Voting System Examination of Dominion Voting Systems Democracy Suite 5.5-A

Brian Mechler, Technical Examiner
Exam Dates: October 2-3, 2019
Report Date: November 3, 2019

1 Background

An examination of the Dominion Voting Systems Democracy Suite (D-Suite) 5.5-A was conducted at the Texas Secretary of State Elections Division offices on October 2-3, 2019. D-Suite 5.5-A is a comprehensive voting system which consists of the following components [1][2]:

- Election Management System (EMS) – the set of client and server applications and hardware used to define and manage elections including the tabulation and reporting of results.
- Adjudication – EMS server and client components responsible for ballot adjudication as well as reporting and generation of adjudicated result files.
- ImageCast Central (ICC) - A ballot scan tabulator and associated ballot processing application for use in central elections offices.
- ImageCast Precinct (ICP) - An optical scan ballot tabulator for use at polling places.
- ImageCast X (ICX) Ballot Marking Device (BMD) – Commercial off-the-shelf (COTS) hardware and operating system, which utilizes custom applications to act as a BMD.

The Election Assistance Commission (EAC) certification includes tables that describe in detail the voting system software components, voting system platforms, and hardware components. [3].

On June 20, 2019, the State of Texas denied certification of Dominion Voting Systems D-Suite 5.5 [4]. This denial was based on findings from the January 16-17, 2019 examination for which I was present [5]. Development of D-Suite 5.5-A was already complete by the time Dominion received feedback from the January exam of D-Suite 5.5. Thus, none of the changes in D-Suite 5.5-A were intended to address the issues raised during the January exam. The following is the complete list of changes between D-Suite 5.5-A and 5.5 [6]:

- “Modification to ICX straight party behavior to show a modal pop-up window when a voter attempts to undervote a partisan contest after selecting a partisan choice in the straight party contest; the pop-up clarifies that the voter needs to remove their straight-party vote and manually vote all partisan contests if they wish for one or more of those contests affected by the straight party vote to be undervoted”

- “Updated default ICX localizations to change wording of final voter session wording to reflect that the ballot is being printed rather than cast”
- “Removed the ICX DRE configuration as it was not required by the State of Pennsylvania”
- “Removed the ICX Classic 15” model for marketing purposes”
- “Used MCF v5.5.10.19 (EMS 5.5 default configuration file for the ICX) as changes to MCF v5.5.10.20 from D-Suite 5.5 were related to VVPAT printer component and not relevant to the 5.5-A system configuration”

In addition to the above changes, D-Suite 5.5-A significantly reduced the number of hardware configurations available compared to D-Suite 5.5.

- The Express EMS hardware configuration is not offered, only the Standard client-server configuration.
- The ICX Prime BMD is the only available voting machine; all ICX Classic platforms, ICX Prime DRE, and ICX Prime DRE with VVPAT are not within the scope of certification for D-Suite 5.5-A.

The Secretary of State Elections Division obtained the software and firmware (FW) images used in the EAC certification directly from the EAC. Dominion personnel used those same files to perform installation under the supervision of the technical examiners. In [7], Dominion provides instructions for the identification and verification of the components included in D-Suite 5.5-A.

The examination also consisted of an accessibility test, vendor presentations and demos, a mock election, and a free-form session where examiners could ask follow-up questions and use the voting equipment in an unscripted manner.

I was not present for the accessibility portion of the exam. ADA compliance will be presented in the legal examiners’ reports. A detailed description of the Texas Secretary of State examination, including my observations, concerns, and recommendations, is presented in the sections that follow.

2 Election Management System

The EMS is the set of client and server hardware and associated software used in pre-voting and post-voting activities.

The Standard EMS configuration is the only one available in D-Suite 5.5-A. The Standard configuration consists of a Dell PowerEdge R640 Server and one or more Dell Precision 3431 Workstations [8]. The server uses Microsoft Windows Server 2012 R2 as its OS and the workstations run on Microsoft Windows 10 Professional.

The server is configured with dual 1-TB hard drives in RAID 1 mode and four 1-TB hard drives in RAID 10 mode for data redundancy.

The server, EMS workstations, and ICC workstation communicate over a network switch that is provided by Dominion. The server host operates a DHCP server with a static pool of IP addresses. The

EMS system must be operated within its own isolated private network (i.e. not connected to any public or other internal networks). It should connected only to other components of the certified configuration.

The EMS system creates media for the voting and tabulating equipment. CFast cards are used to load election definitions on to the ImageCast Precinct. USB thumb drives are used to load election definitions on to the ICX BMD. The EMS system also creates iButton keys and SmartCards for two-factor authentication.

