ALEX PADILLA | SECRETARY OF STATE | STATE OF CALIFORNIA
OFFICE OF VOTING SYSTEMS TECHNOLOGY ASSESSMENT
1500 11th Street | Sacramento, CA 95814 | **Tel** 916.695-1680 | **Fax** 916.653.4620 | www.sos.ca.gov

DOMINION VOTING SYSTEMS
Interscan 821D HiPro Scanner
Modification to DemSuite 5.2
Administrative Approval Report

Components:
Interscan 821D HiPro Scanner,
Dell OptiPlex 7040 Workstation,
ImageCast Central Version 5.2.2.7

Staff Administrative Approval Report
Prepared by:
Secretary of State's Office of
Voting Systems Technology Assessment
May 8, 2018

Table of Contents

I. INTRODUCTION

1. Scope

This report presents the test results for all phases of the approval testing of the Dominion Voting Systems (Dominion) modification to the Democracy Suite (DemSuite) 5.2 voting system. This modification is for the addition of the Interscan 821D HiPro ballot scanner and ImageCast Central (HSS-ICC) software. The purpose of testing is to test the compliance of the modified voting system with California Voting Systems Standards, and State and Federal laws. Testing also uncovers other findings, which do not constitute non-compliance, and those findings are reported to the voting system vendor to address the issues procedurally. The procedures for mitigating any additional findings are made to the documentation, specifically the California Use Procedures.

2. Summary of the Application for Administrative Approval

Dominion submitted an application for Administrative Approval of the modification to the DemSuite 5.2 voting system on October 18, 2017. The modification is comprised of the addition of the Interscan 821D HiPro scanner, and Dell Optiplex 7040 workstation running Windows 10 and HSS-ICC software version 5.2.2.7. The HSS-ICC version 5.2.2.7 software is a modified version of the ImageCast Central utility which was previously approved for use in California with the Canon X10 and Canon G1130 scanners.

In addition to the software, which includes the executable code and the source code for the amended HSS-ICC, Dominion was required to submit the following:

- Technical Documentation for the Interscan 821D HiPro scanner;
- All the hardware components to field a working version of the Interscan 821D HiPro scanner;
- Optiplex 7040 Workstation running HSS-ICC software, including all peripheral devices;
- Amended California Use Procedures.

3. Contracting and Consultants

Upon receipt of a complete application, the Secretary of State released a Request for Proposal (RFP) for assistance with both Source Code and Security and Telecommunications Review.

Through the formal California contracting process, the Secretary of State awarded a contract to SLI Compliance (SLI), 4720 Independence Street, Wheat Ridge, Colorado.

II. SUMMARY OF THE SYSTEM

The Dominion DemSuite Interscan 821D HiPro scanner/HSS-ICC system consists of a

Interscan 821D HiPro scanner and ImageCast Central workstation, and is used for processing ballots (such as vote by mail) in a central tabulation configuration. This ballot counter unit is based on commercial off the shelf (COTS) hardware coupled with custom-made ballot processing application software. It is used for high-speed centralized scanning and counting of paper ballots.

III. TESTING INFORMATION AND RESULTS

1. Background

Testing of the modification to the DemSuite 5.2 voting system took place from November 13, 2017, through May 1, 2018. Testing began with the Functional Testing Phase, which included Volume Testing, followed by Security/Telecommunications Testing, and Source Code Review for the modified HSS-ICC software.

2. Functional Test Data and Results

The Functional Test of the modified Dominion DemSuite 5.2 voting system was conducted by Office of Voting Systems Technology Assessment and Dominion staff at the Secretary of State's Office located at 1500 11th Street, Sacramento, California. The Functional Test focused on the border connections with the existing system, and testing of the Interscan 821D HiPro scanner.

