

BRANDON HURLEY

4122 Mapleridge Drive
Grapevine, Texas 76051
(817) 454-3142
brandon.hurley@outlook.com

September 21, 2020

Mr. Keith Ingram
Director of Elections
Texas Secretary of State
Elections Division
208 East 10th Street
Austin, Texas 78711

Re: Inspection of the Election Systems & Software's 6.1.1.0 System conducted on
August 21, 2020

Dear Mr. Ingram:

Pursuant to my appointment by the Texas Secretary of State as a voting systems examiner under TEXAS ELECTION CODE § 122.035, please allow this letter to serve as my report concerning the above referenced examination. On August 21, 2020, the appointed examiners and Secretary of State staff met with representatives of Election Systems & Software ("**ES&S**") via video conference to review the new ES&S voting system known as the "**EVS 6.1.1.0 System**".¹ The room used at the Secretary of State's offices for the examination was locked when no one was present and all inspection proceedings were broadcast live so all inspectors could watch the proceedings. Chuck Pinney from the Secretary of State's office was physically present with the ES&S officials during the examination.

The examiners observed the testing and presentation of above referenced software and equipment on August 21st. Prior to and after that inspection, I reviewed the written materials for the EVS 6.1.1.0 System. The presentation of the physical inspection and review of written materials show ES&S's compliance with the relevant provisions of the TEXAS ELECTION CODE and Texas Administrative Code related to the requirements for election machines and software.

The EVS 6.1.1.0 System is the next version of the ES&S Voting system originally numbered 6.1.0.0. rolled out in January of 2020. The limited changes in the EVS 6.1.1.0 System from the previous version of the EVS 6.1.0.0. System are in the ballot adjudication functions of the system and a misalignment issue on the adjudication screen and some security updates. No other new physical hardware or firmware were changed from the previous EVS 6.1.0.0 System

¹ Another ES&S System numbered 6.0.3.0 was simultaneously examined on the same day, but will be addressed in a separate report.

ACCESSIBILITY TESTING

Because there were no changes to any of the hardware or software related to accessibility use of the machines in the EVS 6.1.1.0 System, the examiners and Secretary of State staff did not perform any accessibility testing of the EVS 6.1.1.0 System.

TESTING OF HARDWARE AND SOFTWARE

Prior the beginning of the exam, ES&S completed the loading and installation of the EVS 6.1.1.0 System. The hash validation files were later sent to the examiners for review.

ES&S provided the examiners an overview of the EVS 6.1.1.0 System. There was an initial discussion about the adjudication function changes that were the majority of the upgrades in the EVS 6.1.1.0 System. A discussion concerning new security features (in particular the ability to disable the automatic password reset function) also occurred.

Later, Chuck Pinney of the Secretary of State's office ran a script of sample ballots to test each piece of equipment and software for security, functionality and accuracy. The script of ballots were tabulated and sorted with the election software of the EVS 6.1.1.0 System. The results of the tabulation matched the verified voting numbers from the Secretary's office. In addition, ES&S officials and the examiners reviewed the new adjudication features of the System.

OBSERVATIONS

1. Each of the separate pieces of hardware and software examined met the listed requirements of the TEXAS ELECTION CODE and TEXAS ADMINISTRATIVE CODE.
2. The changes to address the adjudication issues appeared to function as intended.
3. The additional security issues also seemed to work as intended; however, there was some question about whether the modification of the password expiration is a good idea if it can last indefinitely.

RECOMMENDATION

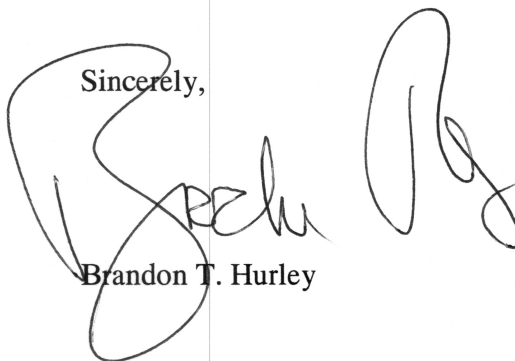
Based on the foregoing observations and my examination of the EVS 6.1.1.0 System, its accompanying literature and the representations made by ES&S officials both in its literature and at the examination, I recommend that the EVS 6.1.1.0 System be certified as compliant with the requirements of the TEXAS ELECTION CODE and the TEXAS ADMINISTRATIVE CODE.

This report should not be construed as a tacit or implied comment on any of the technical aspects of the EVS 6.1.1.0 System except as expressly stated herein. In the event any of the equipment, software or security devices examined are altered, changed or decertified by any accrediting agency (other than a "minor modification qualified for administrative certification

process” as that term is defined in § 81.65 of the Texas Administrative Code), this report should be considered withdrawn.

Thank you for the opportunity to serve as an examiner and participate in this important process that protects the integrity of Texas’ voting systems.

