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
DEMOCRACY SUITE 5.10

System Components
Election Management System: Software version 5.10.11.24
ImageCast Evolution: Software version 5.10.9.3
ImageCast Central: Software version 5.10.0.1002
ImageCast X: Software version 5.10.11.11
Adjudication: Software version 5.10.10.1
ImageCast Precinct 2: Software version 5.10.3.6
Mobile Ballot Production: Software version 5.10.11.24
ImageCast Voter Activation: Software version 5.10.11.24

Staff Report

Prepared by:
Secretary of State's Office of
Voting Systems Technology Assessment
August 19, 2019

Table of Contents

I. INTRODUCTION

1. Scope

This report presents the test results for the four phases of the certification test campaign of the Dominion Voting Systems Democracy Suite (DS) 5.10 voting system. The purpose of testing is to test the compliance of the voting system with California Voting Systems Standards, and State & 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

Dominion submitted an application for the DS 5.10 voting system, which is comprised of the following major software components:

- Election Management System: Software version 5.10.10.1
- ImageCast Evolution: Software version 5.10.8.1
- ImageCast Central: Software version 5.10.0.1002
- ImageCast X: Software version 5.10.10.1
- ImageCast Precinct 2: Software version 5.10.1.2
- Adjudication: Software version 5.10.10.1
- Mobile Ballot Production: Software version 5.10.11.24
- ImageCast Voter Activation: Software version 5.10.11.24

In addition to the software, which includes the executable code and the source code, Dominion was required to submit the following:

- The technical documentation package (TDP);
- All the hardware components to field two complete working versions of the system, including all peripheral devices, one for the Functional Test Phase and one for the Security Test Phase;
- Twenty ImageCast Evolution voting machines, fifteen ballot boxes and all the peripherals that would be in the polling place;
- Twenty ImageCast X ballot marking machines and all the peripherals that would be in the polling place;
- Fifty ImageCast Precinct 2 ballot marking machines and all the peripherals that would be in the polling place; and
- The California Use Procedures.

3. Contracting and Outsourcing

Upon receipt of a complete application, and an initial examination of the system and technical documentation provided by Dominion to ensure all components and documentation necessary to complete testing had been submitted, the Secretary of State released a Request for Proposal (RFP) for the Trusted Build compile, Functional Testing including Physical and Functional Configuration Audits, Hardware Testing, Accessibility Testing, Volume Testing, and Security Review including Source Code and Security Testing.

Through the formal California contracting process, the Secretary of State awarded a contract to SLI Compliance (SLI).

II. SUMMARY OF THE SYSTEM

The DS 5.10 computers represented in this system are all current operating systems that were patched current at the time of the installations. Currently, Microsoft is scheduling Extended Support for Windows 10 until October 14, 2025. Microsoft is currently scheduling Extended Support for Server 2016 until January 1, 2027.

The network protocol is Transmission Control Protocol/Internet Protocol (TCP/IP) using Dynamic Host Configuration Protocol (DHCP) for addressing. The DHCP service runs on both Election Event Designer (EED) and Results Tally Reporting (RTR) servers. Domain Name Service (DNS) is used for address resolution, and runs on both servers as well. Unused ports are closed on all machines, and services that are not needed are disabled. The system is setup in a client server configuration, with all election data stored on the servers. This facilitates backups, and the server drives are encrypted. The Election Management System (EMS) and RTR servers utilize Dell Self Encrypting Drive (SED) Technology. These drives are provisioned with a key at installation time, and the EMS database files are stored under the encrypted disk drives. The encryption platform utilizes a National Institute of Standards and Technology (NIST) certified hardware-based cryptographic engine which provides real-time encryption and decryption of data using AES-256 algorithms. In addition, the encrypted storage platforms provide the access control through using iButton security keys.

The default storage configuration on the servers is two drives in a RAID 1 (Disk Mirroring) configuration for the operating system, and four drives in a RAID 10 (mirroring and striping) configuration for data storage.

The system does not include modems, or telecommunications devices, and there is no provision for accessing external networks. No failover/redundant configuration was tested, however, the servers each run both EED and RTR providing redundancy.

The Democracy Suite 5.10 voting system consists of eight major components.

1. Election Management System (EMS), v. 5.10.10.1

EMS is a set of the following applications that are responsible for pre-voting and post-voting activities, including ballot layout, generation of audio files, programming media for voting equipment, importing results data, accumulating and reporting results.

a) EMS-Election Data Translator (EDT), v. 5.10.11.24
EDT is an application that imports and exports election data, such as districts, precincts, contests, candidates, translations, etc., to and from the election project (a.k.a. election definition).

b) EMS-Election Event Designer (EED), v. 5.10.11.24
EED is an application that handles the majority of the pre-voting activities. EED is the application that receives the imported data from EDT and Audio Studio in order to generate ballot structure, ballot artwork, and tabulator files, including all the audio for an accessible voting session on the precinct tabulators.

c) EMS-Audio Studio, v. 5.10.11.24
Audio Studio is an application that assists jurisdictions with the creation of audio files. It can be used to verify, listen and record audio files in EED.

d) EMS-Results Tally Reporting (RTR), v. 5.10.11.24
RTR is the main application for post-voting activities. It receives election results from the tabulators, allows for validation of the results, and reports the results. RTR can be used for the addition, and deletion of tabulator files. It also allows for manual resolution of qualified write-ins.

e) EMS-File System Service, v. 5.10.11.24
File System Service is a stand-alone service running on client machines enabling access to low level operating system application programming interface (API) for portioning compact flash (CF) cards.

f) EMS-Data Center Manager, v. 5.10.10.1
Data Center Manager is a system-level configuration application used in EMS back-end data center configuration.

g) EMS-Application Server, v. 5.10.11.24
Application Server is a server side application responsible for executing long running processes, such as rendering ballots, generating audio files and election files.

h) EMS-Adjudication Service, v. 5.10.10.1
EMS-Adjudication Service is a software service that provides EMS data to the Adjudication Services application.

i) EMS-Smart Card Helper Service v. 5.10.11.24

EMS-Smart Card Helper Service is a software service that provides the connection to the smart card reader to allow you to program technician, poll worker, and voter cards.

j) EMS-ImageCast Voter Activation v. 5.10.11.24
EMS-ImageCast Voter Activation is a software service that allows you to activate voter cards.

2. ImageCast Evolution (ICE), v. 5.10.8.1

ICE is an all-in-one precinct optical scan tabulator and ballot marking device. The ICE can accept pre-marked ballots, give voters a second-chance notification on ballot errors, and provide a final ballot review based on the machines interpretation of the hand-marked ballot. The software prevents the scanning and tabulating of a vote with a marginal mark based on thresholds set in EED. The ballot marking capabilities allow a voter to place a blank ballot into the machine and vote using the accessible tactile interface (ATI), sip-n-puff, or paddle switches. When the ballot marking capabilities are turned on the voter also has the capability to use the audio features. The version submitted for California has the audio capability to handle any of the ten languages required by the U.S. Department of Justice (English, Spanish, Chinese, Japanese, Tagalog, Korean, Vietnamese, Thai, Hindi, and Khmer).

3. ImageCast X (ICX), v. 5.10.10.1

The ICX was tested in two versions: The Avalue-21 Classic and the Avalue 21 Prime. ICX is an accessible ballot marking device. The ballot marking capabilities allow a voter to vote using the accessible tactile interface (ATI), sip-n-puff, or paddle switches. The version submitted for California has the audio capability to handle any of the ten languages required by the U.S. Department of Justice (English, Spanish, Chinese, Japanese, Tagalog, Korean, Vietnamese, Thai, Hindi, and Khmer). The ICX requires the voter to insert an activation card which is generated by a poll worker. The activation card can be created with accessible options enabled so that the voter is presented with all of the accessible options when the voting session is initiated.

4. ImageCast Central (ICC), v. 5.10.0.1002

ICC uses commercial-off-the-shelf (COTS) Canon DR-X10C, Canon DR-G1130, Canon DR-G2140, and Interscan HiPro scanners at the central tabulation location to scan vote by mail ballots and post-voting ballots, such as provisional ballots, vote by mail ballots not delivered until Election Day, ballots that need to be duplicated, and ballots that were scanned into a multi-precinct ICE tabulator. The results from batches scanned through the ICC are dropped into a folder on the server for the Adjudication Client to access.

5. Adjudication Client, v. 5.10.10.1

Adjudication Client is an application that allows the jurisdiction to resolve a ballot on screen that would normally be outstacked to be remade or hand counted because it had

one or more exception conditions, such as write-ins, over-votes, marginal marks, under-votes, or because it is a completely blank ballot. The Adjudication Client has two roles, Administration and Ballot Inspection. The functionality of the Administration role is to configure user accounts, exception reasons (e.g. write-ins and over-votes), batch management, and report generation. In the California configuration, the Administration role must be performed directly on the server. Ballot Inspection allows users to review ballots that have at least one exception condition as defined by the Administration role. The user may accept the ballot as is or resolve the ballot pursuant to California law. Each ballot that is adjudicated is stamped with the username of the user who made the change.

