Voting System Examination of Dominion Voting Systems Democracy Suite 5.5

Brian Mechler, Technical Examiner
Exam Dates: January 16-17, 2019
Report Date: February 15, 2019

1 Background

An examination of the Dominion Voting Systems Democracy Suite 5.5 was conducted at the Texas Secretary of State Elections Division offices on January 16-17, 2019. The Democracy Suite 5.5 is a comprehensive voting system which can consist of a subset of the following components:

- The Election Management System (EMS)
- The ImageCast Central (ICC)
- The ImageCast Precinct (ICP)
- The ImageCast X (ICX) Prime Direct-Recording Electronic (DRE) Voting Machine with Voter Verifiable Paper Audit Trail (VVPAT)
- ICX Prime Ballot Marking Device (BMD)
- ICX Classic BMD 15-Inch Display
- ICX Classic BMD 21-Inch Display

The Secretary of State obtained the software and firmware used in the Election Assistance Commission (EAC) certification directly from the EAC. Dominion personnel used those same files to perform installation of the software and firmware under the supervision of the technical examiners. The EAC certification includes tables that describe the voting system software components, voting system platforms, and hardware components [1]. In [2], Dominion provides instructions for the identification and verification of the certified products included in Democracy Suite 5.5 product group.

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 Election Management System (EMS) is a set of applications that handle the definition and management of elections. The EMS was presented in two different hardware configurations, Express and Standard.

2.1 Express Configuration

The EMS Express configuration is intended for smaller jurisdictions. All of the software components reside on a single PC workstation which runs on the Windows 10 Pro operating system (OS). The EMS Express workstation has mirrored, self-encrypting hard-drives. It is connected to the ImageCast Central via private LAN over a managed switch. The managed switch runs a DHCP server to serve a static pool of IP addresses. While data file contents are protected by encryption and signing, the network communication channel itself is not encrypted. Dominion strongly recommends that the LAN be air-gapped from public or other private networks.

2.1.1 Observations

The operating system and most of the third-party prerequisites were already installed prior to the examination. The technical examiners observed the installation and configuration of the following applications [3]:

- EMS Data Center Manager (DCM) – an application for back-end data center configuration
- EMS Application Server – a server application dedicated to executing long running processes
- EMS File System Service (FSS) – a client-side application that enables data movement across EMS applications and access to low-level interfaces with compact flash (CF) memory cards
- EMS Election Event Designer (EED) – a pre-voting application for designing election definitions
- EMS Results and Tally Reporting – a post-voting application for results acquisition, validation, tabulation, reporting, and publishing
- EMS Adjudication Services – services which support the Adjudication Client
- EMS Adjudication Client – application to review voter intent on ballots
- EMS Election Data Translator – application to import/export election data to/from election projects
- ImageCast Voter Activation (ICVA) – application used by poll workers to activate smart cards for voting sessions
- EMS Smart Card Helper Service – service to enable read/write access to smart cards
- EMS Audio Studio – application to record or add audio files to an election project

Overall, the EMS installation and configuration was not a user-friendly process. The DCM provided misleading information regarding the sharing permissions of the network attached storage (NAS). Various paths have to be manually set which can cause issues later on.

The use of some of the above applications was observed during the adjudication, tabulation, and reporting portions of the mock election. Election definitions were created prior to the exam using an older version of the EED. Dominion personnel explained that the difference in versions was minor and that there would be no compatibility issues; none were witnessed during the mock election.

During the tabulation portion of the mock election, there was a delay in tabulating ballots from the ICC because the path for the ballot images was not set right. Ideally, this type of issue would be caught during integration and test (I&T) prior to election day. However, it could be prevented in the first place if the software configuration allowed for default paths.

There were also setbacks with adjudication during the mock election. While troubleshooting the aforementioned ICC path issue, the adjudication services froze. Dominion personnel opted to force a stop and restart of the services. New adjudication databases were created after the restart of services. These did not include any of the adjudication decisions that had already been made. The databases resulting from the prior adjudication session were still on the drives, but they could not be merged with the new databases and the ballot adjudication had to begin again from scratch.