The Secretary of State ran the Functional Test as if it were a jurisdiction that just purchased the modified voting system utilizing the Interscan 821D HiPro scanner. Testing of the system began with building the HSS-ICC workstation. The HSS-ICC workstation is a Dell OptiPlex 7040 computer running the modified ImageCast Central software. This build was started by wiping the Optiplex 7040 computer in order to clean the existing Dell provided software from the workstation. The wipe was followed by the installation of the Windows 10 operating system, commercial-off-the-shelf drivers, HSS-ICC trusted build software, and then continued through the security hardening process. Upon completion of the installation of the system, it was run through an acceptance and readiness test to determine that each piece of equipment was functioning properly and that all networking and permissions were configured correctly.

Functional Testing of the system utilized a Multi Seat Ranked Choice Voting (RCV) Election utilizing 14 inch ballots printed on 100# card stock, a Presidential General Election utilizing 14 inch ballots printed on 100# card stock, a Special Recall Election on 22 inch ballots printed on 100# card stock, and several targeted test elections. The specific election definition databases used in testing were based on a fictitious RCV Election to elect four candidates consisting of 12 candidates and four write ins, the Presidential General Election, and the California Statewide Special Recall Election. The Presidential General and Special Recall Elections were configured using actual data that was exported from California counties election management systems (EMS) and/or voting systems.

The mock elections were conducted as if the system had just been purchased by a county. The ImageCast X Ballot Marking Device was utilized to duplicate ballots when needed. It was discovered that three ballots were damaged in printing, and were duplicated. The mock elections were conducted in an environment that simulated a small or medium sized county.

Ranked Choice Voting Election: The RCV Election was conducted utilizing one ballot style with one contest containing ten ranks of choices for twelve candidates and one write-in. The ImageCast X Ballot Marking Device was utilized to create five voted ballots, recreations of five of the original ballots, which were then placed in the deck of twenty three thousand ballots, replacing the originals. The test deck of 23,000 ballots was tabulated once for ten rounds of ranked choice voting. Polls were opened in accordance with California Use Procedures. Results were loaded into the EMS, and a simulated draw from a hat was utilized to advance through the ten rounds of RCV. In the test, the threshold was 16. The Interscan 821D HiPro scanner/HSS-ICC/EMS correctly identified all ten rounds of RCV. The results were tabulated correctly through ten rounds of RCV. Polls were closed in accordance with California Use Procedures, including printing all reports. Reports were generated printing contest rankings for each round of RCV.

The RCV Election was conducted by scanning ballots simultaneously on the Interscan 821D HiPro scanner, the previously certified Canon G1130 scanner, and the previously certified Canon X10 scanner. OVSTA scanned 16,878 ballots on the Interscan 821D HiPro scanner, 398 ballots on the Canon G1130 scanner, and 6,111 ballots on the Canon X10 scanner. Ballots were scanned in batch sizes from one to 1,044, and approximately 25% of the ballots in the face-up, header first orientation, 25% of the ballots in the face-up, foot first orientation, 25% in the face-down header first orientation, and about 25% in the face-down, foot first orientation. At the close of polls, the electronic files from the HSS-ICCs were brought into the Results-Tally-Reports (RTR) utility. Ballots containing an exception condition were resolved using adjudication. The results were matched against the expected results file supplied by Dominion. Finally, the Official Canvass Summary report and Statement of Votes Cast report were generated. Additionally, the Secretary of State Statement of Vote (SOV) and Supplemental Statement of Votes (SSOV) reports were generated.

The ballots utilized for the RCV Election constantly shed small slivers of paper from the edges. The slivers were approximately ½ inch long or shorter, and the ballots were badly contaminated with them. The slivers appeared to be a result of improperly trimming/cutting the ballots at the printer. The large nature of the paper dust caused repeated read errors on the Interscan 821D HiPro scanner. It was discovered that fanning the batches, then wiping the edges of the ballots, in conjunction with keeping the read heads clean on the Interscan 821D HiPro scanner greatly improved performance.

Special Recall Election: The Special Recall Election was comprised of one ballot style with one contest containing 155 candidates and one write-in. After replacing the arms on the Interscan 821D HiPro scanner with longer extensions to accommodate the 22 inch ballots, all ballots were scanned on the Interscan 821D HiPro scanner. Four blank

ballots and an incorrect ballot were placed at random in the batch. All incorrect or blank ballots were identified correctly. The 22 inch ballots scanned without error at a rate of 600 ballots in 6 minutes and 36 seconds. All ballots were tabulated correctly.