6. ImageCast Precinct 2, v. 5.10.1.2

The ImageCast Precinct 2 (ICP2) device is a precinct-level, optical scan ballot counter designed to provide two major functionalities: ballot scanning and tabulation, and ballot review and second chance voting. The ballot review feature allows voters to review their selections and change any votes by remarking the ballot. Once a paper ballot is processed, the voting results for a given ballot are displayed on the monitor for verification. The results are presented in text format, which allows voters to identify any voting errors they may have made and to verify that the tabulator has correctly identified the selections.

7. Mobile Ballot Production, v. 5.10.11.24

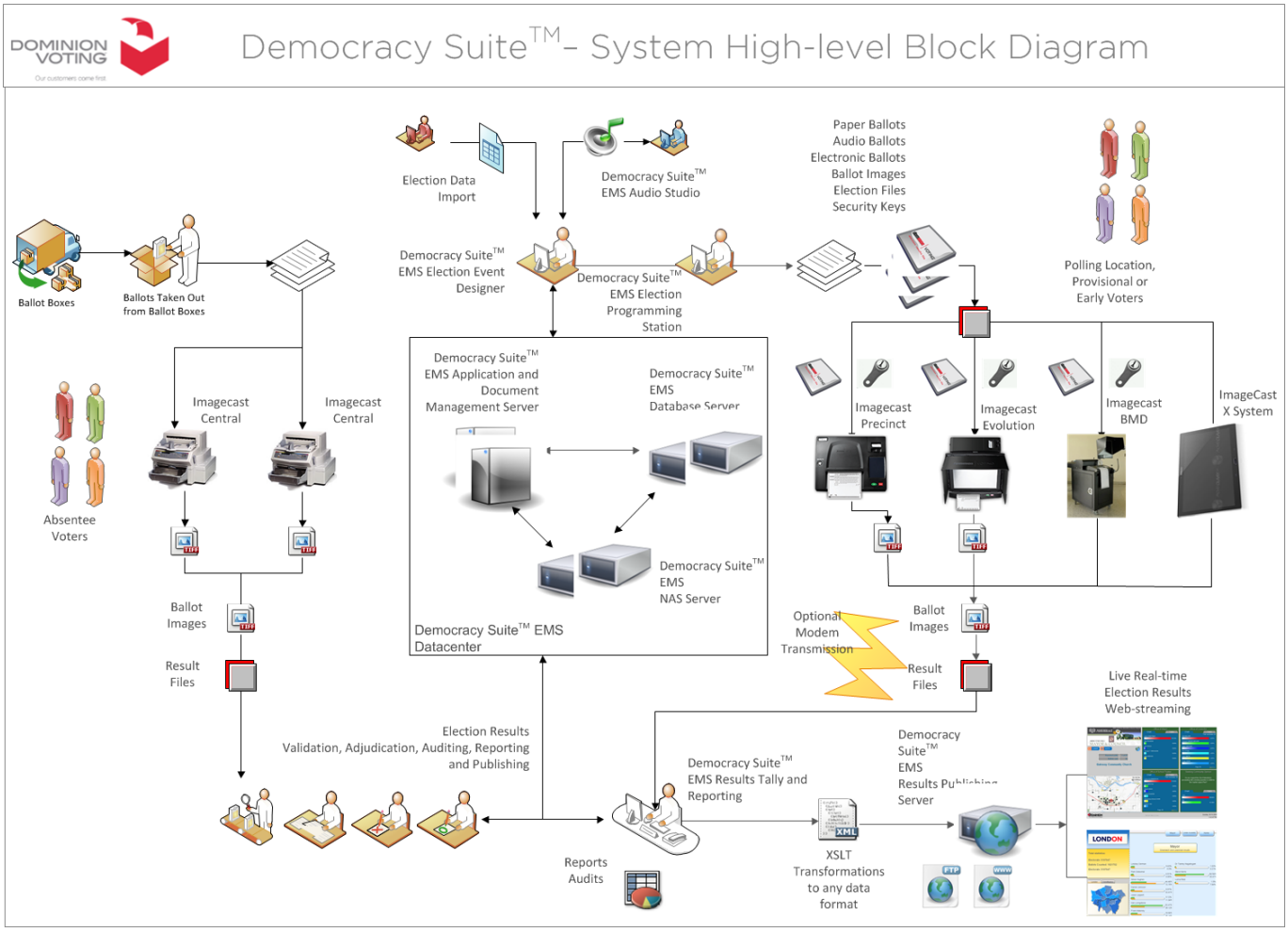
The Mobile Ballot Production (MBP) 5.10.11.24 system is an on-demand ballot printing system consisting of a Dell Latitude 3490 laptop, OKI C712, and OKI C931 printers.

The MBP 5.10.11.24 system operates in conjunction with the Democracy Suite 5.10 voting system. The DS 5.10 EMS creates MBP ready ballot images in .PDF format complete with tint and watermark. These ballot images are exported to the MBP laptop, and then printed on blank paper. To identify the correct ballot style, the MBP system can sort by precinct, ballot group, and several other data points. Once setup and configuration is complete, the MBP laptop only contains geopolitical information, and does not contain any voter information. The MBP system will generate many different reports, including total number of ballots printed, and number of each ballot style printed. The reports can be generated in Excel, Word, and PDF formats.

8. ImageCast Voter Activation, v. 5.10.11.24

The ImageCast Voter Activation (ICVA) 5.10.11.24 application is a polling place/vote center location tool that allows poll workers to program smart cards for voters in order to activate voting sessions on ImageCast X. Voter Activation cards can be created in either standard or accessible modes. The ICVA consists of the application, Dell Latitude 3490 laptop and USB Smart Card reader/writer.

High Level Block Diagram



III. TESTING INFORMATION AND RESULTS

1. Background

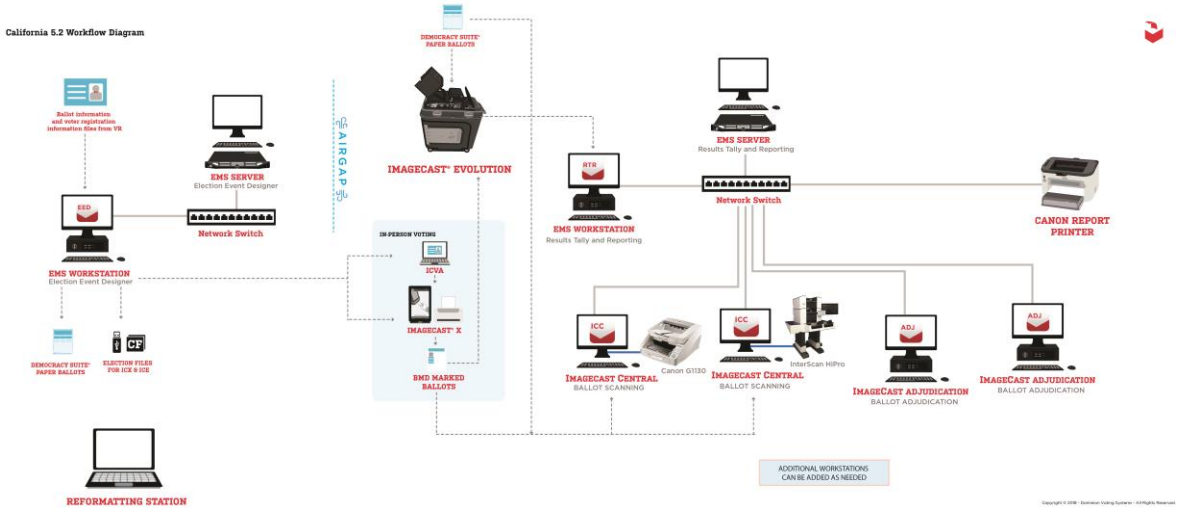
Dominion submitted an application to the Secretary of State for certification of the DS 5.10 voting system on October 24, 2018.

California certification testing of the DS 5.10 voting system began in April 2019. The testing began with the build and compile of the Trusted Build, followed by Source Code Review, followed by all phases of Functional Testing, Security Review, and finally Volume and Accessibility Testing.

The test lab was configured in a real world environment simulating an actual voting system in use by a California County. The Vote Center/Polling Place was setup with the Voter Activation Card Laptop, ICX machines, and ICE machines. EED and RTR were setup as per the logical map below. Strict adherence to the air-gap architecture was

maintained throughout testing. Media of any kind was only allowed to go from EED to RTR, and was then cleaned, reformatted and returned to the test.

Functional Testing Configuration



The Secretary of State performed the Trusted Build phase of testing on April 8-10, 2019. Due to a software change by Dominion, all the machines were wiped, and the software recompiled on May 16 and 17.

The Trusted Build was accomplished by SLI Staff, and California Secretary of State Staff. The trusted build software and firmware was completed for the EMS, ICE, ICX, ICR, and ICP2. The compiles were accomplished per the Dominion manuals for each product. Utilizing VMWare Player, a virtual machine (VM) was created, followed by operating system installation of Windows or Ubuntu depending on the product, compiler installation, and then resources were copied to the virtual machines. The products were then compiled. Snapshots were taken of the VMs at various milestone stages of the build, and were saved as artifacts. The trusted build creation documents (refer to the Overall Test Plan for document names) were amended as necessary, and Dominion provided the final versions.

The Secretary of State contracted with SLI to conduct the Functional Testing, Physical Configuration Audit, and Functional Configuration Audits. This testing took place at the Secretary of State's Test Lab between April 29 and May 7.