Sincerely,

A handwritten signature in black ink, appearing to read "Brandon T. Hurley", written over the printed name.

Brandon T. Hurley

Voting System Examination of Election Systems & Software EVS 6.1.1.0

Brian Mechler, Technical Examiner

Exam Dates: August 21, 2020

Report Date: September 20, 2020

1 Background

An examination of the Election Systems & Software (ES&S) EVS 6.1.1.0 voting system was conducted at the Texas Secretary of State Elections Division offices on August 21, 2020. EVS 6.1.1.0 is a comprehensive voting system which can consist of a subset of the following components [1][2][3]:

- Electionware - a suite of end-to-end election management software applications
- ExpressVote Previewer – a ballot preview utility
- PaperBallot – a ballot layout editor
- Event Log Service – a service which monitors and logs users’ interactions with the Election Management System (EMS)
- Removable Media Service - a utility that runs in the background of the Windows operating system used for media validation purposes
- ExpressTouch - a direct recording electronic (DRE) voting device which supports electronic vote capture (for use in Texas only as a curbside voting device)
- ExpressVote XL - a ballot marking device (BMD) that provides a large-format touch screen interface and integrated thermal printer
- ExpressVote (HW 1.0 & 2.1) - a BMD that provides a touch screen interface and printer
- DS200 - a digital scanner and tabulator for use in the polling place
- DS450 - a central scanner and tabulator
- DS850 - a central scanner and tabulator with increased speed compared to the DS450
- ExpressLink - a standalone application that interfaces with voter registration systems (e.g. electronic pollbooks) and the ExpressVote Activation Card Printer
- ExpressVote Activation Card Printer - a small thermal printer used to print the ballot activation code on a vote summary card
- Toolbox – a software suite run on non-EMS workstations

Configuration options are presented in detail in [3]. The Election Assistance Commission (EAC) certification includes tables that describe in detail the voting system software components, voting system platforms, hardware components, and system limits [2].

Due to the COVID-19 pandemic, some of the examiners, including myself, participated in the exam remotely using a video teleconferencing system. This exam was conducted in tandem with an exam of EVS 6.0.3.0 which will be covered in a separate report. A one day exam was sufficient due to the fact that 6.0.3.0 and 6.1.1.0 are software-only updates relative to their previously certified baselines.

The Secretary of State obtained the software and firmware images used in the EAC certification directly from the EAC Voting System Test Laboratory (VSTL). ES&S personnel used those same files to perform installation under the supervision of the examiners. In [4]-[11], ES&S provides instructions for the identification and verification of the components included in EVS 6.1.1.0.

The examination also consisted of vendor presentations, a mock election, and a free-form session where examiners could ask follow-up questions.

There were no accessibility tests performed during this exam. There have been no updates to the voter facing hardware or firmware since the previously certified EVS 6.1.0.0. At the time this report was submitted, the certification documentation for EVS 6.1.0.0 was not yet hosted on the Texas Secretary of State website. Documentation of this nature can typically be found at:

https://www.sos.texas.gov/elections/laws/ess_system.shtml

2 Election Management System

The election management system (EMS) is a set of servers, workstations, and software which provides an end-to-end solution for jurisdictions to define, manage, configure, export, and tabulate elections. The following subsections will describe the hardware workstations and servers, media, software, and observations from the exam.

2.1 Hardware

EMS workstations can be standalone or act as a client connected to a server. Client and standalone workstations are all Dell products. The following models have been certified by the EAC for use with EVS 6.1.1.0:

- Latitude 5580
- OptiPlex 5040, 5050, and 7020

The client/standalone workstations run 64-bit Windows 10 Enterprise LTSC SP1 as the operating system (OS). The server certified by the EAC for use with EVS 6.1.1.0 can be a Dell PowerEdge T430 or T630. The server hardware runs 64-bit Windows Server 2016 as its OS.

When election hardware is networked together it must be done in a closed network environment. In [12], ES&S defines a closed network environment as consisting of “a stand-alone server used for a specific purpose, such as an Election Management System (EMS) like Electionware, with restricted

access to specific workstations and no connection to any other network. Only EMS components are allowed on this network, and any voting system component at a precinct voting site is forbidden from being connected.”

Best practices for physically securing EMS workstation and server hardware are found in [13].

The only change to EMS hardware is “the option for increased physical RAM on the EMS in the client, server and/or standalone configurations (optional).” EVS also “increased the amount of virtual RAM available to Electionware (optional).” [14]

2.2 Media

There were no changes to the format or use of media between EVS 6.1.0.0 and 6.1.1.0.

2.3 Software

Electionware is the suite of ES&S software modules used for administering elections. There were only minimal changes to Electionware between EVS 6.1.0.0 and 6.1.1.0 [14].