2.1.2 Concerns

There are two major concerns with the EMS Express: complexity of configuration and the inability to recover adjudication decisions after a crash of the adjudication services. The configuration and use of the EMS Express requires personnel with expertise in information technology (IT). These resources are not always available to smaller jurisdictions. In a real election, the inability to recover prior adjudication decisions could be very time consuming and costly to both jurisdictions and candidates.

There are a few minor bug fixes and feature improvements that could be made by Dominion. They should ensure that the configuration status provided by the DCM is accurate. There should be default path options offered during configuration and project creation. The adjudication client does a good job of visually indicating issues on the ballot images; however, it does not provide any feedback regarding whether a particular ballot issue has been addressed. As a user interface (UI) improvement, they should provide this feedback so that adjudicators do not accidentally skip issues on problem ballots.

2.1.3 Recommendation

Due to the two major concerns addressed in the previous section I do not recommend the EMS Express for use in elections in the State of Texas.

2.2 Standard Configuration

The EMS Standard configuration is intended for larger jurisdictions. Server-side software components reside on a Dell PowerEdge R640 server running a Windows Server 2012 R2 OS. Client-side software

components are installed on PC workstations running the Windows 10 Pro operating system (OS). The server is outfitted with redundant, self-encrypting hard-drives.

The server can connect to the ImageCast Central and client workstations via private LAN over a stand-alone switch provided by Dominion. The R640 server runs a DHCP server with a static pool of IP addresses. All extraneous network interface cards (NICs) are disabled by Dominion. While data file contents are protected by encryption and signing, the network communication channel itself is not encrypted. Dominion strongly recommends that the LAN be air-gapped from public or other private networks.

2.2.1 Observations

The installation of the EMS Standard configuration was observed by the technical examiners. The same software components as outlined in Section 2.1.1 were installed. The only difference was that the client-side applications were installed on the client PC workstation. The configuration was slightly more involved due to the need to define server and client host names within certain applications. Encryption keys generated by the server also had to be imported into the client workstations.

The EMS Standard configuration was not used in the mock election.

2.2.2 Concerns

The concerns expressed in Section 2.1.2 also apply to the EMS Standard since the issues were related to software, not hardware configuration

2.2.3 Recommendation

My recommendation for the EMS Standard is the same as the EMS Express as the major concerns are not tied to the specific EMS hardware configuration. I do not recommend the EMS Standard for use in elections in the State of Texas.

3 ImageCast Central Optical Scanner

The ICC is an all-in-one workstation that is part of both the EMS Express and Standard configurations. The only difference is the commercial off-the-shelf (COTS) scanner that comes with each configuration option. The scanner included with the EMS Standard has higher capacity and faster throughput. An iButton key for authentication is created in the EDD. The iButton key is needed to activate the ICC software. The ICC connects to the EMS server, and scanned ballots are saved locally and on the server.

3.1 Observations

The technical examiners witnessed the installation and configuration of the ICC for both EMS configurations. As part of the installation process, drivers were installed for the iButton key USB dongle. The EAC provided materials did not have the COTS scanner drivers included. Under the supervision of the technical examiners, Dominion personnel downloaded scanner drivers from the manufacturer's website. The driver used during EAC certification was 1.2 SP6; however, that driver

version was unavailable on the manufacturer's website. Driver version 1.2 SP9 was installed instead. There were no obvious issues related to using the newer driver version.

During the mock election the ICC performed as expected. The only minor issue was the error in path configuration with the EMS Express (see Section 2.1.1). The image quality of the scanned ballots was good.

3.2 Concerns

There were no major concerns with the ICC

3.3 Recommendation

The ICC in isolation would be suitable for use in Texas elections. However, it relies on the larger EMS ecosystem to function. Therefore, I cannot recommend that the ICC be used for elections in the State of Texas based on the findings in Section 2.

4 ImageCast Precinct

The ICP is an optical scan ballot counter intended to be operated at precinct polling places. It performs ballot scanning, ballot review, and tabulation functions. Dominion markets this device with two different styles of ballot box attachments: a collapsible corrugated plastic option and a hard plastic ballot box with integrated wheels and cable storage. The ICP has no internal memory; it uses two CF cards for redundant logging and tabulation. A backup battery is integrated into the scanning unit that is capable of operating for at least two hours.