2. Functional Testing Summary

The Functional Test of the Dominion DS 5.10 voting system was conducted by Office of Voting Systems Technology Assessment and SLI staff at the Secretary of State's Office located at 1500 11th Street, Sacramento, California from April 29, 2019, through June 15, 2019.

The Secretary of State ran the Functional Test as if it were a jurisdiction that just purchased the voting system. Testing of the system began by setting up all equipment in a configuration that mirrored a production voting system. The DS5.10 architecture allows elections officials to use one or more, permanent server(s) and set of central-office voting devices, known to be running unaltered, certified software and firmware to create memory cards before each election and to use another, physically separate "sacrificial" server and set of voting devices after the election to tabulate results and generate reports. To transfer election specific data, the ICP2 machines utilize SD cards, the ICC and ICE machines utilize CF cards, and the ICX utilizes USB sticks. The election specific data (files) transferred on these cards are encrypted. An iButton is required to unencrypt the SD and CF cards for the ICP2, ICC, and ICE, and a smartcard is needed to unencrypt the USB sticks used to transfer data to the ICX machines. The key used for these devices can be unified or not. A unified key is one that is election specific. A key specific to that iButton (polling place specific) can be used also. This would prevent a malicious actor from accessing the entire system with just one key.

Next, all COTS computers were wiped with DBAN in order to clean the existing software from them and begin with hardware with absolutely no software installed. The hardware consisted of two Dell PowerEdge R640 servers (EMS & RTR Server), two Dell Tower 3430 (Clients), three Dell Optiplex 3050 All in Ones (ICCs) with touch screen, Dell 7060 (ICC High Speed Scanner), two Dell Latitude 3490 laptops (Voter Activation Card & EED Cleaner). Following the California Use Procedures, the testing began with the installation of the operating system, commercial-off-the-shelf software, voting system trusted build software, and then continued through the security hardening process. Then the firmware was installed on the ICX, ICE, and ICP2 machines. The ICX machines were installed with Android 8.1, and the "new" option was utilized to wipe the lifetime counter on the machines.

Windows Defender was installed and patched on all EED and RTR systems Windows based computers. The ICX voting machines running Android do not have anti-virus installed. The ICE and ICP2 machines run firmware without an operating system.

After the Installations, SLI performed the Physical Configuration Audit (PCA) and took HASHes of the "Trusted Build" installations in order to accomplish validations of the installations at a later date.

Functional Testing of the system included an auto generated Logic and Accuracy (L&A) election using software provided by Dominion, a simple pick two of three election built from scratch, and five main election types: a Presidential Primary, a Presidential General, a Special Recall, a Ranked Choice Voting (RCV), and a Vote Center Election. The test deck ballots were created using the following general rules:

- Per California Elections Code (EC) 13002, ballots are printed with a watermark and tint from the approved list for California;
- Pursuant to the requirements of EC 13203, ballots are clearly labeled as TEST BALLOTS instead of OFFICIAL

BALLOTS;

- Ballots contain Instructions to Voters per EC 13204 and 13205, but may also include instructions at the bottom of the ballot per EC 13231;
- Candidates are listed per EC 13103;
- Candidate's political party are listed per EC 13105;
- Per EC 13107, each candidate is to have an occupation listed under the candidate's name. For economy of testing, the following 'occupation' was used for all candidates: Occupation Prints Here - la ocupacion demuestra aqui; and
- Translated ballots for a character-based language contain the phonetic transliterations of the alphabet-based names of candidates.

The test elections were conducted as if the system had just been purchased by a county. Ballots were supplied by Dominion pre-printed by a printer. Polls were opened and voting at the precincts/vote centers simulating both early voting for a vote center, and election day voting were accomplished using the ICE, ICP2, and ICX. At the close of polls, the memory cards from the ICE voting machines and the ICX voting machines were brought into RTR. Ballots containing an exception condition were resolved using adjudication. When the polls closed the results from the ICE voting machines, and the cast vote records from the ICX's, were tabulated, validated and published. After all ballots were tabulated, 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. Note that the above description was followed for all test elections, however, the Recall, Ranked Choice Voting, and Vote Center Elections were also used to test specific items, such as ballot layout rules and laws, scanner read-head tests to determine the consistency and accuracy of different types of marks using different marking devices simulating actual voters who vote by mail, language tests to determine if the system can populate all fonts used in California correctly and accurately, as well as the capability of the system to operate in a vote center environment that may constitute many more voters both for early voting and on election day. All test elections were evaluated for airgap compliance, with a "cleaner" laptop used to wipe, reformat, and scan all media for malware prior to being re-introduced into the EED environment again.

The L&A test election were completed in order to evaluate the system. Ballots for a Recall Election were generated utilizing Dominion's L&A auto test deck generating software. Twenty ballots were removed from the test deck, and remade on the ICXs, 10 each on ICX Prime and ICX Classic, utilizing standard voter activation cards. The ICX ballots were scanned in the following amounts: five on the ICE, five on the ICP2, and 10 on the Interscan HiPro Scanner. It was noted that the ICX ballots are tabulated by the QR code, and not the human readable portion of the ballot. Fifty ballots were scanned on ICE, and 50 on ICP2. The rest of the ballots were scanned in equal numbers on all ICC scanners. Polls were closed, all results were merged into RTR, and all reports were generated and saved.

The Recall Election was conducted after the L&A, simulating a county that has done an L&A, and then moves the machines to the polling places and conducts the actual election.

Recall Election: The Special Recall was conducted in English, Khmer, Japanese, and Hindi. The election consisted of one precinct and one contest. The contest included 135 choices with one write-in in a gubernatorial contest. The election was printed on twenty two inch ballots, which are the longest ballot size possible for the system. It was verified that the ICP2, and ICE run the election data from cards in the machine and the firmware is installed on an internal drive. The ICX machine stores the election data in a sandboxed partition in the internal hard drive of the machine. During the recall election, activation card functionality was tested. The ICVA was utilized to create all three types of cards: poll worker, technician, and voter. All three types of cards were tested without incident. Both accessible access and regular voter cards were created and utilized throughout all elections without error.

Twenty ballots were marked on the ICX Classic. Four voter activation cards were created for accessible sessions, and used to exercise each language. The ATI worked as expected, and the headphones worked as expected. Text size, contrast, security screen, and language options worked as expected. Ballots appeared to print in the correct language. A Poll worker card was used to vote 10 ballots and worked as expected. The ability to back out of a session (fleeing voter) was verified, and the card had to be reinserted to start another session. Ten of these ballots were scanned on an ICE and ten on ICP2. Ballots were fed in all orientations and the scanners performed as expected.

Twenty ballots were marked on ICX Prime. Four voter activation cards were created for accessible sessions, and used to exercise each language. The ATI worked as expected, and the headphones worked as expected. Text size, contrast, security screen, and language options worked as expected. Ballots appeared to print in the correct language. A Poll worker card was used to vote ten ballots and worked as expected. The ability to back out of a session (fleeing voter) was tested, and the card had to be reinserted to start another session. Ten of the ballots were scanned on ICE and ten on ICP2. Ballots were fed in all orientations and the scanners performed as expected. The Interscan HiPro Scanner was utilized to scan 512 ballots. The Auto Accept feature of the HiPro was verified, and the HiPro accepted each batch and moved to the other tray automatically. One ballot was fatigued and jammed in the HiPro. The ballot was flipped and scanned as expected.

During scanning, it was determined that one ballot from the printer did not print on the back of the ballot. It was only one sided without any printing on one side. The ballot was spoiled and replaced by a ballot printed on the Mobile Ballot Production device, and scanning continued. The ballot scanned as expected.

Polls were closed in accordance with California Use Procedures, including printing results from ICE and ICP2. The results media were utilized to transfer results back to RTR. Post-Election results were consolidated and reported based on upload of results

to RTR from all tabulating (ICE, ICP2, and ICC) units. Results included reconciliation of write-ins as well as generation of final reports and verifying Canvass – SOV, SSOV, Precinct results, over-votes, and under-votes. Backups were taken as if the files would be supplied to the California Secretary of State to meet the "Vote Count" program requirement prior to an election.

Presidential General Election: The Presidential General Election was tested in English, Korean, Chinese, and Vietnamese. One tri-lingual ballot style was included consisting of English, Chinese, and Vietnamese. The election included two ballot measures. The ICX, ICE, ICP2, and ICCs were programmed to support the entire election in all four languages. The election included ten precincts, 18 contests, and 45 options, with two write-ins. The candidates were rotated per EC 13111. The order of offices on the ballot were per EC 13109. Per EC 13105, each partisan candidate had the party affiliation listed to the right of their name. This election was printed on twelve inch ballots which are the smallest ballot size possible and included two cards.

During the process of installing the election on the ICX machines, it was noted that the USB sticks inserted into the ICX throw an error when inserted and this error must be cleared by the poll worker. USB ports are also whitelisted for certified models (Centon DataStickPro 8GB &16GB) and will not work for any other brand of USB stick.