- “Added critical Windows security updates available at the time of certification testing.”
- “Included the recommended Arial fonts”
- “Provided a method for modifying the Microsoft Windows password policy to not expire on the EMS (optional).”
- “Added an updated JAR file to prevent relocated JAI classes from loading. This prevents the Internal Error displayed when attempting to view ExpressVote XL write-in images.”
- “Adjusted misalignment of write-in snippets for ExpressVote XL and ExpressVote vote summary cards so they reflect the correct ballot image.”
- “Provided an additional internal Postgres system logging message to enhance the security and performance of the database.”
- “Provided an additional user logging message to enhance the transparency and security of the database. This additional logging is included within the Reporting module to assist users during ballot adjudication.”
- “Removed all empty entries in the CVR export report.”

2.4 Observations

There were no issues related to the EMS during the mock election and subsequent tabulation and reporting.

The change note that mentions the misalignment of a write-in snippet refers to an issue with the adjudication UI. The voter’s write-in choice is correctly printed on the ballot. ES&S told examiners that supplemental documentation with a work-around was provided to jurisdictions using affected versions of EVS. I recommend jurisdictions reach out to ES&S to ensure they have received these documents.

In 6.1.1.0, the option is provided to set EMS passwords that don't expire. Jurisdictions should never take advantage of this option. The "Election Security Best Practices Guide" published by the Texas Secretary of State recommends forced updates of passwords every 90 days as a priority best practice [15].

3 Voting Devices

ES&S is requesting certification of four different voting devices (one DRE and three BMDs). All devices employ touchscreens and can be configured with accessibility peripherals. The hardware and firmware of the ExpressTouch, ExpressVote XL, and ExpressVote (HW 1.0 and 2.1) remains unchanged since EVS 6.1.0.0. Best practices for physically securing these devices can be found in [13].

3.1 Observations

Examiners observed the installation of firmware, Election Qualification Codes (EQCs), and election definitions on the ExpressVote HW 2.1. No other voting devices were used in the mock election. Refer to EVS 6.1.0.0 exam reports for further detail on the user experience of ES&S voting devices. Because there were no updates to these devices in this version of EVS, concerns raised by examiners during the EVS 6.1.0.0 exam still remain.

During the mock election, no issues were observed with the casting of ballots, tabulation of votes, or reporting of results.

4 Scanners

ES&S is requesting certification of three different scanning devices in EVS 6.1.1.0; the DS200 which is designed as a precinct scanner, and the DS450 and DS850 which are both central scanners. All scanners are capable of scanning both hand-marked paper ballots and machine-marked vote summary cards. The hardware and firmware of the DS200, DS450, and DS850 remains unchanged since EVS 6.1.0.0. Best practices for physically securing these devices can be found in [13].

4.1 Observations

Only the DS200 and DS850 were used to scan and tabulate ballots during the mock election. No issues were observed with scan quality, accuracy, or reliability. The devices did not appear prone to jams or other slow downs.

Refer to EVS 6.1.0.0 exam reports for additional detail on ES&S scanning devices. Because there were no updates to these devices in this version of EVS, any concerns raised by examiners during the EVS 6.1.0.0 exam still remain.

5 ExpressLink and ExpressVote Activation Card Printer

These components are not within the scope of this certification exam nor are they a part of the EAC certification. Nevertheless, they are listed as part of the Form 100 [1], and this section will briefly describe their purpose.

The ExpressLink is a standalone software application that interfaces with electronic pollbooks and the ExpressVote Activation Card Printer. The ExpressVote Activation Card Printer prints a bar code at the top of a vote summary card that encodes the ballot style that the voter should receive. The voter can then use the pre-printed vote summary card to activate their own voting session and receive the correct touchscreen ballot on ExpressVote and ExpressVote XL BMDs.

The ExpressVote Activation Card Printer also provides a mechanism for marking a ballot as provisional and preventing it from being prematurely scanned and accepted as a regular ballot by the precinct scanner.

5.1 Observations

Neither the ExpressLink nor the ExpressVote Activation Card printer were demonstrated during the exam.

Based on the functionality described in the ES&S technical data package, large polling places may benefit from these devices since they will likely reduce the workload on already busy poll workers and reduce voter waiting times.

6 Toolbox

This component is not within the scope of this certification exam nor is it a part of the EAC certification. Toolbox is designed to run on the Windows 7 operating system, and must be run on a host separate from the EMS closed network environment.

The Toolbox has three main components [16]:

- Test Deck – used to create test decks for use in logic and accuracy (L&A) testing
- Text to Speech – used to create audio playback files for use with ADA-compliant devices
- Media Restore – used to securely clear data from ES&S Delkin USB media and reformat media to the FAT32 file system
- Data Conversion - used to convert exported election data to formats compatible with Electionware

6.1 Observations

The Test Deck, Text to Speech, and Data Conversion modules were not demonstrated during the exam. Media Restore was used to create election media for the mock election. No issues with its use were observed.