4.1 Observations

Installation of the ICP firmware is performed using CF memory cards. On the first day of the examination, Dominion personnel were unable to complete the installation because they did not have the appropriate iButton admin key for authentication. An iButton with administrator privileges was shipped overnight, and the installation was completed on the second day of the exam. Even with the correct iButton key, the installation was not a smooth process. Dominion personnel seemed to be learning the process from the installation guide on-the-fly.

The ballot boxes had appropriate seals and locking mechanisms to prevent access to the ballot box interior and scanner. The scanner itself had appropriate seals and locking mechanisms to prevent access to the CF cards and other I/O ports. The corrugated plastic option has an emergency slot for ballot insertion should the scanning unit fail. The seal keeping the emergency slot covered is for one-time-use. Should the seal be broken, jurisdictions would have to purchase new ballot boxes prior to the next election.

During the mock election, the ICP exhibited problems with paper jams. In a real election, a poll worker would have to break a protective seal, lift the scanner up from ballot box, and retrieve the jammed

ballot from the bottom of the scanner. Neither security not secrecy of the ballot are preserved at this point.

It took longer than expected for the scanner to scan and process each ballot. One could easily envision inpatient voters accidentally abandoning their ballots by walking away too soon. The paper jam issue could also be exacerbated by voters inserting their ballots too soon after the previous ballot had been submitted.

During the adjudication portion of the mock election, write-in choices on the hand-filled ballots were not legible due to the scan quality of the ICP. In fact, even the computer printed portions of the ballot were not rendered clearly. Note that the ImageCast Central did not exhibit this behavior. The hand-filled ballots were filled out using ball-point pens. In [4], Dominion recommends using “black-ink, non-smear, quick-drying, non-flaking permanent marking pens”, i.e. Sharpies, to fill out ballots.

4.2 Concerns

The largest concern with the ICP is the tendency for paper jams. If a ballot has to be removed from the underside of the scanner to clear the jam, the privacy of the vote is not maintained. The poll worker would have to break a seal, log their action, and replace the seal. In an understaffed jurisdiction this could place a considerable strain on the operations of the polling place. Exposing the ballot box multiple times per day also adds an unnecessary security risk.

Another major concern is the quality of the scanned ballot images. Write-in selections written in ball-point pen were illegible. Even the scanned images of ballots generated by Dominion's own ballot marking devices were of poor quality. Requiring Sharpies to fill out ballots is an unnecessary constraint. Voters are not conditioned to a use such a narrow set of marking pens. Furthermore, Sharpie-style markers are likely to bleed though and corrupt a two-sided ballot, and it may be difficult to register write-in votes small enough to fit in the space provided.

4.3 Recommendations

Due to the frequency of paper jams, the ICP does not sufficiently preserve the secrecy of the ballot. The mechanism required to clear the paper jams does not keep the system safe from fraud or unauthorized manipulation. I do not recommend the ImageCast Precinct for use in elections in the State of Texas.

5 ImageCast-X Prime DRE With VVPAT

ImageCast-X refers generically to the set of COTS tablets Dominion uses as a platform for their DRE and BMD devices. Prime refers specifically to the aValue 21” Tablet (model HID-21V) running the Android 5.1 OS. During the examination, Dominion demonstrated the ICX Prime in both the BMD and DRE with VVPAT configurations. This Section focuses on the DRE with VVPAT configuration.

ACOS-6 smart cards are used to authenticate users as voters, poll workers, or technicians. The smart card technology is not proprietary to Dominion and jurisdictions could purchase them from other suppliers if needed. Smart cards are created using the ImageCast Voter Activation application which is

typically installed on a laptop at the polling place. Poll workers can manually authenticate voters in the event that there is a shortage of voter smart cards.

Voters use the ballot specified by the election definition to make their choices using Dominion's UI. Once the voter has cast their ballot, they are able to see a printout of their choices below a dynamically frosted window covering the VVPAT printer. Votes are tabulated on attached USB storage and in internal memory.