Backend applications and services are installed on the server hardware, and end-user applications (and some supporting services) are installed on the client workstations. In [2], Dominion describes the major software components:

- EMS Adjudication - “Server and client components responsible for adjudication, including reporting and generation of adjudicated result files from ImageCast Central tabulators.”
- EMS AIMS Data Translator - “End-user application that transfers election definitions from Democracy Suite to EMS to AIMS, enabling users to program AutoMARK devices for ImageCast ballots.”
- EMS Application Server - “Server side application responsible for executing long running processes, such as rendering ballots, generating audio files and election files, etc.”
- EMS Audio Studio - “End-user helper application used to record audio files for a given election project. As such, it is utilized during the pre-voting phase of the election cycle.”
- EMS Data Center Manager - “System level configuration application used in EMS back-end data center configuration.”
- EMS Database Server - “Server side RDBMS repository of the election project database which holds all the election project data, including pre-voting and post-voting data.”
- EMS Election Data Exchange Station (EDES) - “End-user helper application used to program the memory cards and iButton security keys required to properly operate the ImageCast series of counting devices. As such, it is utilized during the pre-voting phase of the election cycle.”
- EMS Election Data Translator - “End-user application used to export election data from election project and import election data into election project.”
- EMS Election Event Designer - “Integrates election definition functionality together with ballot styling capabilities and represents a main pre-voting phase end-user application.”
- EMS File System Service - “Stand-alone service that runs on client machines, enabling access to low level operating system API for partitioning CF cards, reading raw partition on ICP CF card, etc.”
- EMS NAS Server - “Server side file repository of the election project file based artifacts, such as ballots, audio files, reports, log files, election files, etc.”

- EMS Results Tally and Reporting - “Integrates election results acquisition, validation, tabulation, reporting, and publishing capabilities and represents a main post-voting phase end-user application.”
- EMS Result Transfer Manager - “Stand-alone application used to transfer result files from the remote locations to one or more central locations where the results can be tallied and reported on.”
- EMSLogger - “a stand-alone application that runs on client or server machines and is used to gather diagnostics for troubleshooting.”
- Smart Card Helper service - “Installed on a workstation or laptop at the polling place, and provides required data format for programming smart cards for ImageCast devices, or, for jurisdiction’s voting registration system in case of integration.”
- ImageCast Voter Activation application - Installed on a workstation or laptop at the polling place, that allows the poll workers to program smart cards for voters. The smart cards are used to activate voting sessions on ImageCast X.”

Version numbers for the D-Suite 5.5-A EMS software components are the same as those included with D-Suite 5.5 [3][9].

2.1 Observations

The use of most of the EMS software components was not directly observed by examiners during the mock election and free-form portion of the exam. The following subsections will cover the installation process and components which were directly observed or responsible for issues during the exam.

2.1.1 Installation

Examiners witnessed Dominion personnel install the server and client software components. The installation process is very complex and requires the manual entry of certain paths and host names. Dominion provides a custom installation helper application which allows the user to navigate to and launch installers for individual components. Those components are not necessarily presented in order within the installation helper application. There is a point during the install process where the user must divert from using Dominion’s custom installer to install certain 3rd party prerequisites from DVD. Users must take great care to follow the exact installation instructions provided by Dominion. Though hyperlinks are provided in the documentation to help the user navigate from one step to the next, instructions are not presented in order within the documentation and, in fact, are spread across multiple documents.

A problem was encountered during the installation of Adjudication Services on the server. The only way to resolve this issue was to wipe the server clean with a fresh installation of the operating system (as well as all of the prerequisites up to that point). According to Dominion personnel, the server hardware should have been rebooted prior to installing Adjudication services. As a result of missing that step, the installation of the EMS was delayed by hours.

2.1.2 Election Event Designer (EED)

The Secretary of State's office provided Dominion with election data for the mock election portion of the exam. Prior to the exam, Dominion used EED to create paper ballots as well as election definitions for the ICC, ICP, and ICX. The election definition for the ICX includes the touchscreen representation of the ballot.

Aside from the misspelling of one candidate's name, there were no issues with the paper ballot. However, the touchscreen ballot had multiple errors beyond the simple spelling mistake. Party affiliations were not listed next to candidate's names, voting instructions specific to each contest were missing, and ballot proposition language was missing. In addition, the wording of the instruction on the final screen of the ballot instructed the voter to "cast" their ballot instead of printing it. Note that this was one of the very small number of changes that was supposed to have been picked up in this revision of D-Suite.