7 Hash Verification Issues

EVS 6.1.1.0 (as well as other EVS versions) has multiple issues with its prescribed hash verification procedures.

Hash verification is the process that is used to ensure that the software and/or firmware of a voting system matches exactly with what was certified by the EAC. A hash is the output of a cryptographic function run on a file or program executable. If a file or program is changed in any way, it will produce a different hash result.

Hash verification is a critical component of acceptance testing to ensure the proper delivery of voting systems. In Election Advisory No. 2019-23, jurisdictions are directed to perform a complete system validation which includes the verification of hashes [17]. Though not yet mandated by the State of Texas, I believe that jurisdictions should perform hash verification on all voting system equipment before and after each election.

7.1 ES&S Personnel Performing Hash Verification

It was disclosed during the concurrent EVS 6.0.3.0 exam that ES&S personnel have performed the hash verification process instead of their customers. Jurisdictions should always perform this process themselves. To have the vendor perform a required component of acceptance testing creates, at best, a conflict of interest. The Secretary of State Elections Division has taken an action to work with ES&S and their Texas customers to better define their roles and responsibilities with respect to acceptance testing and hash verification.

7.2 Bug in Hash Verification Script

The hash verification process involves the creation of two USB thumb drives; one containing the system export data of the system to be verified and the other containing the verification scripts and trusted hash file. A host separate from the EMS is booted using a live Ubuntu DVD. The live Ubuntu DVD allows the user to run the Linux OS from the DVD without altering the non-volatile memory of the host computer. The export and scripting media are then mounted and a set of scripts are run to configure the user's environment, compute hashes of the system export data, and compare those hashes with the trusted hash file.

While working through this process, I initially overlooked the instruction to add the trusted hash file to the scripting media. Despite the missing trusted hash file, the verification script erroneously reported that the exported hashes matched the trusted hashes.

```
$ ./DS200-VerifyHash.sh DS200-TxSos6110ExamAug2020
diff: HashTrusted-DS200.txt: No such file or directory

DS200 firmware matches Trusted Hash File.
Hash File, DS200-TxSos6110ExamAug2020_Hash.txt, copied to output
```

Though this example shows the output of the DS200 verification script, the bug is also present in the verification scripts for the DS450, DS850, ExpressTouch, ExpressVote (HW 1.0 and 2.1), and ExpressVote XL devices.

ES&S's documentation states [5]:

If the DS200 firmware matches the Trusted Hash File, the following message will be displayed.

```
DS200 firmware matches Trusted Hash File.  
Hash File, DS200-Identification_Hash.txt, copied to output.
```

Where, DS200-Identification is the name used to identify the DS200 for which the verification reports were generated.

If the DS200 firmware does not match the Trusted Hash File, the following message will be displayed.

For details, see Appendix F Results when DS200 Firmware Does Not Match.

```
DS200 firmware DOES NOT MATCH Trusted Hash File!  
Difference report, DS200-Identification_Report.txt, copied to output.  
Hash File, DS200-Identification_Hash.txt, copied to output.
```

It could be very easy for personnel performing hash verification to assume a good result when, in actuality, no hash comparisons were made. Within their scripts, ES&S should have performed explicit checks on the existence of the two files being compared; failing loudly if either does not exist.

A common open-source application, diff, is used to compare the hash files. In order to determine if they match, ES&S only examines the text that diff writes to the standard output stream. In doing so they miss the error messages written to the standard error stream. In general, it is bad coding practice to condition a critical decision on the written output of a 3rd party application. The reason is that the developer would have to know every possible output (intended or otherwise) in order to craft a reliable conditional.

A more robust way to check the result of the diff call would have been to query its exit status. The diff manual clearly defines the meaning of its exit status as [18], “0 if inputs are the same, 1 if different, 2 if trouble.”

It is my opinion that this bug (in addition to the overall process) indicates that ES&S has not developed their hash verification process with sufficient care, quality assurance, and concern for usability.

When jurisdictions run their hash verification, they should carefully examine the media they create for correctness and carefully monitor the output of the verification scripts to make sure no error messages are printed along with text claiming a successful result.

Texas' Election Security Best Practices Guide [15] states that as a priority best practice jurisdictions should "ensure that every election function from ballot programming to Election Night Reporting uses a two-person verification method in which one person performs the task and a second person witnesses and verifies the accuracy and integrity of the result." It is not clear to me whether this guidance includes the hash verification process or acceptance testing activities, but it should.

7.3 Lack of Traceability in Procedure for EMS Hash Verification

The hash verification document for the EMS host(s) describes a procedure where the user creates a set of "golden" hashes immediately after installation [4]. Subsequent checks are only verified against this "golden" set. This procedure, as written, only verifies that the EMS has not been altered since the first installation; it is not traceable to the hashes generated by the EAC. ES&S should document a procedure that jurisdictions can use to verify EMS hashes against those created by the EAC.

