ES&S 6100

The Election Systems and Software (ES&S) release of the EVS 6.1.0.0 election system was examined in Austin on January 15 and 16, 2020. This release was certified by the federal Elections Assistance Commission (EAC) in September 2019.

This release is a modification to the 6.0.4.0 release which was previously certified in Texas. This release includes an operating system software upgrade for the server and workstations, security improvement for the scanners, and minor cosmetic and functional changes to some voting machine components. This report builds on the 6.0.4.0 report so interested parties should read that report as well. Some of the findings from the previous examination are repeated in this report for emphasis.

The following table lists the modified 6.1.0.0 components used for the examination.

Table 1 - Releases for new Proprietary Hardware/Software Components

Hardware/Software	Version/Firmware #	Location
Software		
Electionware (EMS)	6.0.0.0	Central office
Event Log Service	2.0.0.0	Central office
Paper Ballot (ballot designer)	6.0.0.0	Central office
Toolbox (utilities)	3.5.0.0	Central office
Hardware		
ExpressVote HW1.0 (BMD)	4.0.0.0	Precinct
ExpressVote HW2.1 (BMD)	4.0.0.0	Precinct
DS200 precinct scanner	2.30.0.0	Precinct or central
ExpressTouch (DRE)	1.0.3.0	Precinct (curbside)
ExpressVote - XL (BMD or tabulator)	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 please refer to the EAC's certification test report. For system capabilities and limitations refer to the Scope of Certification document.

Findings

- The responses provided on Form-101 are acceptable.

- The Technical Data Package (TDP) documentation appears to be accurate and complete.

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

- The audit logs are detailed and easy to understand.

- The operating systems for the EMS workstations and servers were upgraded. The workstations were upgraded from Microsoft Windows 7 to Microsoft Windows 10 Enterprise LTSC. The servers were upgraded from Microsoft Windows Server 2008 R2 to Microsoft Windows Server 2016. The upgrades also change the EMS from a 32-bit to a 64-bit architecture. All workstations/servers are now using Bitlocker to encrypt the hard drives.

- Contrary to what was said by an ES&S representative during the examination, a jurisdiction must deploy the system using the servers and/or workstations specified in the EAC's Scope of Certification document in order to be in compliance.

  If the servers or workstations are no longer available due to end-of-life, ES&S can use the EAC's ECO process to upgrade the server and workstation specification if this occurs between releases.

- An ES&S representative reiterated what was said in the 6.0.4.0 examination; that the ExpressVote XL will only be sold as a BMD in Texas. That it will not be sold as a DRE. Voters will receive a vote summary card that is scanned in the precinct (using a DS200 scanner), or on a central-site scanner (DS450 or DS850).

- An ES&S representative said the ExpressTouch (DRE) will only be sold in Texas for curbside voting.

- The ExpressVote XL layout used for this examination was better than the layout used for the 6.0.2.0 and 6.0.4.0 examinations, but still not as clear as it should be. The design software should automatically use thicker lines or double lines, or more space between the races. The XL uses a full-face ballot display by default, which makes it too easy to accidentally select a candidate from a different race as you look on the right side of the screen, far from the race name, without a clear delineation of the races.

- There is a new ExpressVote voting booth workstation designed for ADA-compliant voting. The voting booth workstation can be positioned to accommodate both standing and seated voters. It can accommodate seated voters using a side-approach position.

- The touch screen layout design program is now used for all voting devices. This is the interface and functionality used for the ExpressVote XL since the 6.0.2.0 release. No

need to create separate layouts for the ExpressVotes BMD's or the Touch DRE. The ExpressVote XL defaults to a single screen (full-face ballot). When in ADA mode, it has a multi-page display. The same display format used by the ExpressVote and ExpressTouch.

- Ballot review on ExpressVote BMD is on the screen before the ballot summary card is printed, when in ADA only. Also when the ExpressVote is in ADA mode, a voter's selection is outlined lightly when using a 2 button input device. The outline is hard to see. Selections should highlight the entire selection box in blue like a regular voting session.

  Non-ADA voters can still review the printed ballot before casting their ballot.

- The DS200 scanner should be configured to not notify a voter for an under-voted ballot. This is preferred because the voter would have already been warned of undervotes by the BMD voting machine.

  If the DS200 is configured to warn for an undervote, voters might walk away after inserting their ballot card into a DS200 because they don't expect a warning. This could be a problem for poll-workers who have to deal with fleeing voters.

- There is a new secured CF card capability for the DS200. If a secured card is used, the card is "married" to that DS200, and cannot be used in another DS200.

- An optional read-only compact flash was added for the 450 and 850 central scanners. The CF cards used are locked by a ES&S technician, so they cannot be modified.