When asked, Dominion stated that this election definition had been put through an internal logic and accuracy (L&A) test prior to the exam. Yet none of these issues were caught.

After the mock election portion of the exam, Dominion personnel created a new election definition to show that they could fix all of the errors and misconfigurations, and it appeared that they did.

Similar to the install process, it appears that EED is overly complex and fragile. Many troubling questions come to mind. If Dominion personnel, theoretically the most expert users of this software, can create an election definition with so many glaring errors, how error-prone will the system be for jurisdictions that opt to create their own election definitions? What level of service will jurisdictions receive if they outsource the creation of election definitions to Dominion? One would assume that a certification exam sets the benchmark for the quality of service vendors provide to jurisdictions.

2.1.3 Adjudication

Examiners adjudicated hand marked ballots scanned on the ImageCast Central. The Adjudication user interface displays the scanned ballot image and highlights the machine interpretation of voter intent in green (see Figure 1). These green bars were occasionally offset from where the chosen candidates appeared on the ballot creating a confusing and frustrating user experience (see Figure 2). The highlighting feature can be disabled should users find it to be counterproductive.

In the January exam of D-Suite 5.5, examiners witnessed a crash of Adjudication Services due ostensibly to a misconfigured path. The crash of Adjudication Services required the readjudication of all previously adjudicated ballots. This issue did not occur during the exam of D-Suite 5.5-A. However, since there were no changes made to the Adjudication software, this issue could arise again.