Post-election results were consolidated and reported based on upload of results to EMS from the HSS-ICC and Interscan 821D HiPro scanner. Results included generation of final reports and verifying canvass including the SOV and SSOV.

Presidential General Election: The Presidential General Election was utilized as a modified volume test for the Interscan 821D HiPro scanner. The ballots were the same ones used in the original volume test for the DS 5.2 system, but showed little fatigue. These ballots were relatively clean, and shed a small amount of dust. Working in a simulated small to mid-sized county environment, and at a casual pace, we scanned 20,000 ballots in 2 hours and 13 minutes.

Polls were closed in accordance with California Use Procedures. Post-election results were consolidated and reported based on upload of results to EMS. Results included generation of final reports including the SOV and SSOV.

Targeted Elections: Several elections were run to target specific areas of the Interscan 821D HiPro scanner and HSS-ICC. The first was a test of 1,000 12 inch ballots on 32# stock generated from the ImageCast X Ballot Marking Device. The ballots were scanned in landscape orientation and the system scanned them in 3 minutes and 34 seconds for an estimated hourly rate of 16,822.

The next test was for marginal marks. Ballots were marked manually with a black Sharpie pen, a yellow highlighter, a red pen, a black pen, and a pencil. Ballots were marked with X's, check marks, small dots, lines, and completely filled ovals. The ballot ovals were marked from 5% filled to 100% filled, as well as completely outside the oval. The Interscan 821D HiPro scanner was set for "red dropout" because the actual ballot ovals were red. As a result, the Interscan 821D HiPro scanner did not read the red pen which was the expected result. The Interscan 821D HiPro scanner read all other markers without error. In every case, the system sent the images to adjudication when necessary, and processed all the ballots correctly. The adjudication system appropriately identified all marks including the highlighter.

The next test simulated an all vote by mail election utilizing ballots from the 2016 Presidential Primary which were machine folded tri-fold ballots. The ballots were unfolded, flattened manually, and counter bent against the fold twice. Utilizing the two trays on the Interscan 821D HiPro scanner, ballots were continually loaded in stacks of approximately 125 ballots in the unused tray while the Interscan 821D HiPro scanner was scanning ballots from the other tray. The Interscan 821D HiPro scanner automatically switches from one tray to the other. In this fashion, 2,875 ballots were scanned, running continuously. One read error was experienced after scanning 1,963 ballots that was mitigated by opening the Interscan 821D HiPro scanner, wiping the read head with a feather duster, and continuing. No other errors or problems occurred.

The final test was a marginal ballot test. These ballots would most likely be duplicated in a real election. Ballots were folded diagonally, horizontally, and vertically at random. Just the corners and edges were folded on some ballots. Ballots were folded both singly, and up to ten ballots together. Two ballots were crumpled and then flattened. Ballots were loaded into the Interscan 821D HiPro scanner trays with folds going in both directions. After some initial jams and subsequent calibration changes, the Interscan 821D HiPro scanner read these ballots without error, however the rate of scanning dropped to a point that would not be acceptable for election purposes. Several pickup roller problems were experienced when the next ballot to be scanned was loaded with the folds in a different direction from the previous ballot, and the pickup rollers did not pull them into the Interscan 821D HiPro scanner. OVSTA recommends that ballots with this amount of wear and tear be duplicated, or scanned on the X10.

Additional Functional Testing

At Dominion's request, two additional days of functional testing were performed to optimize the Interscan 821D HiPro scanner for coated ballots printed on an inkjet printer. The pickup rollers and separation unit were replaced with rollers better suited for the glossy paper used in the inkjet printing process, and an extension was added to the feed tray. These modifications/parts are COTS parts available from Interscan 821D HiPro scanner. The parts replaced are as follows:

- Friction lining Green with Riffles part number e0073053
- Pre-input roller – e0083027
- Separation roller – e0073142
- Separation unit assembly (with backing plate)– f600120a

Ballots from two different counties were used to test the modification. The test ballots were examined and an expected results file was built. The ballots were scanned and the results reported and matched against the expected results. The Interscan 821D HiPro scanner performed as expected.