Polls were opened and zero tapes were printed. All ballots were scanned, tabulated, and aggregated in RTR, and after the results were evaluated, the expected results did not match the actual count. A clear pattern of error was identified, and this eventually led to the error being attributed to the Auto Test Deck generation software used by Dominion to generate the test decks. The software did not correctly build the two card General ballots. A thorough check of the test decks determined that the Vote Center Election test deck was not complete. The ballots from both elections were re-printed, and the new Presidential General ballots were tested as follows:

Twelve ballots (24 cards) were marked on ICX Prime, and twelve on ICX Standard, utilizing six each of Voter Activation and Poll Worker cards. Two voter activation cards were created for accessible sessions, and used to exercise each language. The ATI, headphones, text size, contrast, security screen, and language options worked as expected. Ballots appeared to print in the correct language. The ability to back out of a session (fleeing voter) was tested, and the card had to be reinserted to start another session. Twelve ballots were tabulated on ICE and twelve on ICP2. Ballots were fed in all orientations and the scanners performed as expected.

ImageCast Remote was used to generate 25 cast vote records. These were duplicated on an ICX, and by hand, and then scanned on all scanners to verify compatibility. ICR cast vote records, and ICX ballots consist of a QR code containing results, and a human readable portion. The QR code is encrypted. There is no way to verify that what is in the QR code matches what is in the human readable portion of the cast vote record/ballot without scanning on an ImageCast device. All the ICCs scanned these remade ballots as expected.

Ballots were scanned on all four ICCs. The Canon 2140 experienced communications errors, and was eventually replaced with a new unit, which operated as expected. The HiPro ICC threw an error, and it was determined it had not been rebooted after the change of elections. It was rebooted and all scanners operated as expected.

Polls were closed in accordance with California Use Procedures. At this time it was noted that the ballot counter on the ICP2 display reads ballots, but actually displays the number of cards. All results were uploaded to RTR from ICE, ICP2, and ICC units. Results were printed from ICE and ICP2, and results media were used to transfer results back to RTR. Post-Election results were consolidated from the ICCs. Results included generation of all reports and verifying canvass – SOV, SSOV, precinct results, over-votes, and under-votes. Backups were taken as if the files would be supplied to the California Secretary of State to meet the "Vote Count" program requirement prior to an election.

Simple Pick Two of Three Election: The Simple Pick Two of Three Test Election was created from scratch on EED per the California Use Procedures, and the ballots were printed on Mobile Ballot Production. The ballots were marked by hand, and an expected results spreadsheet was generated from the ballots. The ballots were scanned on all scanners in equal numbers, aggregated into RTR, and the results matched the expected results spreadsheet with no errors.

Vote Center Election (Maximum Ballot Styles): The Vote Center Election was a fictitious election including five contests, ten choices, and 3000 precincts. The Vote Center Election was tested in English on twelve inch ballots. As a system test of label capacity, one candidate was created as candidate Last Name starting with the character 'L' and extending with 29 digits as indicated below. The First Name starting with the character 'F' and extending with 19 digits: "F12345678901234567890". Last name was: "L123456789012345678901234567890". The Vote Center Election ballots were machine pre-folded, and unfolded by hand.

Loading the election took approximately 15 minutes for each device. Polls were opened in accordance with California Use Procedures. Zero reports for all devices were printed and verified. The ICE, ICP2, ICX prime, ICX Classic, all performed as expected with three thousand precincts. It was noted at this time that the Mobile Ballot Production performed as expected with 3000 precincts, however the OKI C712 printer needed some adjustment to print the twelve inch ballots duplex without error. It was noted that the OKI C712 printer should be manually duplexed for ballots over nineteen inches in length.

Twenty ballots were printed on Mobile Ballot Production per the pattern which consisted of every 150th ballot throughout the entire 3000 precincts, which generated 20 ballots across the entire number of precincts. The ballots were hand marked, and expected results generated. All 20 ballots were tabulated on an ICE, and then all 20 on an ICP2. All 20 were remade and marked on an ICX Prime, and then all 20 on an ICX Classic. The remade ballots/cast vote records were scanned and tabulated on an ICE machine, and then on an ICP2. The ICP2, ICX, and ICE machines were suspended several times and re-enabled to simulate early voting at a vote center. It was discovered there were

no instructions in the California Use Procedures to suspend these machines. These procedures were added, and testing continued. The entire test deck was then scanned through each ICC machine. Results were as expected.

A marginal marks test was accomplished at this time. The adjudication workstation was configured to check for every option, and ICE and ICP were configured to test for all error conditions. Eight ballots were marked by hand with marginal marks. Pens, pencils, and highlighters of various colors were used to mark these ballots, and then the ballots were labeled one through eight in order to compare the scans. The system had red-drop-out enabled because the test election ballots were printed using red ovals. Ballots were fed face up and header first, through every scanner and the results were compared. The yellow highlighter, pink highlighter, and red were not picked up by the system. The ICE and ICP2 interpreted the results slightly differently, rejecting ballots for different marginal marks. All other marks were interpreted as expected, with marks outside the oval not picked up, and marks inside the ovals were. The Canon 2140 interpreted a ballot with a red pen mark as a vote, but the other three ICCs interpreted it as a blank ballot. Black ovals may be advisable for this system. All scanners interpreted marks slightly outside the oval, ovals marked with an X, very small dot shaped marks, and all other marginal marks as expected. The Auditmark maintains a forensic record of everything that has happened to the ballot image. The Auditmark on the ballot image will automatically mark the ballot with ballot type and ID if the jurisdiction did not print style on the ballot. New is the quarantine feature where a marginal ballot can be quarantined for additional evaluation. The Auditmark/ballot image is a TIFF file with front page, back page, and Auditmark that is always together. The Auditmark now includes the scanner that the ballot was scanned on. The adjudication information is added to the Auditmark.

Polls were closed in accordance with California Use Procedures, including printing results from ICE and ICP2. Results media were removed and used to transfer results back to RTR. Post-Election results were consolidated and reported based on upload of results to RTR from all tabulating (ICE, ICP2, and ICC) units. Results included reconciliation of write-ins as well as generation of all final reports. Backups were run and executed as expected.

Primary Election: The Presidential Primary was tested in English and Spanish. The election included 10 precincts and eight party splits per precinct. It included 20 contests and 65 choices. Ballots included one bi-lingual ballot style consisting of English and Spanish. The ICEs, ICP2s, ICXs, and MBP were programmed to support the entire election in English and Spanish. Ballots were seventeen inch which is the medium size possible for the system, and double sided.

Polls were opened and zero tapes printed. The ICX Prime and Classic devices were utilized to mark ballots in English and Spanish, including changing from English to Spanish midway through the ballot being voted. The ICX correctly printed the ballot in whatever language was chosen last. Text size and contrast were verified to meet expected criteria. The ability of the ICX to return from the review screen to alleviate any problems, including activation cancellation (fleeing voters) was verified. Ballots in English and Spanish were scanned on the ICE, ICP2, and ICCs without problem.

Mobile Ballot Production was used to print ten ballots in each language, and the results were as expected. Two ballots from each party were scanned on an ICE, and two on ICP2 (Precinct 13102). One ballot from each party was marked on ICX Prime and One from each party on an ICX Classic. During this test, an ICX Classic froze after touching "print ballot" the ballot printed about 60 seconds later with a bar code, but no human readable portion. The screen read "Unfortunately, Something went wrong". We hit continue, but it did not clear the error. This ICX Classic incremented the counter, and the ballot had a QR code (which included votes), but no human readable portion. A poll worker would have spoiled this ballot. The ICX was rebooted and worked as expected after the reboot. One hundred sixty ballots were scanned through each ICC (one complete deck), and the rest through the HiPro, and the results were as expected.

Polls were closed in accordance with California Use Procedures, including printing results from ICE and ICC, removing results media to transfer results back to EMS, and then shutting down devices. Post-Election results were consolidated and reported based on the upload of results to EMS from all tabulating (ICE and ICC) units. All reports were generated and verified including SOV, SSOV, precinct results, over-votes, and under-votes.

RCV Election: The Ranked Choice Voting Election was tested in English, Ilocano, Tagalog, and Thai. A fictitious election with one ballot style with two contests containing ten candidates. The ballot consisted of a single seat contest on one side of the ballot, and a multiple seat RCV contest on the other side of the ballot. The single seat contest was tabulated through eight rounds, and the multi seat contest was tabulated through ten rounds. The Mobile Ballot Production device was used to print 312 fourteen inch ballots, 78 in each language on the OKI 712C and performed as expected. An OKI 332C printer for the Mobile Ballot Production device was introduced at this time. The printer was to be exercised by printing 200 ballots each of eleven inch, fourteen inch, seventeen inch, and twenty two inch. The eleven inch ballots printed fine. Utilizing the fourteen inch ballots, the printer performed as expected for about 50 ballots, and then began to overheat and slow down. The printer finally overheated so badly that the safety mechanism in the printer shut it down, and it would not continue. The printer was withdrawn from testing.

Polls were opened in accordance with California Use Procedures. Zero reports for all devices were printed and verified. The test deck consisted of 78 ballots for each language, and one ballot was replaced (pulled from test deck, spoiled, and reprinted on MBP) for each language for each ICX. One ballot was marked on each ICX from each language for a total of four ballots on each ICX. One ballot from each language was marked on an ICE. All ballots were tabulated on both the ICE, ICP2, and ICCs. Results were loaded into the RTR, aggregated, and results checked against the expected results. The multi seat contest tabulated through 10 rounds correctly. The single seat contest tabulated through eight rounds correctly.