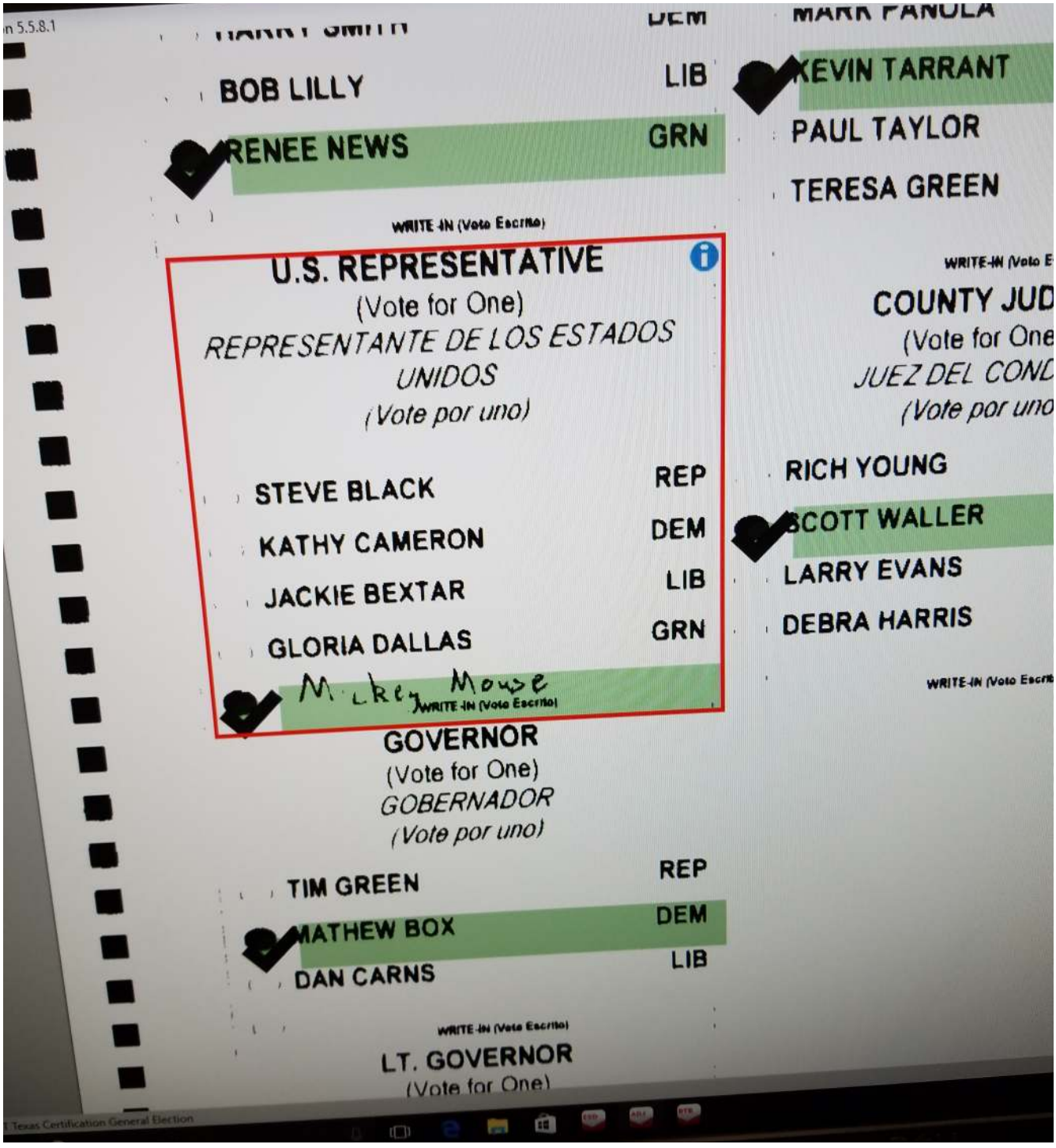


Figure 1: Properly Aligned Visual Aid

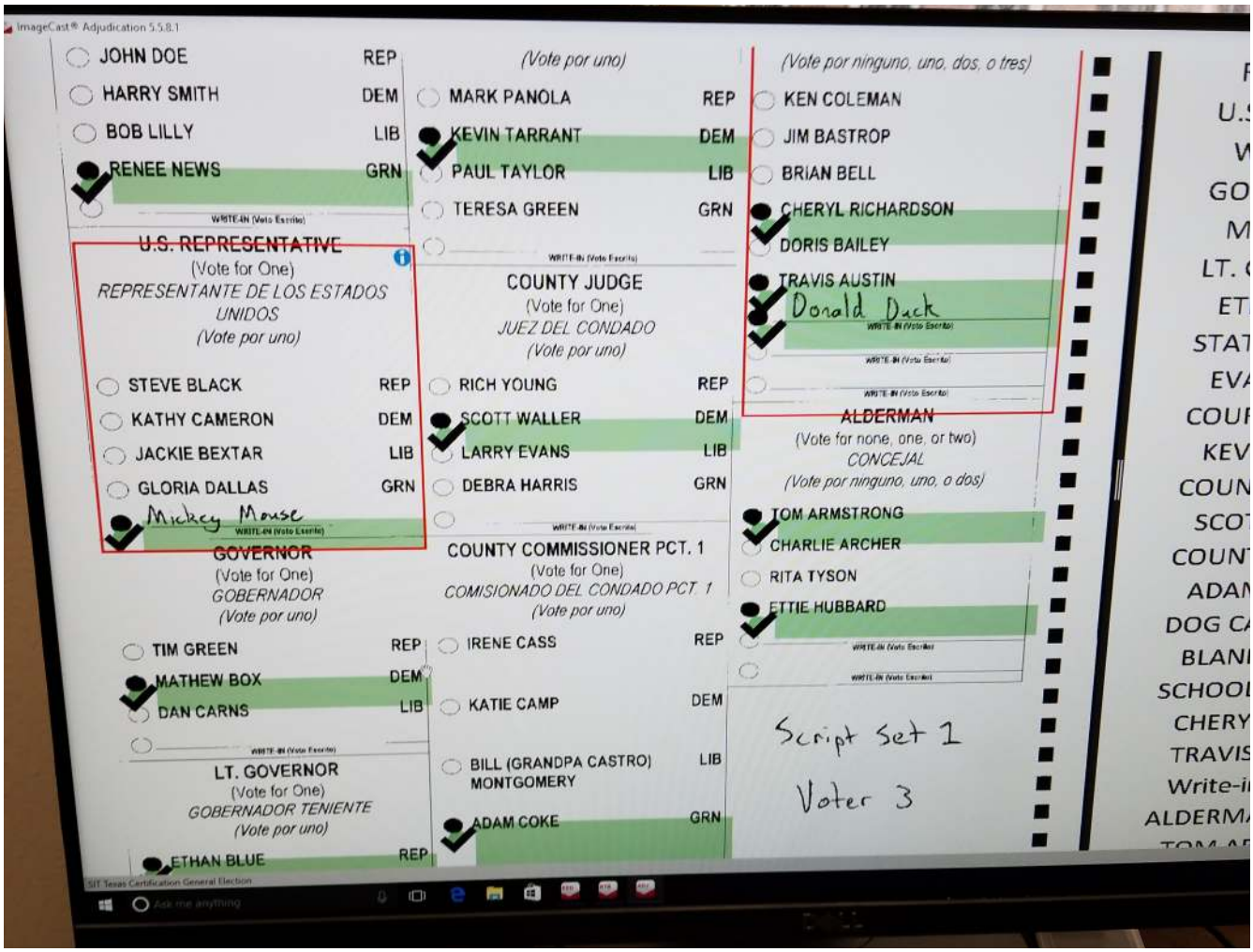


Figure 2: Misaligned Visual Aid

2.1.4 Results Tally and Reporting (RTR)

RTR was used to tally votes and produce reports from the mock election. No issues were observed. Votes were tallied and reported accurately.

