Democracy Suite 5.5A

The Dominion Voting Systems Democracy Suite 5.5A election system (DVS) was re-examined in Austin on October 2-3, 2019. The same system was examined in January 2019, but failed to achieve certification at that time.

There were minor changes to the ICX firmware as outlined in the change notes. There were updates to the messaging for staigh-tparty crossover and the button text. Another firmware change was related to the removal of the ICX DRE configuration and it's VVPAT. None of the changes were material to the functionality or security of the system.

There were hardware changes. Notably, the ICX DRE and the ICX 15" tablet were removed. The hardware and software considered for certification for this examination are listed in the following table.

Proprietary/COTS Hardware/Software Components

Name	Version/Firmware #	Hardware
Election Management System (EMS)	5.5.12.1	Dell PowerEdge R640 Server
Adjudication Services (ADJ)	5.5.8.1	Dell Precision 3431 Workstation
ImageCast Central (ICC)	5.5.3.0002	Dell Optiplex 3050 AIO Workstation
ICC Scanner	DR-G1130 driver - version 1.2 SP6	Canon DR-G1130
ImageCast Precinct (ICP)	5.5.3-0002	PCOS-320C (proprietary device)
ICP Ballot Box	BOX-330A and BOX-341C	Stackable Molded Plastic and Foldable Coroplast Plastic
ImageCast X BMD	5.5.10.30 - Android 5.1	Avalue HID-21V-BTX (21.5 in. screen-Prime)
ICX BMD Printers	402dn	HP LaserJet
ICP Ballot Box	BOX-330A and BOX-341C	Stackable Molded Plastic and Foldable Coroplast Plastic

For a complete detailed listing of the hardware and software components used in the 5.5A system, please refer to the EAC certification Scope of Certification here.

Findings

The findings listed below are in addition to the findings reported on the first examination of the 5.5A system. Rather than repeat many of those here, the reader should review the report for the first examination. If a finding for the second examination of a particular issue is different from the first examination, it will be pointed out in this report. Some of the key findings are repeated in this report.

- The Technical Data Package (TDP) documentation provided appears to be accurate and complete. However, there is documentation for devices and other features which were not part of the Texas configuration. This could cause confusion for a jurisdiction.

- The pre-marked and the manually voted test ballots were recorded and tallied correctly.

- * There was a problem installing the Dominion software. A fresh install of the MS-Windows operating system software was required after the failure. Since the Dominion experts had difficulty installing their system, Dominion should be required to do the installation, or the installation program must be improved.

  Eventually, the software was built successfully. The release numbers on the devices and the EMS were verified to match the releases that were used for the EAC (U.S. Elections Assistance Commission) testing.

- There are methods a jurisdiction can use to verify the integrity of the software/firmware programs (using hash codes). The methods are described in the document *SystemIDGuide-5.5* for each device, and the EMS.

  The method that Dominion provides to generate the hashes for the EMS programs on the server should be improved. It would be preferable that a read-only CD is provided that has a program to both generate and compare the hashes. The hashes generated by the testing lab should also be on the CD. This would simplify the operation so a jurisdiction could easily validate the software before and after each election.

  * Because it is difficult to verify, a jurisdiction may choose not to before and after an election.

- The ICP precinct scanner can utilize either a plastic collapsible ballot box or a rolling plastic ballot box. They both have 3 bins: regular, write-in, and emergency. The ballot box styles have locks and two places to use security seals.

  The cardboard collapsible ballot box with the punch-out emergency slot was not included in this examination and should not be sold as part of the system.

- The ICC scanner jammed when scanning a batch. The batch must be redone whenever this occurs.

- No paper jams occurred on the ICP during the examination even though an attempt was made to cause one.

- * The messages on ICP display were visible only for about three seconds. One message said to press the “More” button for more information, but it quickly disappeared and the button could not be pressed. Messages should display until the user acknowledges.

- * It was not necessary to get the Canon drivers for the ICC from Canon site. No explanation was given why this was necessary for the first examination.

- The two ICX machines used in this examination were configured as BMD’s. The DRE configuration for an ICX was removed from the scope of certification.

- Straight-party voting can be turned off in the EMS when creating the election definition. This will be necessary when the law eliminating straight-party selection is in effect.

- The ICX BMD produces a printed summary ballot of the voter’s choices. The ballot 2D barcode is read by the ICP precinct scanner. A ballot image of the text of the voter choices is also created. The images can be used for an election audit.

- Voter activation can be done on the ICX BMD by a poll worker, or on a standalone laptop using a pollbook application to create the voter activation cards.

- The ICX BMD system warns a voter that there is a problem if the laser printer paper tray is ajar. The warning instructs the voter to seek help from a poll worker.

- The ICX BMD can be used for curbside voting on a cart. It has an arm that can be used to extend the tablet into a vehicle. * However, using it for curbside voting would be difficult and could damage the machine if the pathway to the curb is not very smooth.

- The ICP precinct scanner and ICX BMD can be used for a voting center. They are capable of providing all ballot styles. The collapsible ballot box is not appropriate for early voting because there is no cover to secure it at the end of the day.