Polls were closed in accordance with California Use Procedures, including printing results from ICE and ICP2, and results media were used to transfer results back to the RTR. Reports were generated printing contest rankings for each round of RCV. RTR supports exporting this file in two third party formats: RCR and BLT.

At this point, the County Release HASHes were validated again per the California Use Procedures. The Mobile Ballot Production printer was tested for the ability to audit print jobs to verify that it printed exactly what was requested. Files generated were: Print report for each election, and one audit log report from May 23 to June 6. These logs meet the criteria for batch printing in CVSS. It was also verified at this time that the Mobile Ballot Production printer files generated by EED for the MBP are encrypted and a SHAW file is produced.

Test results showed that the voting system performed in a manner consistent with California Voting System Standards and all test cases were executed successfully and accurately. The testing did uncover many issues in the California Use Procedures. All were clarity issues and each of the issues discovered was resolved by editing the California Use Procedures.

3. Volume and Accessibility Testing Summary

As part of its testing, the Secretary of State conducts a Volume Test on all voting machines under test with which the voters will directly interact. The Dominion DS 5.10 voting system contains the ICE, ICP2, and the ICX ballot marking device machines at the precinct or vote center. The Volume Test took place between July 8, 2019, and July 10, 2019. The Accessibility Test took place between July 12, 2019, and July 16, 2019. The Secretary of State partnered with volunteers from the voters with disabilities communities to complete the heuristic evaluation of the accessibility features of the ICE and ICX, as well as to provide findings in this report. Both the Volume and Accessibility Tests used a modified version of the 2012 Presidential General Election as the basis for the election definition files. The Volume and Accessibility Tests were setup in a vote center model, with all ballot styles available on all ICEs, ICP2s, and ICXs, as opposed to being loaded with a single precinct, similar to that of a polling place.

3.a. Volume Testing Summary

The ICE precinct all-in-one machines, and the ICX Classic ballot marking devices presented for the DS 5.10 test are identical to the hardware that has been previously tested with the DS 5.2 voting system, but with new firmware. Per the California Volume Test Protocol, the Volume Test consisted of a total of 20 ICE precinct all-in-one devices, 20 ICX Prime ballot marking machines, ten ICX Classic devices, and 50 ICP2 precinct tabulators. The ICC machines in the SOS lab were utilized to verify all the counts from the test. Three Voter Activation Card (ICVA) laptops were used to generate the voter activation cards needed for the test. Consistent with Functional testing, one ICC utilized a Canon X10 scanner, and one utilized a Canon G1130 scanner. The Secretary of State used a total of 30 voters, ranging in age, skill, and voting experience, to vote ballots on the machines. Each class of machine was labeled in numerical order for proper identification.

Dominion provided fifty test decks, each with four hundred ballots for the ICE, and ICP2 machines. The ICP2 precinct tabulators were tested first. The software on each machine was validated to be the correct software, polls were opened, and a total of 400

ballots were scanned by each machine to simulate the voters a precinct or vote center would have on Election Day. The zero tapes created when the polls were opened were kept on the machines, and along with the results after the polls were closed, were saved as artifacts. As the test was being conducted, anytime there was an incident that took "poll worker" assistance, the incident was documented. Two different errors were noted on the ICP2 machines. The first was a "Ballot Jammed" error, and the second was a "Ballot Not Read" error. The Ballot Jammed error occurred 78 times on twenty eight ICP2 machines. The minimum was once, and maximum was eight times. Each time, the ICP2 reported it had counted the ballot. This was verified after the test when the counts were checked. In all cases, the ballot stacking plastic (box) was opened, the ballot removed from the back of the ICP2 machines, and the jam cleared by using the poll worker key to login and clear the error. The Ballot Jammed error was attributed to voters inserting a ballot too soon after the last one. The Ballot Not Read error occurred 52 times on 11 ICP2 machines. In every case except one, the ballot was pulled from the machine, reinserted in a different orientation, and was read without error. In one case, the ballot could not be read at all, and this was attributed to a printing error on the ballot where a white mark existed on one of the timing marks.

The ICE machines were next, and after the software was validated on all machines, polls were opened, and four hundred ballots were scanned into each machine. The zero tapes created when the polls were opened were kept on the machines, and along with the results after the polls were closed, were saved as artifacts. There were no incidents recorded on the ICE precinct tabulators.

The ICX and ICE ballot marking machines were tested next. Activation cards were created, and used to mark and print 50 ballots on each ICX machine. At this time, one of the ICX machines froze up after 22 ballots, and it was determined the cable from the tablet to the machine had become unconnected. Dominion related that it would be too hard to take the machine apart and connect the cable, so the machine was replaced and the test was completed on all machines. The machines performed as expected.

The ICE machines were tested in their ballot marking capacity next, and after the software on each machine was validated to be correct, polls were opened, and fifty blank ballots were marked on each ICE machine. ICE #5 was damaged in transit, and was replaced. Polls were then closed, and the paper tapes were verified. The ICE machines performed as expected except for the #5 machine.

After the test concluded, the Secretary of State verified the results of vote totals both locally, off of the ICE results tapes, and then overall, out of RTR. The verification resulted in a 100% accuracy rate. Based on the fact that the ICE performed with a 100% accuracy rate and the incidents and poll worker intervention rates were well below the 2% ballot rejection rate allowed by the California Voting System Standards, the Volume Test for the precinct count optical scan functionality of the ICE, and the ballot marking functionality of the ICX was deemed successful.

During the volume test, a Mobile Ballot Production laptop was setup, and the OKI C931 printer was tested. Two hundred ballots each were printed in 8.5X11, 11X14, 11X17,

and 11X22. The ballots were examined for accuracy, and then scanned through the ICE, and all ICCs back at the SOS Test lab. The printer performed as expected.

During volume testing, the Dominion L&A script file was also tested. The script is approximately 15 lines of XML. It was used to exercise the ICXs for L&A testing by printing 50 ballots on each of ten ICX Classics, and ten ICX Primes. The script was run with the ICX screens active so it could be examined while running. The script ran as expected.

3.b. Usability, Accessibility & Privacy Testing Summary

The Accessibility Test consisted of one ICE precinct all-in-one machine, which also functions as an accessible machine, one ICX Prime, and one ICX Classic. The machines were setup in privacy booths in the SOS Test Lab, giving enough space in between to allow some privacy.

Voters who were voting an Accessible Voting Session (AVS) had the ability to use any of the following components: the Audio Tactile Interface (ATI), lap pad, adaptive/paddle switches, headphones, sip and puff device, or rubber coated lap pad with ATI.

The ICE has the capability to support voters with the following disabilities:

- Cognitive - ballot display via paper and large Liquid Crystal Display (LCD) screen;
- Perceptual and Partial Vision - ability to change screen color scheme, contrast, and font size;
- Low or No Vision - audio, tactile interface;
- Dexterity - integrated ballot marking device that does not require the voter to manipulate the ballot, low force buttons for voter interface;
- Mobility –California Voting System Standards required reaches and wheelchair access, ICE product allows voter to avoid manipulating the ballot to go from the ballot marker to the scanner and obtain a scanned vote verification;
- Hearing - audio interface, same as for low/no vision; and
- Speech - no speech is required to operate the voting system.

The ICX ballot marking machines have the capability to support voters with the following disabilities:

- Cognitive - ballot display via paper and very large LCD screen;
- Perceptual and Partial Vision - ability to change screen color scheme, contrast, and font size;
- Low or No Vision - audio, tactile interface;
- Dexterity - ballot marking device that does not require the voter to manipulate the ballot, low force buttons for voter interface;
- Mobility –California Voting System Standards required reaches and wheelchair access, ICX product allows voter to mark the ballot, which must then be inserted into a tabulator or ballot box;

- Hearing - audio interface, same as for low/no vision; and
- Speech - no speech is required to operate the voting system.

The Secretary of State tested the voting system for usability and accessibility with four volunteer voters from the general population with the various disabilities mentioned above. Of the four voters, two identified that they are visually impaired, one identified dexterity problems, and one did not identify a disability. These volunteer voters were asked to vote two separate ballots, one each on the ICE and ICX.

The sessions were conducted with Dominion personnel acting as poll workers and the volunteers voting on the Dominion devices. Two SLI employees documented the test process and experience for each volunteer tester. When the volunteers arrived, they were given a quick briefing on the testing and the devices. The sessions were a free form, ad hoc test where the volunteer was able to vote a ballot in any manner that they chose. The volunteers voted on both the ICE device and the ICX Prime device. The volunteer provided feedback both real-time as they were voting, as well as completing an Accessibility Test survey for each device. Additionally, observations were made as each volunteer navigated their way through the process.

Activation cards for the ICX machine must be generated with the accessible option turned on for voters who are voting an Accessible Voting Session (AVS).

The Secretary of State survey asked twelve questions describing the voter's experience with the voting system. To categorize responses, the first ten questions were specific to the voting system. The questions and responses can be viewed in Appendix A.

The consensus of the volunteers was that they felt the technologies implemented for accessibility and usability improved the experience for voters that are most in need of them. From a privacy point of view, all volunteers seemed to feel that their privacy was kept intact and none expressed any issue or concern.