8 Conclusions

The ES&S hash verification process has been a growing issue of concern over the past few certification exams. In this exam, their customer relations with regard to this process have also become a concern. At this point, these issues have been communicated in detail to ES&S. I ***will not*** recommend certification of future ES&S releases unless they make substantial improvements to the ease-of-use, reliability, and traceability of their hash verification process.

As a mitigation for EVS 6.1.1.0 and past versions of EVS, I strongly recommend jurisdictions perform hash verification for themselves using a two-person verification method as described in Texas' Election Security Best Practices Guide.

With appropriate procedures in place, EVS 6.1.1.0 is a comprehensive voting system that is secure, accurate, and easy for the voter to use. ES&S's responses to the Voting System Certification Form 101 are truthful and adequate [19]. The system tabulated and reported results accurately during the mock election portion of the exam.

I recommend certification of EVS 6.1.1.0.

9 References

- [1] Application for Texas Certification of Voting System – Form 100, Election Systems & Software, ES&S EVS 6.1.1.0
- [2] United States Election Assistance Commission Certificate of Conformance, ES&S EVS 6.1.1.0, EAC Certification Number: ESSEVS6110, Jul-27 2020
URL: <https://www.eac.gov/voting-equipment/evs-6110>
- [3] System Overview, ES&S Voting System 6.1.1.0, Document Revision 1.2, Document ID ESSSYS_6'1'1'0_D_SYSOVR
- [4] Verification Procedure: Election Management System, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_EMS
- [5] Verification Procedure: DS200 Precinct Scanner and Tabulator, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_DS200
- [6] Verification Procedure: DS450 High-Throughput Scanner and Tabulator, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_DS450
- [7] Verification Procedure: DS850 High-Speed Scanner and Tabulator, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_DS850
- [8] Verification Procedure: ExpressTouch, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_ETOUCH
- [9] Verification Procedure: ExpressVote Hardware 1.0, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_EVOTE_HW1'0
- [10] Verification Procedure: ExpressVote Hardware 2.1, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_EVOTE_HW2'1
- [11] Verification Procedure: ExpressVote XL, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_D_VERPROC_EVOTEXL
- [12] Electionware Vol. I: Administrator Guide, Software Version 6.0.1.0, Revision 1.0, March 2020
- [13] Best Practices for Physically Securing ES&S Equipment, ES&S Voting System Security, Document Revision 1.0, Document ID ESSSYS_6'1'1'0_SPC_SECBESTPRACT
- [14] System Change Notes, ES&S Voting System 6.1.1.0, Document Revision 1.2, Document ID ESSSYS_6'1'1'0_D_CHANGENOTES
- [15] Election Security Best Practices Guide, Texas Secretary of State Elections Division, April 2020, URL: <https://www.sos.texas.gov/elections/forms/election-security-best-practices.pdf>

- [16] Electionware Toolbox User Guide, Software Version 4.0.0.0, Document ID EW_Toolbox_4'0'0'0_SOP
- [17] K. Ingram, Director of Elections, Electronic Voting System Procedures Advisory, Election Advisory No. 2019-23, Oct-23 2019, URL: <https://www.sos.texas.gov/elections/laws/advisory2019-23.shtml>
- [18] <http://manpages.ubuntu.com/manpages/xenial/man1/diff.1.html>
- [19] Voting System Certification – Form 101, EVS 6.1.1.0

The State of Texas

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



Ruth R. Hughs
Secretary of State

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

MEMORANDUM

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

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

DATE: September 21, 2020

RE: Election Systems & Software – EVS 6.1.1.0 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 August 21, 2020, in the offices of the Texas Secretary of State at the James E. Rudder Building, 1019 Brazos, Austin, Texas 78701.

On August 21, 2020, the examiners appointed by the Texas Secretary of State and the Texas Attorney General examined EVS 6.1.1.0, a voting system that was presented by Election Systems & Software (“ES&S”) 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 |
|-------------------------------------|----------|-----------------------------------|
| ExpressTouch | 1.0.3.0 | 4/24/2020 |
| DS200 | 2.30.0.0 | 4/24/2020 |
| DS450 | 3.4.0.0 | 4/24/2020 |
| DS850 | 3.4.0.0 | 4/24/2020 |
| ExpressVote (HW 1.0) | 4.0.0.0 | 4/24/2020 |
| ExpressVote (HW 2.1) | 4.0.0.0 | 4/24/2020 |
| ExpressVote XL | 1.0.3.0 | 4/24/2020 |
| ElectionWare | 6.0.1.0 | 4/24/2020 |
| ExpressLink | 2.0.0.0 | 4/24/2020 |
| Event Log Service | 2.0.0.0 | 4/24/2020 |
| ExpressVote Activation Card Printer | N/A | 4/24/2020 |

| | | |
|-------------------------|---------|-----------|
| ExpressVote Previewer | 4.0.0.0 | 4/24/2020 |
| PaperBallot | 6.0.0.0 | 4/24/2020 |
| Removable Media Service | 2.0.0.0 | 4/24/2020 |
| Toolbox | 4.0.0.0 | 4/24/2020 |

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

Background

ES&S previously received certification in Texas for the Unity voting system and previous versions of EVS. The most recent version of their software, EVS 6.1.0.0, was presented by ES&S in January 2020, and was certified in April 2020.