Functional Test Results

Test results showed that the modified voting system including the Interscan 821D HiPro scanner performed in a manner consistent with California Voting System Standards and all test cases were executed successfully and accurately.

Anomalies Identified During Functional Testing

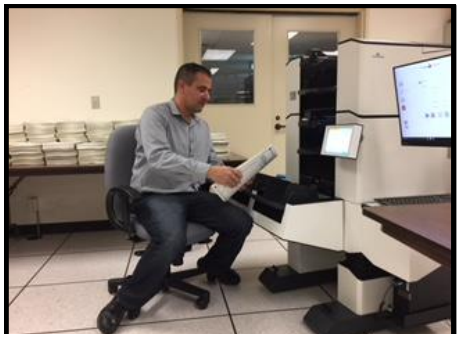
As identified above, one anomaly was identified during Functional Testing:

- The Interscan 821D HiPro scanner tended to experience read errors in the RCV Election. In every case, the read error was mitigated by wiping the inside of the Interscan 821D HiPro scanner with a duster. The provided ballots were cut in a way that generated a great deal of small slivers of paper that coated not only the inside of the Interscan 821D HiPro scanner, but the table the ballots were resting

on, and the operators using the Interscan 821D HiPro scanner. The amount of ballot dust from the printing process should be carefully monitored for ballots tabulated on this Interscan 821D HiPro scanner. Excessive ballot dust may slow the scanning process for the Interscan 821D HiPro scanner.

3. Accessibility Testing

The Interscan 821D HiPro scanner, while not a voter usable device, includes the ability to lower and raise in order to accommodate an elections office worker.



It was found that the Interscan 821D HiPro scanner is easily adaptable for sitting or standing elections workers. It was determined that the technologies implemented for accessibility and usability in the Interscan 821D HiPro scanner improved the experience for election workers that may be required to spend hours at a time operating the Interscan 821D HiPro scanner.

4. Security and Telecommunications Review

The Secretary of State contracted with SLI in Denver, Colorado to conduct the Security and Telecommunications Review. The Security Review took place at SLI's office between February and March, 2018.

Security and Telecommunications testing covered:

- Top-level system design and architecture.
- System documentation and procedures.
- Testing of relevant software and operating system configuration for pertinent vulnerabilities.
- Testing of hardware, including examination of unused hardware ports and security measures applied to those ports.
- Testing of system communications, including encryption of data as well as protocols and procedures for access authorization.

The testing was divided into three phases:

Phase I included review of all pertinent documents for appropriate processes and

procedures for implementing a secure system. This included a review of the system design and architecture.

Phase II included testing of relevant software, operating systems, and hardware configurations.

Phase Ill included testing of all telecommunications aspects of the system.

Phase I

During Phase I testing, review of the TDP validated that all requirements have been met.

Phase II

It was determined that because the Interscan 821D HiPro scanner/ HSS-ICC is a central count location implementation, several of the requirements were not applicable. The Interscan 821D HiPro scanner does not provide monitoring of physical security, however, as a central count implementation isolated from outside access, physical security of the Interscan 821D HiPro scanner would be mitigated procedurally by the jurisdiction implementing the device.

The Interscan 821D HiPro scanner currently acts as a USB 3.0 connected scanning device, which is not currently configured with access controls. The HSS-ICC system controls the Interscan 821D HiPro scanner via the direct attached USB connection. The HSS-ICC system contains required access control identification measures. The Interscan 821D HiPro scanner utilizes a Linux-based operating system that contains usernames and passwords that could be accessed in particular conditions. If properly configured, the Linux-based access controls would meet the requirements. The HSS-ICC computer runs on the Windows Operating System, which provides access control as expected.