- When voting on the ICX BMD during the examination, some screens had only one race; other screens had two races. Because of this, it was not clear that there was a second race on the page. It would be clearer if the layout was consistent (i.e. one race per screen). The ballot designer in the EMS has an option for this.

- * The ballot on the ICX BMD screens did not have the party affiliation next to the candidate names. It also did not translate the race names (i.e. Senator). The system is capable of providing both so it is not clear how this occurred.

  The audio ballot did have the race names which presumably came from the same data entered in the ballot designer. It is odd that the information was not displayed on the screen. An operator should be alerted to this by the ballot designer software even though it is likely to be discovered before election day.

- * The ethernet port is active on the ICX BMD during an election. It should be disabled when the machine is put into voting mode by the poll worker. This is an unnecessary open port during the voting period and could be used as an attack vector. An additional safeguard would be to automatically put the ICX in kiosk mode whenever the machine is open for voting.

- The ICP and ICC machines required an iButton dongle and the correct passcodes to access the poll worker and technician functions. Each type of iButton is programmed for a specific role.

  The ICX BMD machine requires a smart card and passcode. Session activation for the ICX is also done by a smart card. Each type of card is programmed for a specific role. Digital signatures are verified to match the signature in the election definition when the poll worker card or voter activation card is inserted.

- No problems were encountered during the adjudication testing. The wrong path error which happened during the previous examination did not occur. A better design would be to include all important paths in the election definition to eliminate human error.

  * During the previous examination, the system could not recover from the wrong path error and adjudication had to be redone. This is unacceptable. At the very least, the system should recover gracefully.

- * The Auditmark program keeps a record of all changes to a ballot during adjudication. Red boxes around a race indicates that the race needs to be adjudicated. The boxes were slightly offset from the race. It was necessary to look at the AuditMark view to verify the selection. This is unacceptable. The operator may not view the AuditMark record and adjudicate the wrong ballot and/or miss a ballot that need to be adjudicated.

- The images from the ICP scanner were much clearer and were easy to read during adjudication. Dominion offered that reason the ICP images from the previous exam were unreadable was that 1) they were compressed, or 2) the scanner was damaged. The system should not have an option to compressed images if it renders them unreadable. Also, it does not seem likely that the unreadable images were caused by a damaged scanner. * There was not a definitive root cause given for the problem, so it could occur again.

- Substantial training is essential to successful operation of the system. Dominion stated that training is customized for each customer. * The Dominion experts had difficulty operating the system at times, training and experience is critical to prevent errors during the election. Therefore, significant training should be included in a purchase contract.

- The server used for the examination was a rack mounted server. A rack mounted server would typically be in a room other than a room used for the central count. This could be a potential security risk since it is out of sight.

  A tower server can be purchased with the same internal chipset and disk storage as the rack mounted server used for the examination. This is preferred since it can operate in the same room as the scanner and workstations.

  The EMS software will run without the hardening script being applied. The following statement is from section 6.1.8 of the DemocracySuite System Security Specification document: “*No other component with the Democracy Suite platform is ever connected to a public or County network, and procedures for malicious software protection are specific and differ from regular IT systems” .* * However, the firewalls on the various central site machines are not configured as part of the hardening procedures. This is left to the jurisdiction and since many jurisdictions do not have the expertise, the machines could be vulnerable to a rogue operator on a machine if the election LAN is not confined to just the machines used for the election. The machines should be configured to only allow networking between the server, central scanners, and the workstations use for the election system. No internet access or other machines should have access to the LAN.

- The voting devices logs and ballot images, and the EMS logs contain the necessary information to audit an election.

  * However, when a second USB drive was inserted into the ICX BMD, it was not logged. It was explained that the second drive would not be read by the software and therefore was not a risk of infecting the machine. The second USB drive may be ignored by the election software, but a non-DVS drive should not be allowed as the disk could contain a rogue program that could access the election files directly.

  Text from the security document (4.4 Monitoring System Access and Use) states:
  From the initial state of the election project, until the deactivation state, the EMS system maintains an activity log within the EMS Database. This activity log contains every action that any of the users have performed within the system and represents a detailed audit log that can be analyzed and printed in the form of an audit report. The audit record information cannot be modified or permanently deleted ***using the EMS client applications.***

  * This implies that the log could be modified by a SQL tool. The integrity of the audit log is essential. Therefore, it is important that no database access tools, other than the election software, be installed on the EMS server. The database and the log files are encrypted which helps to prevent unauthorized, unlogged editing, but they could be deleted.

Conclusion

This examination went better overall than the last examination of the system, but many of the problems remain that caused it to fail certification previously. There have only been de minimis changes to the software since the previous examination. This is reflected by the same release number. The de minimis changes and the removal of the ICX DRE device did not correct all the problems stated in this and the previous report.

The Dominion experts still had problems installing the software. Therefore, installation cannot be assumed to be correct when installed by a jurisdiction. There are too many problems (see * above) installing and operating the system that cannot be mitigated by documentation and training. Dominion should implement the improvements that have been suggested. It is disappointing that the problems documented in the previous examination's report were not read, or not taken seriously.

The Dominion Democracy Suite 5.5A system does not meet the standards required by the Texas Election Code. I **do not** recommend that it be certified.

Tom Watson - Examiner