLI's assessment of prior work for the D-Suite 5.16 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 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 2005 VVSG and NYS requirements against any modifications or prior work. This high-level assessment is then mapped directly to the master test plan, individual test plans, and — at the lowest level — test cases. NYSTEC's final review, including all comments, is 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.

The 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 D-Suite 5.16 system against all applicable NYS 2021 election law, §6209 Voting System Standards, and 2005 VVSG 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, and our 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.

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 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 evaluated the code base against NYS 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 D-Suite 5.16 code base. A list of potential vulnerabilities was produced that showed 16 of high severity and 1,084 of medium severity. No JIRAs were created for those findings. In total, 52,877 potential vulnerabilities were identified, but approximately 95% of findings were marked as "Not Exploitable."

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. For an explanation of each shortcoming, see Sections 3.3.2.1, 3.3.2.2, and 3.3.2.3.

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. Roughly 95 percent (51,785 out of 52,877) of the Checkmarx vulnerabilities were identified as false positive. 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 *52,877* 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, Dominion 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 v4.0 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 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.

3.3.2.3 Quality of Source Code

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

> *"The report that focused on the quality of the source code only identified 60 dangerous functions. No other code quality issues have been identified."*

Most of the source code quality issues are 2005 VVSG requirements, and SLI performed such reviews on only 10% of the code base, which explains the low number of code quality findings.

In addition, NYSTEC verified that SLI manually investigated for any known vulnerabilities for installed commercial off-the-shelf (COTS) software.

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

	FUNCTIONAL (JIRAS)	SOURCE CODE	SECURITY SOURCE CODE (POTENTIAL VULNERABILITIES)	TOTAL
Discrepancies found during testing	34	60	1,095	1,189
Open discrepancies	2	60	1,095	1,157

4.2 Open Discrepancies

As of the conclusion of this testing effort, there are two open discrepancies (JIRAs) from SLI and 1,155 from source code reviews that will be tracked for remediation in a future release.

5 NYSTEC Activities

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

- Reviewed all pre-testing 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 pre-testing 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.
    - Source code review test report.
    - Security source code review test report.
- NYSTEC reviewed the security functional test cases and found SLI sufficiently tested the system. Any issues noted by NYSTEC 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 Dominion 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, SLI TEST PLANS, TEST CASES, AND REQUIREMENTS MAPPING

SLI TEST PLANS, TEST CASES, AND REQUIREMENTS MAPPING
• Evaluation of Prior Work for Dominion DS 5.16 v2.0.
• TDP Review for Dominion DS 5.16.pdf. ○ Attachment A - NYS Dominion DS 5.16 TDP List.pdf. ○ Attachment B - NYS Dominion DS 5.16 TDP Issues v2.0.pdf.
• NYS Dominion DVS 5.16 Requirements Matrix v1.3.xls.
• NYSBOE Dominion DVS 5.16 Master Test Plan v3.0.pdf. ○ Attachment A – NY Dominion D-Suite 5.16 Requirements Matrix. ○ Attachment B - SLI Testing Approach DVS 5.16 - 1.28.2022 – FINAL.
• NYSBOE Dominion DS 5.16 Functional Test Plan v3.0.pdf.
• NYSBOE Dominion DS 5.16 Security Functional Test Plan v2.0.pdf.
• NY Dominion 5.16 Security Functional Test Cases. ○ NY Dominion 5.16 Security Test Suite.pdf.
• NYSBOE Dominion D-Suite 5.16 Security Source Code Review Test Plan v3.0. • NYSBOE Dominion D-Suite 5.16 Source Code Review Test Plan v2.0. ○ Attachment A – NY Dominion D-Suite 5.16 Requirements Matrix.xls. ○ Attachment B - SLI Testing Approach DVS 5.16 - 1.28.2022 – FINAL.pdf. ○ Attachment C – Dominion Declared Coding Standards.
SLI TEST REPORTS
• NY Dominion DS 5.16 Master Test Report v5.0. ○ Attachment A – NY Dominion D-Suite 5.16 Requirements Matrix w TestCases.xls. ○ Attachment B - SLI Testing Approach DVS 5.16 - 1.28.2022 – FINAL.pdf. ○ Attachment C – NYS Dominion Voting Systems DS 5.16 Master JIRAs v3.0 (Confidential).
• NYSBOE Dominion DS 5.16 Functional Test Report v4.0.pdf. ○ Attachment A – NY Dominion D-Suite 5.16 Requirements Matrix w TestCases.pdf. ○ Attachment B - NYS Dominion Voting Systems DS 5.16 As Run Test Cases (Confidential). ○ Attachment C – NYS Dominion Voting Systems DS 5.16 Functional JIRAs (Confidential).pdf
• NYSBOE Dominion DS 5.16 Functional Security Test Report v6.0.pdf. ○ Attachment A - NYS Dominion DS 5.16 Requirements Matrix.xlsx. ○ Attachment B - NYS Dominion DS 5.16 Security Test Cases (CONFIDENTIAL).pdf.

○ Attachment C - NYS Dominion DS 5.16 Security Jira Issues v5.0 (CONFIDENTIAL).pdf. ○ Attachment D – NYS Dominion DS 5.16 Security Test Artifacts (CONFIDENTIAL). ○ Attachment E - NYS Dominion DS 5.16 Security Test Notebook (CONFIDENTIAL).pdf.
• NYSBOE Dominion D-Suite 5.16 Source Code Review Test Report v3.0. ○ Attachment A – NY Dominion D-Suite 5.16 Requirements Matrix.xls. ○ Attachment B – D-Suite 5.16 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 - Dominion Declared Standards.
• NYSBOE Dominion D-Suite 5.16 Security Source Code Review Test Report v5.0.pdf. ○ Attachment A – NY Dominion D-Suite 5.16 Requirements Matrix.xls. ○ Attachment B – D-Suite 5.16 List of Source Code Reviewed (Confidential). ○ Attachment C – CheckMarx Final Results (Confidential). ○ Attachment D – DVS 5.16 Checkmarx Software Audit - Dominion Response (Confidential). ○ Attachment E – CheckMarx Queries List. ○ Attachment F – Checkmarx Informational Results (Confidential).
REPORTS FROM NYSTEC SUBCONTRACTOR CYBER CASTELLUM
• Dominion D-Suite 5.16 Code Review Test Plan Comments - Cyber Castellum.
• Evaluation of SLI Dominion 5.16 Code Review Reports - Cyber Castellum.

7 Attachments

A. Dominion D-Suite 5.16 - Prior Work - NYSTEC Comments.pdf
B. Dominion D-Suite 5.16 - TDP Review - NYSTEC Comments.pdf
C. Dominion D-Suite 5.16 - NYS Requirements Matrix - NYSTEC Comments.pdf
D. Dominion D-Suite 5.16 - Master Test Plan - NYSTEC Comments.pdf
E. Dominion D-Suite 5.16 - Master Test Report - NYSTEC Comments.pdf
F. Dominion D-Suite 5.16 - Functional Test Plan - NYSTEC Comments.pdf
G. Dominion D-Suite 5.16 - Functional Test Report - NYSTEC Comments.pdf
H. Dominion D-Suite 5.16 - Security Functional Test Plan - NYSTEC Comments.pdf
I. Dominion D-Suite 5.16 - Security Functional Test Report - NYSTEC Comments.pdf
J. Dominion D-Suite 5.16 - Security Functional Test CASES - NYSTEC Comments.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