3 Scanners

D-Suite 5.5-A includes two ballot scanners. The ImageCast Central (ICC) is for use at the jurisdiction's central office and is typically used to scan mail-in ballots. ImageCast Precint (ICP) is a polling place scanner. The ICC and ICP can both process hand-marked and machine-marked ballots.

3.1 ImageCast Central

The ICC utilizes a COTS Canon DR-G1130 scanner connected to a Dell Optiplex 3050 AIO Workstation. The workstation runs Windows 10 (64-bit) Professional edition as its OS. The ICC workstation can be connected over the isolated private network to the EMS server. If connected to the server, the ICC can be configured to save scanned ballot images and cast vote records (CVRs) on both the ICC workstation and the EMS server.

The Canon DR-G1130 has a feeder capacity of 500 sheets. It can scan one hundred 8.5”x11” pages per minute. Ballot stock in lengths ranging from 11” to 22” can be used.

An iButton security key is required for two-factor authentication, decryption of election files, and encryption of results files.

The ICC can be configured to reject ballots that have issues, such as ambiguous marks and under/over votes.

3.1.1 Observations

Examiners observed the installation of the ICC workstation software and there were no notable issues with this process.

During the mock election, examiners observed the processing of ballots through the ICC. The ICC properly rejected ballots that did not meet the criteria of the loaded configuration. There is some latency between the scanning of the ballot and the detection of an issue. As a result, a handful of ballots are scanned subsequent to the problem ballot. However, the ICC workstation application correctly informs the user of how many ballots need to be rescanned. The ICC jammed once during the processing. When the ICC encounters a paper jam, the entire batch must be rescanned.

3.2 ImageCast Precinct

The ICP is a custom hardware device with a scanner, integrated thermal printer, and LCD touchscreen. When a voter is finished marking their ballot (either by hand or using the ICX BMD), they insert it into the ICP where it is scanned and deposited into the ballot box. The ICP can read ballots in any orientation. It can be configured to reject ballots that have issues such as ambiguous marks and under/over votes.

Firmware is loaded from a CFast card along with an iButton Administrator key for authentication. Different iButton keys are required for other roles and actions. The iButton Administrator key is provided by Dominion and color-coded so that it is not accidentally confused with keys that are reprogrammed across elections.

Election definitions are loaded via CFast cards and stored in internal memory. CVRs and scanned images are stored on two CFast cards for data redundancy. Redundancy between the two cards is checked after each file write and if the cards ever fall out of sync, the ICP will cease to operate as a tabulator until the issue is resolved.

3.2.1 Observations

Examiners witnessed the installation of ICP firmware. The installation required the use of an iButton Administrator key. The PIN associated with the iButton Administrator key is only 1-digit long and cannot be changed. Dominion should at the very least make the PIN more complex and preferably issue keys protected by unique PINs.

The FW installer provides an option to install older versions of the ICP FW. According to Dominion, this feature exists to support the recount of an election conducted under an older version. The problem

with this feature is that jurisdictions would have the ability to install FW that has not received certification in Texas. This is an unnecessary convenience that risks the use of a non-certified system in an election. If jurisdictions have purchased older, certified versions of D-Suite, they should already have the FW install files for that particular version. Alternately, they should be able to obtain those files from Dominion.

During the free-form session of the exam, one of the examiners scanned a paper ballot with an ambiguous ballot mark. The ICP properly rejected the ballot, but the error messaged flashed so quickly across the LCD screen that examiners could not easily determine the reason for rejection. When a ballot is rejected, the error message should persist on the LCD screen so the voter and/or poll worker can determine what went wrong and resolve the issue.

Two different ballot box configurations were demonstrated. Both configurations provided adequate ballot security.

Two identical ICP scanners were in use during this exam. Though D-Suite 5.5-A uses the same ICP FW and HW as D-suite 5.5, examiners did not encounter issues with paper jams and poor quality images this time around. Dominion's best guess for the poor performance during the D-Suite 5.5 exam was that the ICP unit used was defective or damaged during shipping.

4 ImageCast-X Ballot Marking Device

The ICX BMD consists of custom software running on COTS hardware (Avalue HID-21V-BTX). The Avalue tablet runs the Android 5.1 OS. The tablet is connected to a HP M402dne COTS printer and optionally an audio-tactile controller and LED indicator light.