The VVPAT utilizes a thermal printer. The paper tape has a shelf life of about 22 months. The VVPAT printer can use a threaded pigtail for power and data if the jurisdiction finds it preferable to swap out whole printers instead of exposing results on the paper tape to install a new roll. Dominion estimates 200-300 votes can be cast per roll.

5.1 Observations

The technical examiners witnessed the installation and configuration of Dominion's proprietary ICX software. The Android 5.1 OS and other third-party prerequisites were already installed on the tablet.

A technician smart card was used to load the election definitions file from a USB thumb drive for the mock election.

The VVPAT prints in same order as votes cast. For the mock election there was only one ICX DRE-VVPAT in use. In a real election, multiple ICX DRE-VVPATs would need to be in use to preserve the secrecy of the ballot.

The UI for voting was fairly intuitive and easy to use. There were a few minor issues that might confuse or annoy a user. When casting votes, the navigation through the ballot pages moves horizontally, but when reviewing the ballot, the navigation controls scroll vertically. The vertical scroll buttons are also placed very close to other controls on the screen.

For the DRE-VVPAT configuration, the "Print Ballot" selection doesn't actually cause anything to print. Instead a warning appears on the screen which provides options to "Cast your ballot" or "Review your choices" (see Illustration 1). I had expected the VVPAT to activate at that time. The Dominion personnel were also initially confused by this. The VVPAT only prints the voter's selections once they have pressed the "Cast your ballot" button.

The voting UI did have one major problem with regard to straight party voting. It does not allow the voter to choose straight party and then opt out of voting in one of the partisan contests.

The aValue 21" Tablet has a set of doors to cover data and power ports. The doors are secured with a hasp fastener using a zip-tie seal. Even with the seal fully tightened in place, the door could be opened wide enough to access the data ports (see Illustration 2). With a caliper type tool a person could easily extract or insert USB or network devices. This is a serious security flaw.

During the mock election we disconnected the power pigtail to the VVPAT printer and then reconnected it. An error message appeared instructing the voter to get a poll worker. The error messages grew more dire and the system eventually shut itself off. Once power cycled, the tablet no longer recognized the smart card reader. The Dominion personnel did not know how to get it running

again. They eventually got it working by powering the tablet down, removing and replacing the battery, and then powering the unit back on. After the mock election was over, we tried to recreate the problem. In the later experiments, the tablet would suddenly power down every time the pigtail was reconnected.

After the mock election, we also experimented with removing and adding USB drives. If the polls were open, the tablet would immediately lock out voter access if any hardware was added or removed. A person with poll worker credentials or higher was required to resolved the issue. If a USB device was added while the tablet was powered down, no warnings appeared at startup and the poll worker could open the polls unaware of any change. A poll worker or technician would have to proactively query for attached devices in the settings menu to detect a change. Presumably the device addition would also appear in the ICX logs. Unfortunately, the logs provided by Dominion did not cover the time period when this experimentation was taking place.