- There is a new functionality which allows the firmware to be updated on an ExpressVote via a flash drive. This saves the ES&S technicians time because they don't have to open the case. This is another reason that hash verification is important and should be run before each election. The new method creates a potential attack vector from an internal rogue operator who has access to the voting machines.

- Hash validation for the EMS is too cumbersome and prone to error. There is too much human interaction required. Also, the script that generates the hashes and validates the hashes could easily be edited to output a bogus report.

  For the examination, the output from the verification process had more than 6800 files reported. Most were dynamic files like logs, sound files, but at least 19 DLL files were reported. DLL and EXE file hashes should never be different from the official list of hashes. The vendor stated initially that the election software was installed on a "bare metal" machine. It was later explained that the large list of changed files was due to the machine being used for other examinations and multiple test elections. The "golden hash" of the EMS machine was taken in October, not right before the Texas examination. In the meantime, printer drivers, etc. were added to the system. If the "golden image" had been created right before the exam, there would be zero DLL's and EXE's in the list of files. Only log files, data files, images, etc. should be in the non-static list.

In the future, ES&S should begin the examination with the EMS software installation using a clean machine. Only a fresh Windows installation should exist on the machine. There should not be any previous election definitions, results, etc. on the machine. This was not the case for this examination.

There is also a fundamental flaw in the EMS hash verification process. The EAC VVSG Vol. 1 Section 7.4 states that the hashes for the programs on the EMS machine should be compared to the hashes generated and supplied by the lab, EAC, or a designated repository. The ES&S verification uses hashes taken from the EMS "golden image". If the EMS machine was corrupted during the installation or soon after, the hashes would be bogus and the verification program would not report the invalid hashes.

The vendor should supply a CDROM (i.e. read-only as required by the VVSG) disk with the hash verification software, list of all programs (including COTS and 3rd-party drivers, etc.), and the VSTL generated hashes. The machine should be booted from CDROM disk, mount the drive(s) on the EMS machine(s) and then with only minimum operator interaction, proceed to compare the hashes for the list of program files, and produce the reports. This would be much easier and hopefully encourage a jurisdiction to verify the hashes for the EMS machines before and after each election.

Another improvement would be to sort the list of files by file type (e.g. dll). Currently, the list is not sorted so different types are interlaced. The executable files are the most critical so they should be grouped together. Also, the non-static files list is typically large, and this would make it easier to see which files are logs, data files, etc.

- A couple of recent election problems that occurred in Pennsylvania were discussed. ES&S said the errors should have been caught in the L&A testing, even though there was an ES&S employee present during the test. Unfortunately, the problems were not detected before election day.

  One problem was due to screen miscalibration on several voting machines. The problem was exasperated because the ballot layout was allowed to extend all the way to the edge of the screen. The layout used the small selection box on the top left edge of the candidate's selection box and due to the miscalibration, some voters inadvertently selected the adjacent candidate.

  The previous release's examination report recommended not to use the boxes because it can be confusing. This is a configuration option. Selections can be made by pressing the larger box which has the candidate's name. This problem should be prevented by the ballot layout software. There should be a hard-coded minimum margin around the screen.

  A second issue that occurred in Pennsylvania was experienced using the ExpressVote XL DRE. The problem should not occur in Texas since the XL will only be used as a BMD, but the extent of the problem is not known at this time. A detailed root cause analysis was not provided and so it could be a problem on the ExpressTouch which uses

the same ballot layout software. The problem would be unrecoverable since the ExpressTouch does not also print ballot summary cards like the XL.

The problem was caused by a late addition to the ballot. The jurisdiction wanted instructional text to be embedded in the space where normally a candidate's name would be. ES&S said that this was a unique ballot layout, and the first time it was used. The problem manifested itself by a specific candidate's lack of votes. The internal DRE tabulator assigned votes to an incorrect tally. Not the tally for the candidate.

The mapping of the layout x,y coordinates to the candidates' vote tallies in the XL tabulator was different than the mapping for the printing program on the XL. It became obvious that there was a problem since that candidate didn't get any votes. The jurisdiction was able to scan the paper ballot summary cards to get an accurate tabulation. The printed ballot cards had the correct selections, but the DRE tabulation did not. If this problem occurred on a ExpressTouch which does not produce voted paper ballot summary cards, there likely would be no recovery from the error.

A single mapping should be used by both the tabulation and print programs. Also instructions should not be allowed to be embedded into the candidate selection space.

Conclusion

The modifications to the system were minor. Overall, the system's core functionality, and security protections remain intact.

I recommend certification of the EVS 6.1.0.0 system with a couple of provisions:

1) A restriction stated in the scope of certification to alert a jurisdiction to the aforementioned ballot layout issue. No instructions should be allowed to be embedded in the candidates' space on the ballot.

2) The EMS hash verification must be improved, and in compliance with the EAC's VVSG for the next release.

Tom Watson
Examiner