The State of Texas

Elections Division
P.O. Box 12060
Austin, Texas 78711-2060
www.sos.state.tx.us

Phone: 512-463-5650
Fax: 512-475-2811
Dial 7-1-1 For Relay Services
(800) 252-VOTE (8683)

Secretary of State

MEMORANDUM

TO: Keith Ingram, Director of Elections, Texas Secretary of State

FROM: Chuck Pinney, Staff Attorney, Elections Division, Texas Secretary of State

DATE: November 4, 2019

RE: Dominion Voting Systems – Democracy Suite 5.5-A Voting System Examination

In accordance with my appointment by the Texas Secretary of State as a voting system examiner under Tex. Elec. Code §122.067, I present my report on the voting system examination which took place on October 2-3, 2019, in the offices of the Texas Secretary of State at the James E. Rudder Building, 1019 Brazos, Austin, Texas 78701.

On October 2-3, 2019, the examiners appointed by the Texas Secretary of State and the Texas Attorney General examined Democracy Suite 5.5-A, a voting system that was presented by Dominion Voting Systems ("Dominion") for certification in Texas. The following hardware and software components were examined at the Office of the Secretary of State:

Component	Version	Previous Texas Certification Date
EMS – Election Management System	5.5.12.1	None
ADJ – Adjudication	5.5.8.1	None
ICC – ImageCast Central	5.5.3.0002	None
ICX – ImageCast X BMD	5.5.10.30	None
ICP – ImageCast Precinct	5.5.3-0002	None

For the reasons outlined below, I am unable to recommend that this system be certified by the Texas Secretary of State under Tex. Elec. Code §§122.031 and 122.039.

Background

Dominion Voting Systems previously sought certification in Texas for the Democracy Suite 5.5 voting system in January 2019. That certification was denied in June 2019.

The voting system that was the subject of this examination, Democracy Suite 5.5-A, was certified by the U.S. Election Assistance Commission ("EAC") on January 30, 2019.

Summary of the Examination

The examination of Democracy Suite 5.5-A took place on October 2-3, 2019.

The first day of the exam involved the installation of the software and firmware for Democracy Suite 5.5-A using of the trusted build provided to our office by the testing lab.

During the installation of the Adjudication software on the EMS server, the installation failed multiple times. As a result, the system needed to be fully wiped and required a full reinstallation of all EMS software, including the Windows operating system. The installation failed again on the first attempt after the full reinstallation, but succeeded on the second attempt.

Before the beginning of the vendor presentation on the second day of the exam, I conducted the accessibility testing and tested the visually impaired functions, the sip-and-puff controller, and the paddle controller. The system performed well during the accessibility testing and presented no issues.

On the second day of the exam, the vendor provided a presentation of the software and the updates involved in the current version of Democracy Suite. The vendor noted that the only difference between Democracy Suite 5.5 (which was denied certification in June 2019) and Democracy Suite 5.5-A was an update to an instruction relating to straight-party voting on the ICX Prime BMD. No other changes from Democracy Suite 5.5 were included in the update to 5.5-A.

After the vendor presentation, the examiners tested the equipment by voting a series of test ballots and comparing the results of those test ballots. The examiners also conducted additional testing on various components of the system.

Analysis

The standards for a voting system in Texas are outlined in Texas Election Code Chapter 122. Specifically, the system may only be certified for use in Texas if it satisfies each of an enumerated list of requirements contained in Texas Election Code §122.001. Because the system does not satisfy each of those requirements, I would recommend against certification of this system.

In the examination for Democracy Suite 5.5 that took place in January 2019, myself and the other examiners noted a number of issues that led to each of us recommending that certification for that system be denied. The system that we reviewed in this examination, Democracy Suite 5.5-A, did not contain any changes that addressed the issues identified in those examiner reports. The system that we reviewed in this examination was certified by the EAC on January 30, 2019, which was approximately two weeks before our examiner reports from the previous examination were completed on February 16, 2019. Therefore, it is impossible for this system to have addressed any issues in response to the issues raised in those examiner reports because this version was finalized and certified by the EAC before those reports were ever published.

Some of the issues we encountered in the previous exam could be attributed to errors in presentation or configuration in the previous exam and were not reproduced in this exam. The issue with image quality generated by the ImageCast Precinct in the previous exam did not occur in this exam, and the vendor indicated that the issue that occurred in the previous exam may have been caused by damage to that device in transit to the exam or due to the use of image compression settings that were not enabled in this exam. Similarly, the printer tray issue that occurred with the ICX Prime BMD in the previous exam did not occur in this exam, and the device properly provided an error message that allowed the poll worker to fix the printer tray issue without losing the voter's cast ballot.

However, many of the general concerns about the system's ability to be implemented by counties with low technical expertise due to the complexity of the configuration and installation process are still present. The fact that the only change between Democracy Suite 5.5 and Democracy Suite 5.5-A was a change to a straight-party instruction message indicates that these issues and other issues highlighted in the examiners' reports were not addressed in this version of the software.

Regardless of what occurred during the previous exam and the concerns that were raised during that process, there were several issues that occurred during this exam that support my recommendation against certification of this system:

- The installation process for the EMS software (including Adjudication) is incredibly complicated and is not intuitive for the user. The technician performed the install using the installation guide that was included in the vendor's documentation. That documentation provided guidance on how to perform the installation, but the design of the system and the documentation was not intuitive.