Two-factor authentication is role-based and accomplished via ACOS-6-64 SmartCards. The SmartCards authenticate one of three roles; Technician, Poll Worker, and Voter.

Technician cards are used when loading the ICX applications on the tablet and when loading the election definition files. Election definition files are stored on USB thumb drives; the election definition files are not transferred to the tablet's internal memory. EED is capable of programming Technician cards. A Technician card does not grant access to election day related functions.

Poll Worker cards are programmed by EED. They give poll workers the ability to open/close polls, extract audit logs, perform diagnostics tests, and manually activate voting sessions for voters. Election definitions are encrypted when first loaded. Poll Worker cards hold the decryption key which decrypts the election definition upon their first use. Every time a Poll Worker card is used, it verifies the digital signature of the loaded election definition.

The Voter card is typically programmed at the polling place by poll workers using an ImageCast Voter Activation workstation (a piece of hardware that is outside the scope of this certification exam). The Voter card is provided to voters so they can activate their own voting sessions. The Voter card only activates the ballot specific to the voter's precint. After it has been used to print a ballot, the Voter card cannot be used again until it has been reprogrammed by a poll worker.

4.1 Observations

Installation of the ICX application by Dominion personnel was witnessed by the examiners. A Technician card is required to install the ICX application. A Technician card is not required to install other applications. The technician must manually put the ICX tablet in kiosk mode after installing the ICX application. If one has access to ICX data ports, kiosk mode the only thing preventing someone from installing non-certified software. Only a user with Technician card credentials can take the ICX out of kiosk mode. In this exam, and in the January D-Suite 5.5 exam, Dominion personnel failed to place voting machines in kiosk mode after installing the ICX application. This critical step needs to receive greater focus in Dominion's internal training.

Examiners used the ICX BMD to mark ballots during the mock election. The touchscreen user interface is intuitive and easy to navigate. Any difficulty experienced marking a ballot was due to the misconfigured election definition (detail provided in Section 2.1.2).

In my report of the D-Suite 5.5 exam, I found that hasp seals insufficiently secured the doors protecting data and network ports. During the 5.5-A exam, Dominion recommend the use of tamper-evident adhesive seals to secure the doors. This is a very good recommendation. In fact, the same recommendation can be found in the ICX System Operation Procedures manual [12]. However, the ICX User Guide [13] is vague on whether adhesive seals should be used in addition to hasp seals. With regard to securing the doors, the Democracy Suite System Security Specification [14] simply refers the reader to the COTS manual [15]. The Avalue HID-21V-BTX manual only recommends hasp seals to secure the doors. Dominion needs to provide consistent guidance across all of their documentation regarding physical security of ICX devices.

A new hardware peripheral in the form of a COTS LED indicator light was demonstrated. The LED indicator provides voting system status to poll workers without violating the privacy of voters. In theory this would be a welcome feature. Unfortunately, this new peripheral exposed a secured USB port. The LED light is controlled by a detachable USB-C cable (see Figure 3). In [16], Dominion recommended two mitigation options (I recommend the latter):