The voting system that was the subject of this examination, EVS 6.1.1.0, was certified by the U.S. Election Assistance Commission (“EAC”) on July 27, 2020.

Summary of the Examination

The examination of EVS 6.1.1.0 took place on August 21, 2020. That examination was conducted alongside the examination of EVS 6.0.3.0, which will be covered in a separate report.

Due to health concerns relating to COVID-19, a number of accommodations were required in order to comply with social distancing and protective gear recommendations from federal and state authorities. The examination was conducted at the Office of the Secretary of State, and both myself and Lesley French of the Texas Attorney General’s Office attended the examination as in-person examiners. The other examiners were able to participate remotely in the exam process via a live video conference that allowed them to watch the other examiners’ interactions with the equipment and ask questions to the in-person examiners and the vendor.

The exam began with the installation of the software and firmware for EVS 6.1.1.0 off of the trusted build provided to our office by the testing lab, followed by the vendor’s presentation of the software and the updates involved in the current version of EVS.

After the vendor presentation, the in-person examiners tested the equipment by voting a series of test ballots and comparing the results of those test ballots. The examiners also asked questions of the vendor regarding various components of the system and the nature of the updates included in this version of the system.

This version of the system did not involve any firmware changes to any of the hardware involved in this system, and only included changes to the election management system and the Electionware software. Because the firmware on those voting devices did not change, there was no accessibility testing conducted for EVS 6.1.1.0. My opinions on the accessibility features of

the firmware versions that are used on those voting devices for this system can be found in my report for the EVS 6.1.0.0 exam.

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 satisfies each of those requirements, I would recommend that this system be certified.

In general, EVS 6.1.1.0 is an excellent voting system that operates efficiently and effectively. The technical examiners identified concerns regarding the complexity of the hash validation process for this system and regarding the password reset requirements authorized by the system. Those concerns do not affect the reliability, accuracy, or security of the system if proper procedures are followed. I would recommend that the vendor make adjustments to these procedures based on the feedback of the examiners.

Hash Validation Procedures

In this exam and in the EVS 6.1.0.0 exam, the technical examiners noted that the process for conducting the hash validation of this system was overly complicated and difficult to understand. This procedure should be straightforward and simple enough that a jurisdiction with limited technical expertise would be able to conduct that process using the procedures provided by the vendor without requiring vendor technicians to facilitate that process for them.

The technical examiners provided detailed guidance in their reports providing specific instructions for how the vendor can improve their hash validation process for future systems. I would strongly recommend that the vendor review that guidance and implement those suggestions before their next system is presented for certification in Texas.

Password Reset Requirements

This version of the system allows the jurisdiction to customize the timeframe in which a password reset is required for users in the system. In EVS 6.1.1.0, the jurisdiction has the option of setting this requirement in a way that the passwords never expire. I would strongly recommend that jurisdictions not take advantage of this option. The Secretary of State's Office has published an Election Security Best Practices Guide that recommends forced updates of passwords every 90 days. Jurisdictions should follow those best practices recommendations rather than using this functionality offered by the system.

Conclusion and Recommendation

Because EVS 6.1.1.0 is an effective, highly usable voting system that complies with the necessary requirements for a voting system under Texas law, I would recommend certification of this system.

Voting System Examination Election Systems & Software (ES&S)

Prepared for the
Secretary of State of Texas

James Sneeringer, Ph.D.
Designee of the Attorney General

This report conveys the opinions of the Attorney General's designee from an examination of the equipment listed, pursuant to Title 9, Chapter 122 of the Texas Election Code, section 122.036(b).

Examination Date August 21, 2020

Report Date August 25, 2020

Examination of ES&S Voting System (EVS) 6.1.1.0

EAC Certification Number: ESSEVS6110

| Components Examined | Version |
|-------------------------------------|----------------|
| ExpressTouch | 1.0.3.0 |
| DS200 Precinct Ballot Counter | 2.30.0.0 |
| DS450 Central Scanner and Tabulator | 3.4.0.0 |
| DS850 Central Scanner and Tabulator | 3.4.0.0 |
| ExpressVote, HW v. 1.0 | 4.0.0.0 |
| ExpressVote, HW v. 2.1 | 4.0.0.0 |
| ExpressVote XL | 1.0.3.0 |
| Electionware | 6.0.1.0 |
| ExpressLink | 2.0.0.0 |
| Event Log Service | 2.0.0.0 |
| ExpressVote Activation Card Printer | NA |
| ExpressVote Previewer | 4.0.0.0 |
| PaperBallot | 6.0.0.0 |
| Removable Media Service | 2.0.0.0 |
| Toolbox | 4.0.0.0 |

Changes

The purpose of version 6.1.1.0 is to consolidate several minor engineering changes into a new version of EVS rather than having a collection of engineering change orders (ECOs).