4. Security & Telecommunications Testing Summary

The Secretary of State contracted with SLI to conduct the Security & Telecommunications Review which took place at SLI's office in July and August, 2019.

The Security Review 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, and 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 review of the system design and architecture.

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

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

PHASE I

During Phase I testing, review of the TDP validated that all requirements were satisfactorily covered.

PHASE II

During Phase II testing, it was discovered that most requirements were satisfactorily covered.

During the Requirements examination and the Open Ended Vulnerability Testing (OEVT) portion of the testing, issues were noted related to audit logging, passwords, anti-virus, and installation aspects of the voting system. It should be noted that these issues do not directly affect the overall function of the voting system and could potentially be alleviated with manual processes and procedures. In many cases the issues discovered were not in relation to public facing voting system components and required elevated systems permissions for access or manipulation.

It should be noted that proper secure utilization of the voting system solution is reliant upon properly trained personnel, as well as following all processes and procedures set forth to ensure properly configured and secured equipment for use in a live election environment.

In-process Audit Records

Testing performed: As all other requirements were being tested, the audit log was reviewed to verify that appropriate records were recorded for the events occurring. All attempts to circumvent, modify or disable in-process audit logs or capabilities were unsuccessful.

Applicable to: EMS, Adjudication, ICC, ICE, ICP2, and ICX.

Review of the requirement showed that the ICX device does not provide monitoring of physical security. This would be mitigated by polling place procedures and physical security.

Access Control Authentication

Testing performed:

- Attempts to access system functions and resources without successful authentication to the operating system or DS 5.10 system;

- Attempts to find extra authentication data from system storage, including compact flash cards, hard drives, USB sticks and CFAST storage;
- Verified the system equipment allows the administrator to change all passwords, pass phrases and keys if applicable;
- Verified that the system(s) have the ability to lockout accounts after a specified number of failed authentication attempts; and
- Confirmed and tested the system's password complexity, strength, lockout, history, length, and expiration requirements.

Applicable to: EMS, Adjudication, ICC, ICE, ICP2 and ICX.

During enumeration of the Dominion system it was determined that a number of passwords were able to be recovered that were stored in plain text. However, the system is secured with Windows authentication and role based access controls.

Upon investigation of access control and authentication methods for the systems it was discovered that the Dominion technician keys contain all the same default passcode, however the default passcode can be changed by the jurisdiction in Election Event Designer (EED). It should be noted that the Dominion technician keys are not readily available. All other iButton security keys are programmable with new passcode combinations.

It was determined that the system security system iButton keys can be changed for poll-workers, for elections. In the event that the jurisdiction doesn't want old security keys to work, the system must regenerate election security elements prior to regeneration of the election files. However, a stolen smart card without knowledge of the PIN cannot achieve anything. Additionally, technician and poll worker smart cards can have an expiration date set in the EED. Regenerating all resources is only required if a poll worker with knowledge of the PIN becomes a bad actor in the system.

All windows based authentication credentials prohibited username as part of the password.

Review of the requirement showed that SLI was unable to determine if any of the equipment has the ability to expire passwords/passcodes or user accounts. However, Windows based operating systems have password expiration functionality specified for OS login.

Testing demonstrated that the requirement was partially covered. The findings can be mitigated by rigorous manual adherence to industry best practices of password/passcodes.

Physical Security Measures

Testing performed:

- Attempted to circumvent all physical security features including: Picking of

locks, attempts to circumvent or bypass security seals and security screws;
- Examined and tested all ports and connectors;
- Disconnected devices and examined audit logs as applicable to determine if auditing of device disconnection was present; and
- Identified and examined every cover, panel and access compartment.

Applicable to: EMS, Adjudication, ICC, ICE, ICP2 and ICX.

Security seals, locks and security screws can be circumvented, for this reason it is recommended that the jurisdictions have a procedure in place to efficiently manage and monitor security seals and locking devices. Dominion recommends “redwire” or lock style tamper-evident seals for hasps, and multiple tamper evident seals if there is no hasp.

Review of the requirement 7.3.d, showed that for the ICX, all ports are enabled on the system; however, physical access to these ports is restricted.

Protection against Malicious Software

Testing performed: Tests were performed to verify that COTS products are implemented to protect against malicious software, as described in voting system manufacturer documentation.

Applicable to: EMS, Adjudication, ICC, ICE, ICP2 and ICX.

Review of the requirement 7.4.2, showed that on the EMS Server, the AVAST Antivirus (AV) File Shield (the real time AV 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.

The ICX system is an android tablet device and contains no form of AV protection.

The ICE and ICP2 systems are proprietary systems that utilize firmware and compact flash cards to run, load, and store election-based software. These systems contain no operating system and no AV protection.

Testing demonstrated that the requirement was partially covered. The findings can be mitigated by rigorous adherence to physical security processes and procedures, which would preclude the introduction of any malicious applications.

Software Setup Validation

Testing performed: Tests were performed to verify that the installation process for each system component is robust and maintains the integrity of the voting system.

Applicable to: EMS, Adjudication, ICC, ICE, ICP2 and ICX.

Review of the requirement 7.4.6.b.i, shows that Dominion specifies what is required to complete software validation but does not specifically supply the required software or hardware to do so. In the case of the ICX third party, Android developer tools were required to pull packages from the ICX device for hashing. Dominion specifies that third party tools should be obtained from trusted locations for software validation. This provides stronger confidence that the correct software is installed as it is verified by third party tools with no link to the provider of the installed software (Dominion).

Review of the requirement 7.4.6.c.i, shows that Dominion specifies what is required to complete software validation but does not specifically supply the required software or hardware to do so. In the case of the ICX third party, Android developer tools were required to pull packages from the ICX device for hashing. Dominion specifies that third party tools should be obtained from trusted locations for software validation. This provides stronger confidence that the correct software is installed as it is verified by third party tools with no link to the provider of the installed software (Dominion).

SLI was able to modify election specific installers utilizing a hex editor to change minor things including mouse over text and digital signature names. Manipulating files in this way would change their hash values and invalidate the software when utilizing the software installation validation specified in the system's technical documentation package.

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 Democracy Suite Installation. However, election projects cannot be downgraded from 5.10 to 5.2, so a 5.2 installation cannot run an election project from 5.10. Additionally, Dominion provides the 5.10 System ID guide with hashes of the trusted build components, so these can be verified on a jurisdiction's configuration at any time necessary. Validating the software often, and on every system component is crucial to a secure system. Finally, Democracy Suite does not support mixing and matching of versions between components.

SLI believes it would be possible to inject more lethal payloads into the installers given the opportunity. This would require an insider with unhindered access to the system to edit the source code.

Review of requirement 7.4.6.f.i.2 determined that the ICX devices have no visual indicators showing if the port is enabled or disabled. All ports on the ICX are covered, locked, and sealed with tamper evident seals.

Review of requirement 7.4.6.f.i.3 determined that the ICX devices have no visual indicators showing that the port is disabled during voting. All ports on the ICX are covered, locked, and sealed with tamper evident seals.

Review of requirement 7.4.6.f.i.3 determined that there is not a specific method to

be able to verify or determine exactly all contents on the system. Dominion provides the 5.10 System ID guide with hashes of the trusted build components, so these can be verified on a jurisdiction's configuration at any time necessary.

Maintaining Data Integrity

Individual public facing voting components are not networked nor do they transmit individual voting results. This includes the ICE, ICP2 and the ICX. The only telecommunications that are in use are an isolated closed network to link the EMS/ADJ/ICC devices together at a central count location.

Testing performed: Tests were performed to verify that data is properly encrypted and that receipt is verified.

Applicable to: EMS, Adjudication, and ICC.

The examination determined that all results files and election relevant data that is transmitted in these methods are encrypted.

Access Control

Testing performed: Tests were performed to verify the documented procedures as well as attempts to defeat the implemented access control security on each system component.

Applicable to: EMS, Adjudication, ICC, ICE, ICP2 and ICX.

It was determined that the Dell managed switch was not sufficiently hardened during the engagement, this included an unencrypted telnet server with default username and password combinations. The findings can be mitigated by rigorous adherence to manufacturer specifications of hardening the switch, including encryption and use of non-default username/password combinations.

PHASE III

During Phase III testing, it was discovered that most requirements were satisfactorily covered. None of the issues directly affect the functioning of the voting system and could be alleviated with manual processes.

Testing performed: Testing was performed to verify appropriate encryption, receipt validation, and data integrity.

Applicable to: EMS, Adjudication, ICC, ICE, ICP2 and ICX.

Nessus vulnerability scans were conducted on all equipment that were connected to the private EMS network. These included the EMS Server, EMS Workstation, Adjudication Workstation, and ICC systems, as well as the managed switch.

Operating system level transmissions provided appropriate encryption, receipt validation, and data integrity.

The managed switch was scanned with Nessus and determined to have 12 medium vulnerabilities, and four low vulnerabilities. The switch is isolated from public networks, and access control policies limit who has access to the physical device. This can be mitigated by rigorous adherence to manufacturer specifications of hardening of the switch, including encryption and use of up to date security certificates.

Testing demonstrated that the requirement was partially covered. The findings can be mitigated by rigorous adherence to manufacturer specifications of hardening of the switch, including encryption and use of up to date security certificates.