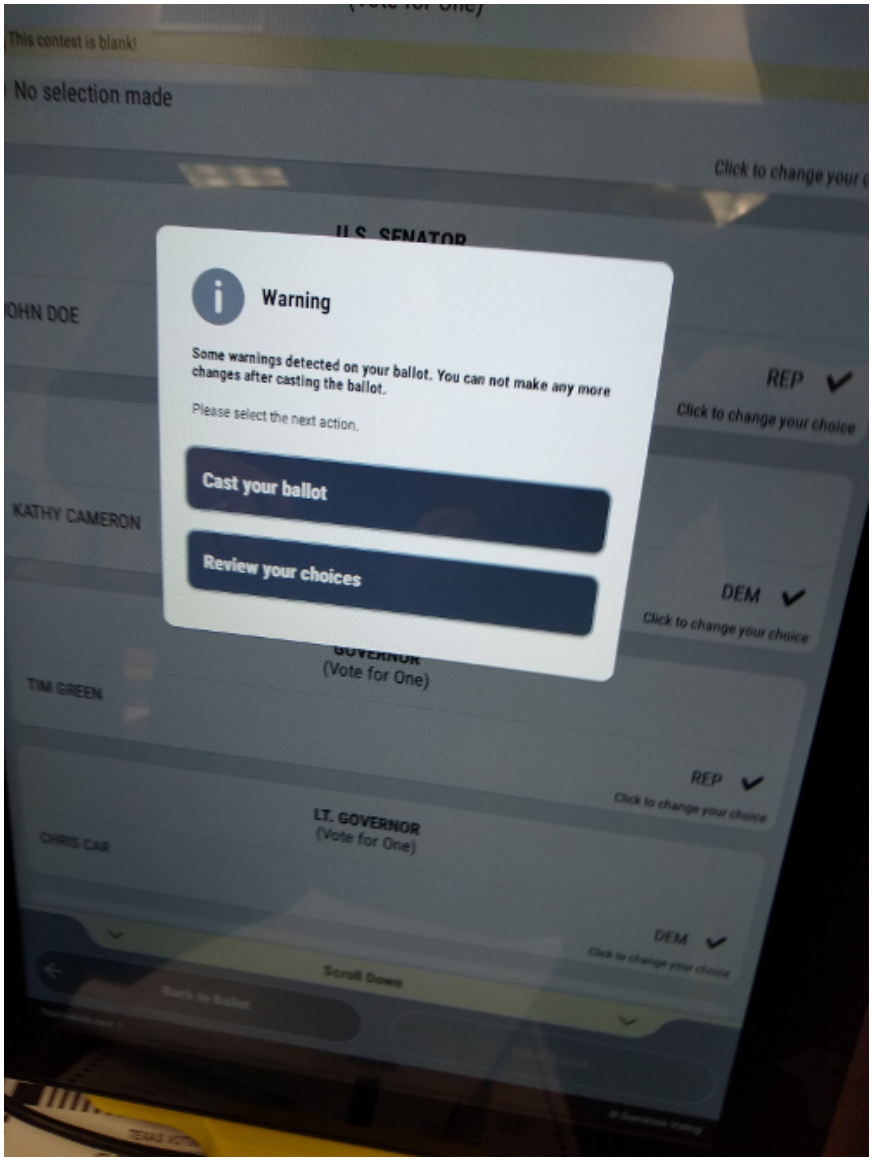

Illustration 1: Warning After "Print Ballot" Selected

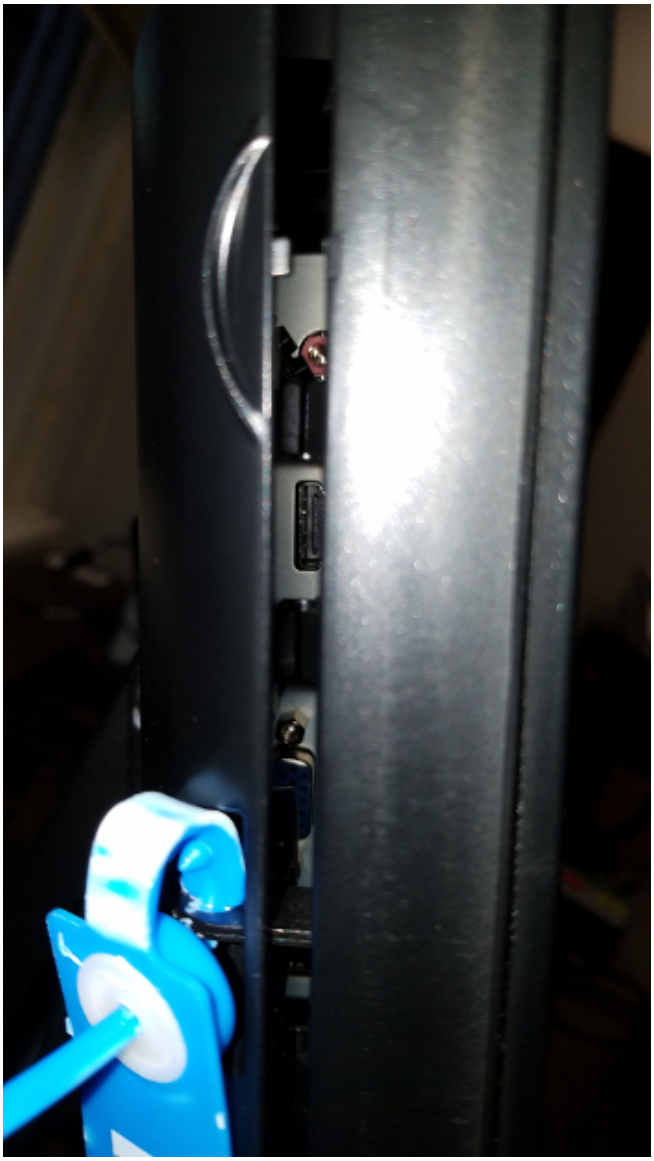

Illustration 2: Physical Access Despite Sealed Door

5.2 Concerns

The pigtail connector which supplies power from the tablet to the VVPAT printer exposes a major hardware flaw. Perhaps the unit under test was faulty. If not, the pigtail option with the VVPAT printer does not work as intended. It is not hot swappable.

The voting UI does not allow a voter to crossover vote from straight party to no selection in a partisan contest.

The doors covering data and power ports on the tablets do not provide sufficient protection using the suggested hasp and zip-tie fastener.

Given the above concern, a bad actor could add a USB device to the tablet while powered down that could remain undetected until after the election had ended.

5.3 Recommendations

The crossover voting issue is an interesting edge-case. I do not have enough legal expertise to say whether or not it meets the straight party voting requirements of the State of Texas. Nevertheless, the pig tail power connector to the VVPAT printer is not suitable for the purpose for which it is intended. The ICX Prime DRE with VVPAT is not safe from fraudulent or unauthorized manipulation due to insufficiently secured data ports in combination with the inability to detect hardware changes under certain circumstances. I do not recommend the ICX Prime DRE with VVPAT for use in elections in the State of Texas.

6 ImageCast-X Prime BMD

ImageCast-X refers generically to the set of COTS tablets Dominion uses as a platform for their DRE and BMD devices. Prime refers specifically to the aValue 21” Tablet (model HID-21V) running the Android 5.1 OS. During the examination, Dominion demonstrated the ICX Prime in both the BMD and DRE with VVPAT configurations. This Section focuses on the BMD configuration.