Additionally, any auditing in relation to election results or ballots are produced from the HSS-ICC that is connected to the Interscan 821D HiPro scanner. The capability for logging is available on the Interscan 821D HiPro scanner but only for issues related to the Interscan 821D HiPro scanner itself. It is determined that the Interscan 821D HiPro scanner, being a commercial off the shelf (COTS) device, is functioning as intended.

All physical ports on the Interscan 821D HiPro scanner are accessible and not physically protected. This includes: one RS232 port, three audio 3.5mm jacks, three USB 2 ports, one USB 3.0, one HDMI port, and one RJ45 network port. It was discovered that the RJ45 network jack was not disabled and once the device was assigned a dynamic IP address from a Dynamic Host Configuration Protocol (DHCP) server, the network capability was fully functional. Once the device was connected to the network, Nessus Vulnerability scans were conducted against both the HSS-ICC scan system and the Interscan 821D HiPro scanner. It was determined during the vulnerability scan that there is an unencrypted Telnet server being served on TCP port 23. This server allows access to the Interscan 821D HiPro scanner operating system. Upon further investigation it was determined that the root account on the Interscan

821D HiPro scanner was unprotected by password and root access to the Interscan 821D HiPro scanner was achieved. While the Interscan 821D HiPro scanner isn't currently configured for network batch transmission, the Interscan 821D HiPro scanner is accessible. This could potentially lead to compromise of the Interscan 821D HiPro scanner and or access to scanned ballot images. Completion of the Nessus Vulnerability scan determined no further vulnerabilities associated with the Interscan 821D HiPro scanner.

Vulnerabilities were referred to Dominion Voting Systems for mitigation, and they provided the following response:

> The Interscan 821D HiPro scanner is a COTS device provided by a third party vendor and utilizes software, firmware, and hardware that are not accessible to Dominion Voting Systems for modification. The Interscan 821D HiPro scanner itself solely provides ballot images to the HSS-ICC application and does not perform any tabulation functions. This vulnerability can be mitigated by applying adhesive tamper-evident seals over the RJ45 Ethernet ports or any other unused ports as they are not required by the HSS-ICC system as part of the tabulator configuration. Additionally, Dominion has requested that the COTS supplier address these shortcomings of their hardware and firmware and we will seek approval for an updated version of the Interscan 821D HiPro scanner when the vendor provides a revised version.

Nessus® Vulnerability scans were conducted on all equipment that were connected to the private EMS network including the HSS-ICC system. Operating system level transmissions provided appropriate encryption, receipt validation, and data integrity. Protection against malware on the HSS-ICC computer is provided by the AVAST Antivirus File Shield. The real time anti-virus monitor was only able to detect and clean one of the four European Institute for Computer Antivirus Research (EICAR) files, which potentially leaves the system open to zipped and double zipped viruses as well as infection strings in plain text.

Vulnerabilities were referred to Dominion Voting Systems for mitigation, and they provided the following response:

> The HSS-ICC system specifies the use of Windows Defender with the latest virus definitions in its system documentation. Additionally, CA conditions of use for the DemSuite 5.2 system certification require that an “air gap” be maintained between the central count system and public networks and that all removable media introduced to the system first be formatted and scanned utilizing a dedicated and physically separate/disconnected workstation specifically configured solely for this purpose.

The system was tested to verify that the installation process for each system component is robust and maintains the integrity of the voting system. It was discovered that Dominion specifies what is required to complete software validation but does not

specifically supply the required software or hardware to do so. SLI was able to replace digitally signed application installers with renamed executables without the installation package failing. SLI was able to modify election specific installers utilizing a hex editor to change minor things including mouse over text and digital signature names. SLI was able to take installers from previous versions of the installation package and use them to install older versions of the software from the DemSuite Installation. SLI believes it would be possible to inject more lethal payloads into the installers given the opportunity. Further, it was discovered that system logs did not provide entries that dealt with a failed or successful installation of software.