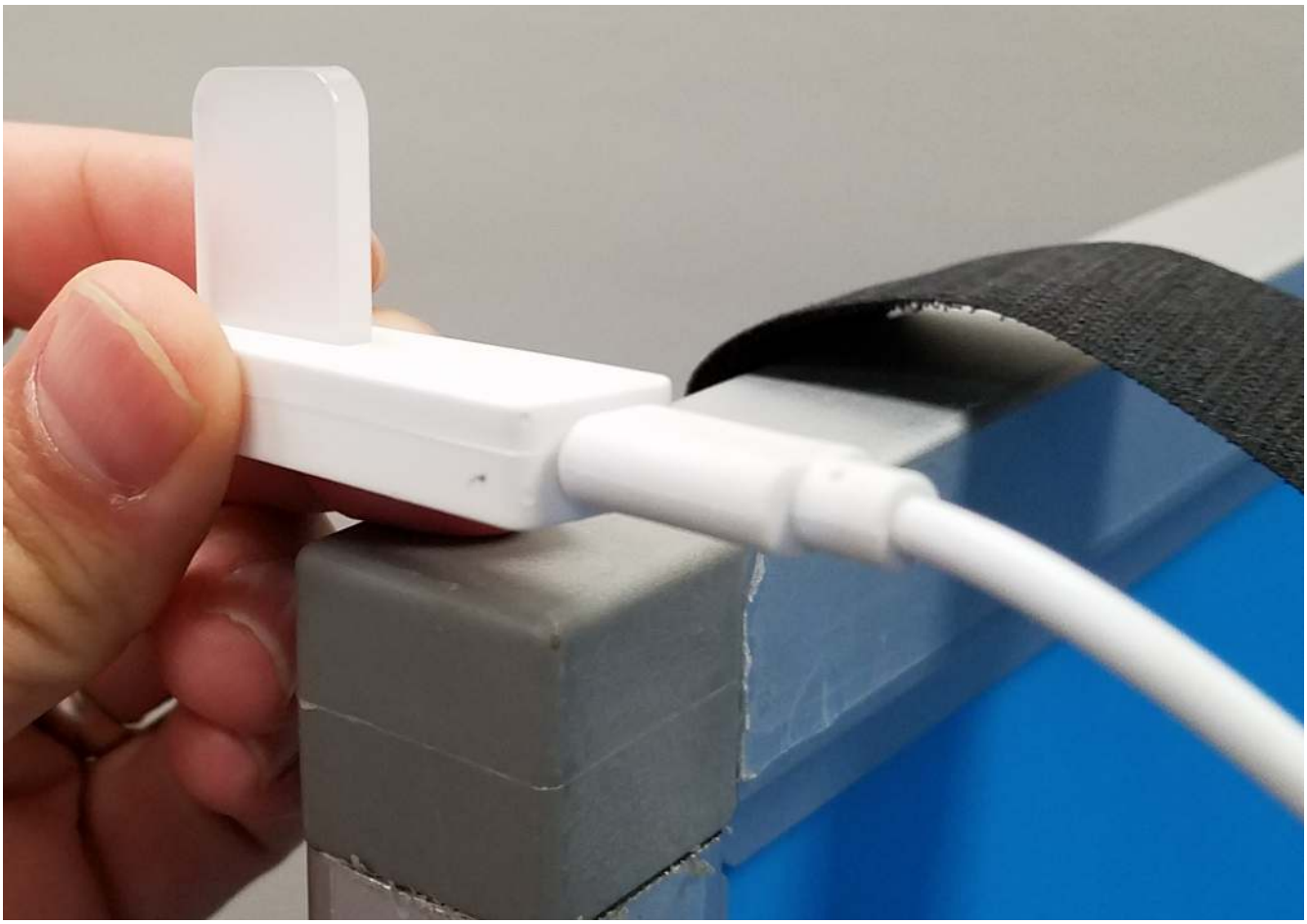
- "Seal the connection between the LED light and the USB cable"
- "Remove the LED light from the Texas configuration altogether"

One issue with relying heavily on COTS equipment in the polling place is that often the end-use is not envisioned by the original COTS product designers. The Avalue tablet is a good example of this disconnect. Door 3 of the device secures DC in/out ports, the power button, and a USB port. Due to the presence of the USB port, this door must be sealed at all times during an election. During early voting, poll workers will have to break and replace this seal at the beginning of each day to power on the device.

It was discovered during an informal test that if a USB peripheral were added while the Avalue device was powered off, users of ICX (even those with Poll Worker card access) would not be made aware of the configuration change. The "Hardware Details" diagnostic provided by the Poll Worker menu only checks the status of defined peripherals (i.e. the printer, LED, and audio-tactile interface). Audit logs can be viewed on-screen, but those logs do not contain the level of detail necessary to discover the

presence of a non-certified device. Only the system logs capture enough detail to detect the addition of non-certified USB devices. The system logs are not typically exported and examined each day during early voting.

In the 5.5-A configuration, the ICX can only be operated in BMD mode; thus it does not create or store CVRs. It's unlikely someone could significantly alter the outcome of an election via this vulnerability (assuming voters carefully review their marked ballots). However, voter confidence in elections systems is a critical component of democracy. Evidence of tampering on even one system undermines this confidence. After this discovery, Dominion recommended the use of a serialized port lock or a non-residue tape seal to secure the USB port behind Door 3 [16].



5 ImageCast Voter Activation (ICVA)

ICVA is an application that runs on a laptop or workstation located at the polling place. It is used to program Voter SmartCards that can activate voting sessions on ICX devices.

5.1 Observations

The ICVA software and hardware are not within the scope of this certification exam. My observations of this component will have no bearing on my recommendations regarding D-Suite 5.5-A. Nevertheless, examiners witnessed the installation and use of this application. No issues were observed. In general, voter activation stations such as ICVA can allow for a more streamlined polling place and reduce the burden on poll workers.