System Overview

EVS is a comprehensive election system that supports most modern voting methods.

Election setup is done using the Electionware software and then transported to the various Election-Day devices on encrypted USB memory sticks.

On Election Day, voters can mark paper ballots manually, or use an ExpressVote, ExpressVote XL, or ExpressTouch voting station. ExpressVote is a touch-screen voting station that can be used either as a direct recording electronic (DRE) device that records voters' choices on electronic media, or for printing their choices on a paper ballot card for separate tabulation.

The printed ballot contains a complete record of the voter's choices in both human-readable form (so the voter can verify it) and machine-readable form (for tabulation).

ExpressTouch is a tablet voting station that is primarily for curbside voting.

At the polls, election workers first identify a voter's precinct and split, and then use ExpressLink to print an activation card to unlock a voting station. For manual voting, the voter is given a paper ballot.

The paper ballots and vote summary card can be scanned in the precinct using the DS200, or in a central-count location using the DS450 or DS850. The results of DRE voting and the ballots scanned in the precinct are written on USB memory, which is then carried to the central-count location for final tabulation.

Examination Procedures

This was a one-day examination. We observed as the vendor installed the firmware and software using files obtained directly from the VSTL by the Secretary of State, thus providing chain of custody. Then we heard a presentation about the system, verified version numbers, asked questions, and conducted a test election to verify correct tabulation.

Concern

Password Expiration

ES&S has provided an optional method for modifying the Microsoft Windows password policy to not expire on the EMS computer. In my opinion, passwords should be changed at least once a year. Otherwise access could be gained by someone who has a password from a previous election and does not have any role in the current election. I understand that the default 60-day limit can be annoying, but I believe it is a mistake to allow passwords that never expire.

This can be mitigated by telling counties not to set password expiration times of more than one year, but this option should still be removed.

Summary

In my opinion the EVS 6.1.1.0 is an excellent voting system, and I recommend certification, although I do recommend requiring passwords to be changed no less frequently than once a year.



KEN PAXTON
ATTORNEY GENERAL OF TEXAS

September 21, 2020

Mr. Keith Ingram
Director of Elections, Texas Secretary of State
Elections Division
P.O. Box 12060
Austin, Texas 78711-2060

Re: Election Systems & Software EVS Version 6.1.1.0—Examination August 21, 2020

Dear Mr. Ingram:

Pursuant to Texas Election Code §122.036 and 1 Texas Administrative Code §81.60, by this letter I am transmitting my examiner's report for the Secretary of State's August 21, 2020 voting system examination. The subject of that examination was Election Systems & Software ("ES&S") voting system EVS 6.1.1.0.

The factual background for this report includes ES&S's presentation to the examiners during an examination at the Secretary of State's office, statements made by ES&S's representatives during that examination, and any e-mail answers to the examiner's follow-up questions sent by ES&S to the Secretary of State's office and then forwarded to the examiners.

The Office of the Attorney General notes that the United States Election Assistance Commission certified EVS 6.1.1.0 on July 27, 2020 as a modification to EVS 6.1.0.0, which has been previously certified for use in Texas elections. EVS 6.1.1.0 consists of multiple software components, but no hardware updates.

Both during and after the examination, the examiners raised specific concerns about legal compliance of EVS 6.1.1.0. Notwithstanding these concerns, proper procedures concerning the use and operation of EVS 6.1.1.0 help ensure compliance with applicable laws and rules. Therefore, after a thorough review of the system, the Office of the Attorney General concludes there are no legal compliance issues with EVS 6.1.1.0 and recommends certification consistent with this report.

Sincerely,

A handwritten signature in black ink, appearing to read "Lesley French".

Lesley French
General Counsel

cc: Charles Pinney, Secretary of State's Office

ES&S 6110

The Election Systems and Software (ES&S) release of the EVS 6.1.1.0 election system was examined in Austin on August 21, 2020. This release is a modification to the 6.1.0.0 release which was previously certified in Texas. This release was certified by the federal Elections Assistance Commission (EAC) in June 2020. Due to the Covid-19 social distancing requirements, my review of the system was done remotely.

The upgrades to the 6.1.1.0 system from the 6.1.0.0 system were modifications to the Electionware (EMS) software and the MS-Windows operating system. Therefore, the focus was to review the functional changes to Electionware.