ACOS-6 smart cards are used to authenticate users as voters, poll workers, or technicians. The smart card technology is not proprietary to Dominion and jurisdictions could purchase them from other suppliers if needed. Smart cards are created using the ImageCast Voter Activation application which is typically installed on a laptop at the polling place. Poll workers can manually authenticate voters in the event that there is a shortage of voter smart cards.

Voters use the ballot specified by the election definition to make their choices using Dominion’s UI. Once the voter has reviewed their ballot, they print it out on an attached COTS printer. The ballot is then taken to the ICP for scanning and tabulation. The BMD devices under examination are not tabulators.

6.1 Observations

The technical examiners witnessed the installation and configuration of Dominion’s proprietary ICX software. The Android 5.1 OS and other third-party prerequisites were already installed on the tablet.

A technician smart card was used to load the election definitions file from a USB thumb drive for the mock election.

The voting UI is the same on all ICX devices; thus, the ICX Prime BMD has the same issue with crossover voting described in Section 5.1

The COTS tablet is the same model used in the ICX Prime DRE with VVPAT configuration. Therefore, the ICX Prime BMD suffers from the same issues with physical security.

6.2 Concerns

With the exception of the pigtail connector (which does not apply to this configuration), the concerns with the ICX Prime BMD are the same as described in Section 5.2

6.3 Recommendations

The ICX Prime BMD is not safe from fraudulent or unauthorized manipulation due to insufficiently secured data ports in combination with the inability to detect hardware changes under certain circumstances. I do not recommend the ICX Prime BMD for use in elections in the State of Texas.

7 ImageCast-X Classic 15-Inch BMD

ImageCast-X refers generically to the set of COTS tablets Dominion uses as a platform for their DRE and BMD devices. Classic 15-Inch refers specifically to the aValue 15” Tablet (model SID-15V) running the Android 4.4 OS.