5. Software Review Testing Summary

The Secretary of State contracted with SLI to conduct the Source Code Review. The Source Code Review took place at SLI between June 2019, and July 2019. The Dominion DS 5.10 voting system includes proprietary software and firmware. The Dominion DS 5.10 voting system code base was tested to the applicable CVSS requirements.

ADJ source code vulnerability review

No discrepancies or vulnerabilities were found within the ADJ source code base reviewed, as a result, no findings were written against the code base.

EMS source code vulnerability review

No discrepancies or vulnerabilities were found within the EMS source code base reviewed, as a result, no findings were written against the code base.

ICC source code vulnerability review

No discrepancies or vulnerabilities were found within the ICC source code base reviewed, as a result, no findings were written against the code base.

ICE source code vulnerability review

No discrepancies or vulnerabilities were found within the ICE source code base reviewed, as a result, no findings were written against the code base.

ICX source code vulnerability review

No discrepancies or vulnerabilities were found within the ICX source code base reviewed, as a result, no findings were written against the code base.

ICP2 source code vulnerability review

No discrepancies or vulnerabilities were found within the ICP2 source code base reviewed, as a result, no findings were written against the code base.

General Notes

It was noted during the installs that the EMS server utilizes DHCP for workstation address assignment, and as such this system would be susceptible to a DHCP starvation attack whereby a malicious device sends requests to the server and leases all the addresses available, or just provides bogus addresses to clients. The attacker would require physical access to the system, and would plug in a small box, or a small COTS router into the RTR network in order to supply bad addresses. This is mitigated by procedural controls and access controls to the physical network.

The ICX ballot marking device uses an encrypted QR code, but includes human readable results on the ballot. This QR code is encrypted, and cannot be read by any other machine except a Dominion device. This requires that the voter trust the machines in order to verify that the human readable results on the ballot are correct. This is mitigated by procedural controls and review by the voter prior to printing the ballot.

The ICE machine includes a design characteristic that merits some attention. Any machine that includes ballot marking and deposit into the ballot box in the same paper path, is not software independent, and could be compromised in a way that is undetectable with a manual tally or risk limiting audit. The ballot-marking printer is in the same paper path as the mechanism to deposit marked ballots into an attached ballot box. This opens up a security vulnerability: the voting machine can mark the paper ballot (to add votes or spoil already-cast votes) after the last time the voter sees the paper, and then deposit that marked ballot into the ballot box without the possibility of detection. Vote-stealing software could easily be constructed that looks for undervotes on the ballot, and marks those unvoted spaces for the candidate of the hacker's choice. This is very straightforward to do on optical-scan bubble ballots (as on the Dominion ICE) where undervotes are indicated by no mark at all. The autocast configuration setting that allows the voter to indicate, "don't eject the ballot for my review, just print it and cast it without me looking at it." If fraudulent software were installed, it could change all the votes of any voter who selected this option, because the voting machine software would know in advance of printing that the voter had waived the opportunity to inspect the printed ballot. This would be mitigated by using the ICE for accessible sessions only. Additionally, the ICE should include procedural controls whereby a technician completes the L&A procedures prior to an election, and then a second technician goes through the validation procedure to validate the firmware and software on the ICE, and then applies the seals to the machine. Any ICE that is presented at a polling place with broken seals should be replaced.

Security and Source Code Review Findings

Within the Dominion DS 5.10 code base, no discrepancies or vulnerabilities were found. All security and telecommunications findings were either low risk vulnerabilities, or they are mitigated by procedural controls.

During the ICX source code vulnerability review, one potential vulnerability was discovered and the level of access required to take advantage of this potential vulnerability would be open to a variety of actors including a voter, a poll worker, an election official insider, and a vendor insider. This potential vulnerability has a more widespread potential. Polling place procedural controls are one method of mitigating this issue, with poll workers actively verifying that the USB ports are covered and the covers sealed to prevent access.

IV. COMPLIANCE WITH STATE AND FEDERAL LAWS AND REGULATIONS

A. Elections Code Requirements

Six sections of the California Elections Code, Sections 19101, 19203, 19204, 19204.5, 19205, and 19270, describe in detail the requirements any voting system must meet in order to be approved for use in California elections. These sections are described in detail and analyzed for compliance below.

1) **§19101 (b) (1):** The machine or device and its software shall be suitable for the purpose for which it is intended.

   The system meets this requirement.

2) **§19101 (b) (2):** The system shall preserve the secrecy of the ballot.

   The system meets this requirement.

3) **§19101 (b) (3):** The system shall be safe from fraud or manipulation.

   The system meets this requirement.

4) **§19101 (b) (4):** The system shall be accessible to voters with disabilities pursuant to section 19242 and applicable federal laws.

   The system meets this requirement.

5) **§19101 (b) (5):** The system shall be accessible to voters who require assistance in a language other than English if the language is one in which a ballot or ballot materials are required to be made available to voters pursuant to Section 14201 and applicable federal laws.

   The system meets this requirement. Democracy Suite 5.10 supports Alaska Native, Apache, Bengali, Chinese, English, Eskimo, Filipino (Tagalog and Ilocano), French, Hindi, Japanese, Jicarilla, Keres, Khmer, Korean, Navajo, Seminole, Spanish, Thai, Towa, Ute, Vietnamese, and Yuman.

6) **§19203:** The system shall use ballot paper that is of sufficient quality that it maintains its integrity and readability throughout the retention period specified in sections 1700 through 17306.

The system meets this requirement.

7) **§19204:** The system shall not include procedures that allow a voter to produce, and leave the polling place with, a copy or facsimile of the ballot cast by that voter at that polling place.

The system meets this requirement.

8) **§19205 (a):** No part of the voting system shall be connected to the internet at any time.

The system meets this requirement.

9) **§19205 (b):** No part of the voting system shall electronically receive or transmit election data through an exterior communication network, including the public telephone system, if the communication originates from or terminates at a polling place, satellite location, or counting center.

The system meets this requirement.

10) **§19205 (c):** No part of the voting system shall receive or transmit wireless communications or wireless data transfers.

The system meets this requirement.

11) **§19270 (a):** The Secretary of State shall not certify or conditionally approve a direct recording electronic voting system unless the system includes an accessible voter verified paper audit trail.

The system meets this requirement.

B. Elections Code Review

1) **§305.5(b):** A paper cast vote record is a ballot only if the paper cast vote record is generated on a voting device or machine that complies with ballot layout requirements and is tabulated by a separate device from the device that created the paper cast vote record.

The system meets this requirement.

2) **§15360:** During the official canvass of every election in which a voting system is used, the official conducting the election shall conduct a public manual tally of the

ballots tabulated by those devices cast in one percent of the precincts chosen at random by the elections official. If one percent of the precincts should be less than one whole precinct, the tally shall be conducted in one precinct chosen at random by the elections official.

In addition to the one percent count, the elections official shall, for each race not included in the initial group of precincts, count one additional precinct. The manual tally shall apply only to the race not previously counted.

The system fully supports this requirement.

3) **§19300:** A voting machine shall, except at a direct primary election or any election at which a candidate for voter-nominated office is to appear on the ballot, permit the voter to vote for all the candidates of one party or in part for the candidates of one party and in part for the candidates of one or more other parties.

The system meets this requirement.

4) **§19301:** A voting machine shall provide in the general election for grouping under the name of the office to be voted on, all the candidates for the office with the designation of the parties, if any, by which they were respectively nominated. The designation may be by usual or reasonable abbreviation of party names.

The system meets this requirement.

5) **§19302:** The labels on voting machines and the way in which candidates' names are grouped shall conform as nearly as possible to the form of ballot provided for in elections where voting machines are not used.

The system meets this requirement.

6) **§19303:** If the voting machine is so constructed that a voter can cast a vote in part for presidential electors of one party and in part for those of one or more other parties or those not nominated by any party, it may also be provided with: (a) one device for each party for voting for all the presidential electors of that party by one operation, (b) a ballot label therefore containing only the words "presidential electors" preceded by the name of the party and followed by the names of its candidates for the offices of President and Vice President, and (c) a registering device therefore which shall register the vote cast for the electors when thus voted collectively.

If a voting machine is so constructed that a voter can cast a vote in part for delegates to a national party convention of one party and in part for those of one or more other parties or those not nominated by any party, it may be provided with one device for each party for voting by one operation for each group of candidates to national conventions that may be voted for as a group according to the law governing presidential primaries. No straight party voting device shall be used except for delegates to a national convention or for presidential electors.

The system meets this requirement.

7) **§19304:** A write-in ballot shall be cast in its appropriate place on the machine, or it shall be void and not counted.

The system supports this requirement.

8) **§19320:** Before preparing a voting machine for any general election, the elections official shall mail written notice to the chairperson of the county central committee of at least two of the principal political parties, stating the time and place where machines will be prepared. At the specified time, one representative of each of the political parties shall be afforded an opportunity to see that the machines are in proper condition for use in the election. The party representatives shall be sworn to perform faithfully their duties but shall not interfere with the officials or assume any of their duties. When a machine has been so examined by the representatives, it shall be sealed with a numbered metal seal. The representatives shall certify to the number of the machines, whether all of the counters are set at zero (000), and the number registered on the protective counter and on the seal.

The system supports this requirement.