6 Conclusions

Multiple major issues are present in D-Suite 5.5-A (enumerated below):

1. Complexity and fragility of the EMS installation process
2. Complexity and fragility of the Election Event Designer revealed by multiple errors in the Dominion generated election definition file for the ICX BMD
3. Inability to gracefully recover from a crash of Adjudication Services (no crashes were witnessed in this exam, but this EMS software component is identical to the one in D-Suite 5.5)
4. Easily cracked PIN on Technician iButton key
5. ICP installer allows installation of non-certified firmware
6. ICP's unclear and buggy behavior in response to an ambiguous mark on a hand-marked ballot
7. ICX LED indicator exposes an otherwise secured data port
8. Unclear and insufficient guidance in technical data package regarding physical security of ICX

In aggregate, Issues 1-3 and prevent D-Suite 5.5-A from meeting Texas Voting System General Requirement 122.001(a)(2): "Must be suitable for the purpose for which it is intended."

In aggregate, Issues 1-3 and Issue 5 prevent D-Suite 5.5-A from meeting Texas Voting System General Requirement 122.001(a)(3): "Operates safely, efficiently, and accurately and complies with the voting system standards adopted by the EAC."

If operated properly, D-Suite 5.5-A could be a system that operates safely, efficiently, and accurately. However, we have not yet witnessed that even Dominion's own subject matter experts can operate the system properly. To be clear, the above statement is not an indictment of Dominion personnel. I found the representatives at the exam to be courteous, professional, knowledgeable, and eager to answer examiners' questions and resolve issues. It is the EMS system itself that is difficult to work within.

Issues 4, 7, and 8 prevent D-Suite 5.5-A from meeting Texas Voting Systems General Requirement 122.001(a)(4): "Is safe from fraudulent or unauthorized manipulation."

Many of these issues could be resolved by placing conditions on the certification of D-Suite 5.5-A.

- Require that Dominion deliver EMS to customers on pre-imaged drives (resolves Issue 1)
- Require that Administrator iButton key be protected by sufficiently complex PIN (resolves Issue 4)
- Remove non-certified firmware versions from ICP installer (resolves Issue 5)
- Remove the ICX LED peripheral from the Texas certification (resolves Issue 7)
- Update documentation to provide clear and consistent guidance regarding physical security best practices (resolves Issue 8)

Ultimately, this set of conditions is too large to be considered de minimis. I recommend against certification of Dominion Voting Systems Democracy Suite 5.5-A.

7 References

[1] Application for Texas Certification of Voting System – Form 100, Signed Aug-28 2019

[2] Democracy Suite System Overview, Version 5.5-A::155, Dec-12 2018

[3] United States Election Assistance Commission Certificate of Conformance Dominion Voting Systems Democracy Suite 5.5-A, EAC Certification Number DVS-DemSuite5.5-A, Jan-30 2019 URL: https://www.eac.gov/voting-equipment/democracy-suite-55-a-modification/

[4] J. A. Esparza, “Report of Review of Dominion Voting Systems Democracy Suite 5.5”, Jun-20 2019, URL: https://www.sos.state.tx.us/elections/forms/sysexam/dominion-democracy-suite-5.5.pdf

[5] B. J. Mechler, “Voting System Examination of Dominion Voting Systems Democracy Suite 5.5”, Feb-15 2019, URL: https://www.sos.state.tx.us/elections/forms/sysexam/jan2019-mechler.pdf

[6] Democracy Suite System Change Notes, Version 5.5-A::155, Dec-13 2018

[7] Democracy Suite System Identification Guide, Version: 5.5-A::334, Dec-19 2018

[8] D-Suite 5.5-A (TX) Component List, Oct-18 2019

[9] United States Election Assistance Commission Certificate of Conformance Dominion Voting Systems Democracy Suite 5.5, EAC Certification Number DVS-DemSuite5.5, Sept-18 2018 URL: https://www.eac.gov/voting-equipment/democracy-suite-55/

[10] Democracy Suite ImageCast Central Functionality Description, Version 5.5-A::180, Dec-12 2018

[11] Democracy Suite ImageCast Precinct Functionality Description, Version 5.5-A::176, Dec-12 2018

[12] Democracy Suite ImageCast X System Operations Procedures, Version 5.5-A::85, Dec-12 2018

[13] Democracy Suite ImageCast X User Guide, Version 5.5-A::252, Dec-12 2018

[14] Democracy Suite System Security Specification, Version 5.5-A:563, Dec-12 2018

[15] Avalue HID-21V-BTX-A1R User Manual, Avalue Technology Inc., Feb-2 2018

[16] Texas Certification Response, Correspondence from Dominion Voting Systems to Charles Pinney, Oct-30 2019