  The system required the technician to manually install every component of the system (including individual system fonts) in a very specific order, but the design of the installer makes this a fairly confusing process for the technician. For example, at one point, the technician is required to install the second item on the install list, then the first, then the third for the system in that exact sequence for the installation to function properly. This is a questionable design choice that is indicative of several similar choices that creates unnecessary complications that are likely to confuse users and result in incorrect installation of system components.

  During the installation the system also generated default file pathways which the user was required to change to a different pathway identified in the installation documentation. The vendor indicated that there was no situation in which the default pathway provided by the installer would be used. While this is a relatively minor issue, it raises questions as to why the system did not generate the correct pathway by default, or why the installer would generate an incorrect pathway instead of leaving the field blank. This is just another example of a design choice that is unintuitive and could lead to configuration errors during setup by a political jurisdiction.

- The installation of the Adjudication software failed on several occasions during the examination process. In an effort to address those failures, the technician referred to troubleshooting documentation and consulted with engineers from the vendor. These troubleshooting attempts included editing the system registries and other steps that could present issues for a user without substantial technical expertise. The vendor stated that the troubleshooting documentation used during this process was not part of the vendor's Technical Data Package and is an internal document.

  After the first few failures, the vendor chose to wipe the software and operating system off the server system and conduct a full reinstallation of the Windows operating system and EMS software. The installation failed again one more time after the full reinstallation, but succeeded on the second attempt. The system took approximately 10-15 minutes to complete the phase of the installation that had failed on previous attempts after the same amount of time.

  The vendor stated that this installation error occurred because a reboot step was skipped in the initial installation. The vendor also indicated that this part of the installation process takes a long time and that the system may have timed out during the previous attempts. The issues experienced in this part of the process by the vendor's own technical personnel raise concerns about the reliability of the system in general as well as the difficulty in installing and configuring this software.

- The ICX Prime BMD included an LED light to alert pollworkers to potential issues. That LED light was connected to the system via USB. During the examination process, one of the examiners was able to disconnect the LED light from the USB cable that connected it to the system without having to break any of the seals preventing physical access to the USB ports. The examiner was able to connect his cell phone to the voting machine using that exposed cable connection.

  It is unclear whether the system would have allowed any transferring of data or other malicious access to that device over that connection. The system did record that event in its audit logs, so there was at least a record of the incident occurring. However, it is concerning that the connection itself was available to expose the system to such access.

  The vendor recommended two possible forms of mitigation for this vulnerability, (1) that the connection between the LED light and the USB cable be sealed to prevent it from being disconnected, or (2) that the LED light be removed from the Texas configuration.

  If the system were certified, I would recommend that it be made conditional on the fact that this USB LED light or any similar device with an exposed connection cannot be used with the system.

- The ImageCast Precinct (ICP) has a few concerning issues. The firmware is installed using a 1 character pin code along with a physical technician key, and the pin code cannot be changed. While the physical key requirement alleviates part of the problem, it seems like an unnecessary security vulnerability to have such a rudimentary password requirement for a firmware installation.

The ICP also allows for the installation of firmware from prior versions of Democracy Suite which are not certified for use in Texas. This would theoretically allow a jurisdiction to install an uncertified version of the voting system during the firmware installation process. This feature should be removed, and any certification of this system should be made conditional on the vendor's removal of that feature through an administrative modification process before that device could be used in Texas elections.

The examiners also experienced an issue when trying to scan a ballot with an ambiguous mark through the ICP. The device correctly rejected the ballot, but the error message was only available while the ballot was still touching the portion of the scanner that catches the ballot, which only occurred in one of five tests. In the other tests, when the ballot was rejected the scanner pushed the ballot out so far that it was no longer touching that portion and the error message would disappear instantly. This design could create situations where voters' ballots are rejected without the voter having an opportunity to view the relevant error message and find out what needed to be corrected.

- The system does not provide a software solution to address the ballot numbering requirements of Texas law. If certification were granted for this system, it would have to be made conditional on the jurisdiction's use of hand-numbering devices or pre-printed ballot stock that complies with the ballot numbering requirements.

In theory, this system could be certified for use in Texas with a hefty list of conditions. However, there would still be significant concerns with the reliability of the system and the ability of Texas jurisdictions to configure and install the required software. Ultimately, I cannot recommend a system that would require a long list of conditions in order for a jurisdiction to adopt the system and still comply with Texas law and voting system standards.

The flaws and questionable design choices that were identified through this exam that indicate that the system is not suitable for the purpose for which it is intended and therefore cannot be certified for use in Texas under Texas Election Code 122.001(a)(2). In addition, the potential security vulnerabilities that were identified in the exam indicate that the system may not be safe from fraudulent or unauthorized manipulation, and therefore cannot be certified for use in Texas under Texas Election Code 122.001(a)(4).

Conclusion and Recommendation

For the reasons outlined above, I am unable to recommend certification of this system.

If the system is certified, then that certification will need to be made conditional based on the vendor's and the jurisdiction's compliance with several different conditions. However, the conditions that would need to be imposed are so numerous and affect so many fundamental aspects of the system that I am unable to recommend even a conditional certification of this system.