None of the voting devices and ancillary products were updated. A test election was voted and tallied to validate that the system's effectiveness and security were not compromised by the upgrade.

The following table lists the modified 6.1.1.0 components used for the examination.

Table 1 - Releases for Proprietary Hardware/Software Components

| Hardware/Software | Version/Firmware # | Location |
|--------------------------------------|--------------------|---------------------|
| Software | | |
| Electionware (EMS) | 6.0.1.0 | Central office |
| Event Log Service | 2.0.0.0 | Central office |
| Removable Media Service | 2.0.0.0 | Central office |
| Hardware | | |
| ExpressVote HW1.0 (BMD) | 4.0.0.0 | Precinct |
| ExpressVote HW2.1 (BMD or tabulator) | 4.0.0.0 | Precinct |
| DS200 precinct scanner | 2.30.0.0 | Precinct or central |
| ExpressTouch (DRE) | 1.0.3.0 | Precinct |
| ExpressVote - XL (BMD) | 1.0.3.0 | Precinct |
| DS450 scanner | 3.4.0.0 | Central office |
| DS850 scanner | 3.4.0.0 | Central office |

For a detailed explanation of all the hardware components and applications of the 6.1.1.0 system please refer to the EAC's certification [test report](#).

Changes

- Arial fonts are now included with the system allowing jurisdictions more flexibility for the ballot layout.
- Provided the option for increased physical RAM on the EMS in the client, server and/or standalone configurations. This provides an increased amount of virtual RAM available to Electionware.
- Added critical Windows security updates.
- Added an updated JAR file to prevent relocated JAI classes from loading. This prevents the Internal Error displayed when attempting to view ExpressVote XL write-in images.
- Modified Password Policy - the Microsoft Windows password policy is set to not expire on the EMS.
- Created an additional Postgres database index to enhance the security and performance of the database.

An additional user logging message to enhance the transparency and security of the database. This additional logging is included within the Reporting module to assist users during ballot adjudication.

- Removed all empty entries in the CVR export report.
- Resolved a bug that caused an incorrect write-in image snippet to be assigned to the exported cast vote record (CVR). The incorrect snippet would be displayed in the adjudication screen in the EMS.

Findings

- The responses provided on Form-101 are acceptable.
- The Technical Data Package (TDP) documentation appears to be updated with the new information.
- The system software was successfully built and witnessed by SOS staff. A sample of the hash values were verified to match the values of the EMS executables that were used in the EAC testing.
- The voted test ballots were recorded and tallied correctly.
- The additional RAM was not tested during the examination, but it is safe to assume that the upgrade would reduce processing times and increase throughput for CPU intensive processes.
- There were no changes to the database tables or data file formats. This allows a jurisdiction to create a new election setup on a 6.1.0.0 version system, and then migrate the setup to the 6.1.1.0 version after the EMS has been upgraded.
- The addition of an index on a Postgres table adds a database level integrity check to prevent duplicate records from being uploaded into the EMS table. It creates a unique index on the **results.batch** table. Also, an operator loading the batch would get an indication that a record already exists in the table. The Postgres log message would be useful to determine if a batch was processed more than once.

This modification was previously reviewed by me and subsequently approved by means of the de minimis ECO (engineering change order) approval process.

- The JAR file was added to prevent stock JAI classes from loading. The installation instructions are easy to follow, but I can see that for some jurisdictions, installation may be difficult or error prone. In that case, I hope ES&S will provide assistance free of charge, but not via a remote connection. Help should be provided either by phone, video conferencing, or in person.

This modification was previously reviewed by me and subsequently approved by means of the de minimis ECO (engineering change order) approval process.

- The new “never expire” password setting is too lenient. I believe it should be set for no longer than 6 months. Additionally, a jurisdiction should have a policy to change passwords at the beginning of each election cycle. Also, a user’s account should be disabled immediately once they are no longer working for the jurisdiction.
- The ES&S hash validation program continues to be unnecessarily difficult and error prone. Since this is the way jurisdictions verify that they are running the certified software, the validation program should be improved. It needs to be simplified and made

more robust to prevent errors and/or false results.

- The EMS software upgrade can be done either by ES&S or by the jurisdiction. The hash validation should be performed by the jurisdiction.

The ES&S hash software/firmware validation programs continue to be unnecessarily difficult to perform and error prone. Since this is the way jurisdictions verify that they are running the certified software, the validation program must be improved. It needs to be easier to run, require less human input, and be more robust to prevent errors and/or false results.

Conclusion

The modifications to the EMS were minor and presented no loss of functionality. There is a potential for a loss of security because of the more lenient password expiration. This can be mitigated by an election administration policy to force renewal on a schedule, even though it will not be enforced by the MS-Windows operating system.

I believe the system examined meets the requirements of the Texas Election Code. I recommend certification of the EVS 6.1.1.0 system.

Tom Watson
Examiner