Vulnerabilities were referred to Dominion Voting Systems for mitigation, and they provided the following response:

> Dominion specifies that third-party software be downloaded from a trusted source in order to verify the installed software hashes. It is Dominion's belief that utilizing third-party software improves the proof that the hashes are genuine and that using a vendor-supplied tool would essentially result in a self-check of little value to end users of the product. Additionally, the HSS-ICC system specifies hash validation of installed software and does not provide verification methods prior to software installation.

Telecommunications data integrity was determined to be not applicable. Individual public facing voting components are not networked nor do they transmit individual voting results. The only telecommunications that are in use are an isolated closed network to link the EMS/Adjudication/HSS-ICC devices together at a central count location. This requirement is also not applicable to the Interscan 821D HiPro scanner.

Phase III

It was determined that while the Interscan 821D HiPro scanner does have network capabilities there are no wireless transmission devices present.

5. Source Code Review

Source Code Review was conducted at SLI in Denver, Colorado between February and March, 2018.

The source code was delivered to SLI by Dominion Voting Systems prior to testing starting. The modified DemSuite 5.2 system required testing of 5,129 new lines of code and 9,246 lines of modified code for the HSS-ICC /Interscan 821D HiPro scanner.

Three potential vulnerabilities were found within the HSS-ICC source code base:

One potential vulnerability was noted when the HSS-ICC source code was analyzed for its ability to appropriately accommodate error and exception handling. Exploitation of the vulnerability would require access by a Vendor Insider with extensive knowledge of the voting technology design and configuration.

Vulnerabilities were referred to Dominion Voting Systems for mitigation, and they provided the following response:

> As noted by the reviewer, exploitation of this vulnerability would require access by a vendor insider with extensive knowledge of the voting technology design and configuration. As a central scan product typically used in a secure central office with controlled access, the ability of a vendor insider-initiated attack is extremely remote. Exception handling issues generally result in application lockups or crashes rather than exposing potential security attack vectors. No unhandled exception states in the HSS-ICC application were noted during functional and operational testing.

One potential vulnerability was noted when the HSS-ICC source code was evaluated for the likelihood of security failures being detected, and whether data that might be subject to tampering is properly validated and authenticated. Exploitation of the vulnerability would require access by a Vendor Insider with extensive knowledge of the voting technology design and configuration.

Vulnerabilities were referred to Dominion Voting Systems for mitigation, and they provided the following response:

> As noted by the reviewer, exploitation of this vulnerability would require access by a vendor insider with extensive knowledge of the voting technology design and configuration. As a central scan product typically used in a secure central office with controlled access, the ability of a vendor insider-initiated attack is extremely remote. Data passed between functions within the system is generally not able to be manipulated in an exploitable way without modification of the application's source code.

One potential vulnerability was noted when the HSS-ICC source code was evaluated for design and implementation to ensure that sound, generally accepted engineering practices are followed, checking to verify that code is defensively written against bad data, errors in other modules, changes in environment, user errors, and other adverse conditions. Exploitation of the vulnerability would require access by a Vendor Insider with extensive knowledge of the voting technology design and configuration.

Vulnerabilities were referred to Dominion Voting Systems for mitigation, and they provided the following response:

> As noted by the reviewer, exploitation of this vulnerability would require access by a vendor insider with extensive knowledge of the voting technology design and configuration. As a central scan product typically used in a secure central office with controlled access, the ability of a vendor insider-initiated attack is extremely remote. Defensive coding practices are generally used to enhance application stability and are not

typically exploitable as security vulnerabilities. In this instance, we believe the reviewer is noting the same discrepancy described above related to data passed internally within the application. No application stability issues were noted during functional and operational testing.

IV. CONCLUSION

The modification to the Dominion DemSuite 5.2 voting system, in the configuration tested and documented by the Installation and Use Procedures, does not impair its accuracy and efficiency.

Should the modification be approved, it is recommended that the unsecured network port, as well as any unsecured ports on the Interscan 821D HiPro scanner be covered by a seal or a permanent metal cover.

Additionally, it is recommended that the Interscan 821D HiPro Linux-based access controls be properly configured to meet the requirements.