9) **§19321:** The elections official shall affix ballot labels to the machines to correspond with the sample ballot for the election. He or she shall employ competent persons to assist him or her in affixing the labels and in putting the machines in order. Each machine shall be tested to ascertain whether it is operating properly.

The system supports this requirement.

10) **§19322:** When a voting machine has been properly prepared for an election, it shall be locked against voting and sealed. After that initial preparation, a member of the precinct board or some duly authorized person, other than the one preparing the machines, shall inspect each machine and submit a written report. The report shall note the following: (1) Whether all of the registering counters are set at zero (000), (2) whether the machine is arranged in all respects in good order for the election, (3) whether the machine is locked, (4) the number on the protective counter, (5) the number on the seal. The keys shall be delivered to the election board together with a copy of the written report, made on the proper blanks, stating that the machine is in every way properly prepared for the election.

The system supports this requirement.

11) **§19340:** Any member of a precinct board who has not previously attended a training class in the use of the voting machines and the duties of a board

member shall be required to do so, unless appointed to fill an emergency vacancy.

The system does not adversely impact this requirement.

12) **§19341:** The precinct board shall consist of one inspector and two judges who shall be appointed and compensated pursuant to the general election laws. One additional inspector or judge shall be appointed for each additional voting machine used in the polling place.

The system does not adversely impact this requirement.

13) **§19360:** Before unsealing the envelope containing the keys and opening the doors concealing the counters the precinct board shall determine that the number on the seal on the machine and the number registered on the protective counter correspond to the numbers on the envelope. Each member of the precinct board shall then carefully examine the counters to see that each registers zero (000). If the machine is provided with embossing, printing, or photography devices that record the readings of the counters the board shall, instead of opening the counter compartment, cause a "before election proof sheet" to be produced and determined by it that all counters register zero (000). If any discrepancy is found in the numbers registered on the counters or the "before election proof sheet" the precinct board shall make, sign, and post a written statement attesting to this fact. In filling out the statement of return of votes cast, the precinct board shall subtract any number shown on the counter from the number shown on the counter at the close of the polls.

The system supports this requirement.

14) **§19361:** The keys to the voting machines shall be delivered to the precinct board no later than twelve hours before the opening of the polls. They shall be in an envelope upon which is written the designation and location of the election precinct, the number of the voting machine, the number on the seal, and the number registered on the protective counter. The precinct board member receiving the key shall sign a receipt. The envelope shall not be opened until at least two members of the precinct board are present to determine that the envelope has not been opened. At the close of the polls the keys shall be placed in the envelope supplied by the official and the number of the machine, the number written on the envelope.

The system supports this requirement.

15) **§19362:** The exterior of the voting machine and every part of the polling place shall be in plain view of the election precinct board and the poll watchers. Each machine shall be at least four feet from the poll clerk's table.

The system supports this requirement.

C. Review of Federal Statutes or Regulations.

1) The Voting Rights Act (VRA) of 1965, as amended (42 U.S.C. 1973), requires all elections in certain covered jurisdictions to provide registration and voting materials and oral assistance in the language of a qualified language minority group in addition to English. Currently in California, there are ten VRA languages (English, Spanish, Chinese, Hindi, Japanese, Khmer, Korean, Tagalog, Thai, and Vietnamese) as prescribed under the law.

   The system meets this requirement. The system's paper ballots can be easily printed in these languages, as well as others.

2) The National Voter Registration Act of 1993 (42 U.S.C. 1973gg and 11 CFR 8) allows for the casting of provisional ballots through Fail-Safe Voting procedures.

   The system meets this requirement. Provisional ballots can be cast with this system.

3) The Voting Accessibility for the Elderly and Handicapped Act of 1984 (42 U.S.C. 1973ee through 1973ee-6) requires each political subdivision conducting elections within each state to assure that all polling places for federal elections are accessible to elderly and handicapped voters, except in the case of an emergency as determined by the state's chief election officer or unless the state's chief election officer: (1) determines, by surveying all potential polling places, that no such place in the area is accessible or can be made temporarily accessible, and (2) assures that any handicapped voter assigned to an inaccessible polling place will, upon advance request under established state procedures, either be assigned to an accessible polling place or be provided an alternative means of casting a ballot on election day.

   This system supports this requirement.

4) The Retention of Voting Documentation (42 U.S.C. 1974 through 1974e) statute applies in all jurisdictions and to all elections in which a federal candidate is on a ballot. It requires elections officials to preserve for twenty two months all records and papers which came into their possession relating to an application, registration, payment of a poll tax, or other act requisite to voting. Note: The US Department of Justice considers this law to cover all voter registration records, all poll lists and similar documents reflecting the identity of voters casting ballots at the polls, all applications for absentee ballots, all envelopes in which absentee ballots are returned for tabulation, all documents containing oaths of voters, all documents relating to challenges to voters or absentee ballots, all tally sheets and canvass reports, all records reflecting the appointment of persons entitled to act as poll officials or poll watchers, and all computer programs used to tabulate votes electronically. In addition, it is the Department of Justice's view that the phrase "other act requisite to voting" requires the retention of the ballots

themselves, at least in those jurisdictions where a voter's electoral preference is manifested by marking a piece of paper or by punching holes in a computer card.

The system meets this requirement. All votes in this system are recorded on paper ballots that can be retained.

D. Help America Vote Act (HAVA) Requirements

The Help America Vote Act (HAVA) §301(a) mandates several requirements for voting systems, including:

1) The ability to verify the vote choices on the ballot before that ballot is cast and counted,

2) Notification to the voter of over-votes on a ballot,

3) Auditability with a permanent paper record of votes cast, d) Accessibility for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence)

This system supports these requirements in the following manner:

i. The paper ballots themselves lend themselves to visual inspection and verification.

ii. The ImageCast X and ImageCast Evolution provide its users with a ballot review screen prior to printing the ballot. Further, any voted ballot can be inserted into the unit for review and verification.

iii. The ImageCast X and ImageCast Evolution prevent over-voting a contest.

iv. Because all ballots in this system are paper based, there is a fully auditable and permanent record of the election.

v. Deployment of the ImageCast X and ImageCast Evolution in a precinct provides accessibility for persons with disabilities at the polling place.

V. CONCLUSION

The Dominion Democracy Suite 5.10 voting system, in the configuration tested and documented by the Installation and Use Procedures, meets applicable California Voting System Standards and Elections Code requirements.

Appendix A: VOTERS WITH SPECIFIC NEEDS SURVEY RESULTS

1. Survey Results

The Secretary of State conducted an exit survey on the voters who participated in the Accessibility Test regarding their voting experience utilizing the ImageCast Evolution (ICE), and ImageCast X (ICX). The majority of participants found that the voting system would allow them to vote privately and independently; that the voting instructions were clear and complete; the display was easy to read; and that the speech output was understandable. All participants related that they preferred the ICX over the ICE.

Question # 1: The voting method was private.

ICE: 75% of participants agreed strongly that the voting method was private. 25% disagreed somewhat.
ICX: All participants agreed with the statement. All agreed that with the privacy screen in place, their voting experience was private. However, most chose to use the ICX which was setup on a table without the privacy screen to make it more comfortable to reach the ICX machine.

Question # 2: I feel I can use this system to vote independently.

ICE: All but one participant agreed with this statement. One participant disagreed strongly.
ICX: 100% agreed that the voting machine allowed them to vote independently.

Question #3: I am confident that my vote was recorded accurately.

ICE: All participants except one agreed strongly with this statement, however, it is not possible for voters using the ICE to verify their actual paper ballot after voting because it has been dropped into the ballot box.
ICX: All participants agreed strongly that their vote had been recorded accurately.

Question # 4: The voting instructions were clear and complete.

ICE: All participants except for one agreed strongly or agreed somewhat with this statement. One participant disagreed strongly with this statement, and said they would have abandoned the session in a polling place.
ICX: 100% of participants agreed.

Although most of the survey respondents either agreed strongly or agreed somewhat that the voting instructions were clear and complete, they were able to utilize the voting machines much better the second time they voted on the machine.

Question # 5: The voting method was easy to use.

ICE: All of the survey respondents except one disagreed that the voting method was easy to use.
ICX: 100% of survey respondents agreed that the voting method was easy to use.

Question # 6: I could read the display easily.

ICE: One participant with visual impairments rated this N/A. 50% of the other participants agreed with this statement, and 25% disagreed.
ICX: 100% of participants (including the visually impaired participant) agreed with this statement.

Question # 7: I could understand the speech output.

ICE: 75% of participants agreed with this statement. 25% of participants disagreed with this statement.
ICX: 75% of participants agreed with this statement. 25% of participants disagreed with this statement. Two participants related the sound was very inconsistent.

Question # 8: The assistive device(s) were easy to reach and use.

ICE: 50% of participants agreed with this statement. 50% of participants disagreed.
ICX: 75% of participants agreed with this statement. 25% disagreed with this statement.

Question # 9: I found the system was confusing to use.

ICE: 50% of participants agreed strongly with this statement. 50% of participants disagreed with this statement.
ICX: 75% of participants agreed with this statement. 25% of participants disagreed with this statement.

10: The timeframe it took to vote was what I expected.

ICE: 25% of participants agreed with this statement. 75% of participants disagreed with this statement.
ICX: 100% of participants agreed with this statement.