ACOS-6 smart cards are used to authenticate users as voters, poll workers, or technicians. The smart card technology is not proprietary to Dominion and jurisdictions could purchase them from other suppliers if needed. Smart cards are created using the ImageCast Voter Activation application which is typically installed on a laptop at the polling place. Poll workers can manually authenticate voters in the event that there is a shortage of voter smart cards.

Voters use the ballot specified by the election definition to make their choices using Dominion’s UI. Once the voter has reviewed their ballot, they print it out on an attached COTS printer. The ballot is then taken to the ICP for scanning and tabulation. The BMD devices under examination are not tabulators.

7.1 Observations

The technical examiners witnessed the installation and configuration of Dominion’s proprietary ICX software. The Android 4.4 OS and other third-party prerequisites were already installed on the tablet. After the install, one of the examiners noticed the tablet was not in kiosk mode. Dominion personnel had to refer to their documentation to figure out how to properly configure the device. The accessibility test had to be delayed because the Google text-to-speech engine had not been installed on this tablet prior to the examination and Dominion personnel had no way of rectifying the issue in time.

A technician smart card was used to load the election definitions file from a USB thumb drive for the mock election.

The voting UI is the same on all ICX devices; thus, the ICX Classic 15-Inch BMD has the same issue with crossover voting described in Section 5.1

The screen size did not affect the presentation of the ballot in any obvious way.

The doors covering data and power ports on the aValue SID-15V provide sufficient physical security when sealed with the zip-tie provided by Dominion. As a result, the addition and removal of hardware devices was not tested on this model of tablet.

7.2 Concerns

The voting UI does not allow a voter to crossover vote from straight party to no selection in a partisan contest.

7.3 Recommendations

The crossover voting issue is an interesting edge-case. I do not have enough legal expertise to say whether or not it meets the straight party voting requirements of the State of Texas. Given that the ballot marking device must leverage the ICP for tabulation, I cannot recommend the ICX Classic 15-Inch BMD for use in elections in the State of Texas

8 ImageCast-X Classic 21-Inch BMD

ImageCast-X refers generically to the set of COTS tablets Dominion uses as a platform for their DRE and BMD devices. Classic 21-Inch refers specifically to the aValue 21” Tablet (model SID-21V) running the Android 4.4 OS.

8.1 Observations

The observations made regarding install, configuration, and use are the same as described in Section 7.1.

The doors covering data and power ports on the aValue SID-21V provide sufficient physical security when sealed with the zip-tie provided by Dominion. As a result, the addition and removal of hardware devices was not tested on this model of tablet.

8.2 Concerns

The voting UI does not allow a voter to crossover vote from straight party to no selection in a partisan contest.

8.3 Recommendations

The crossover voting issue is an interesting edge-case. I do not have enough legal expertise to say whether or not it meets the straight party voting requirements of the State of Texas. Given that the ballot marking device must leverage the ICP for tabulation, I cannot recommend the ICX Classic 21-Inch BMD for use in elections in the State of Texas

9 Conclusion

Dominion's lack of preparedness for the exam is not directly addressed as a major concern in any of the previous sections. Nevertheless, it is a concerning thread that runs throughout this report. The Dominion personnel at the exam were courteous, professional, and eager to answer our questions. However, there were too many incidents of missing or misconfigured hardware. I would expect that for a certification exam, Dominion would be very motivated to make sure everything went according to plan. I have serious concerns regarding the level of training Dominion personnel are receiving that make me question the quality of support jurisdictions would receive once a sale is made.

There was not a single component examined that I would recommend for use in elections in the State of Texas. Even devices that only had minor issues such as the ICC and ICX Classic BMDs require the use of either the EMS or ICP which did not receive my recommendation.

10 References

[1] 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/

[2] Democracy Suite System Identification Guide, Version: 5.5::327, Oct-16 2018

[3] Democracy Suite EMS Functional Description, Version: 5.5::351, Jan-16 2018

[4] Democracy Suite ImageCast Precinct Functionality Description, Version: 5.5::160, Sept-7 2017