U. S. ELECTION ASSISTANCE COMMISSION
VOTING SYSTEM TESTING AND CERTIFICATION PROGRAM
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

September 29, 2020 **Sent via e-mail**

Steve Pearson, Senior Vice President of Certification
Election Systems & Software
11208 John Galt Blvd.
Omaha, NE 69137

Re: ExpressVote 1.0 Trusted Build

Dear Mr. Pearson,

On September 23, 2020, the U.S. Election Assistance Commission (EAC) was notified by the Texas Secretary of State's office that a voting system they were examining for certification, ES&S EVS 6.0.3.0, was displaying a hash validation error during trusted build installation on the ExpressVote 1.0. When questioned by Texas SOS representatives, the ES&S representative replied that this was expected behavior and that it also existed in EVS 6.0.2.0. Both versions are certified by the EAC to VVSG 1.0 and EVS 6.0.2.0 is currently deployed in 43 counties in Texas. 18 of the 43 counties use a configuration of EVS 6.0.2.0 that includes the ExpressVote 1.0.

Section 5.5 of the EAC's Testing and Certification Program Manual describes the trusted build as follows:

> *5.5. Trusted Build. A software build (also referred to as a compilation) is the process whereby source code is converted to machine-readable binary instructions (executable code) for the computer. A "trusted build" (or trusted compilation) is a build performed with adequate security measures implemented to give confidence that the executable code is a verifiable and faithful representation of the source code. The primary function of a trusted build is to create a chain of evidence which allows stakeholders to have an approved model to use for verification of a voting system. Specifically, the build will:*
>
> *5.5.1.Demonstrate that the software was built as described in the TDP.*
>
> *5.5.2.Show that the tested and approved source code was actually used to build the executable code used on the system.*
>
> *5.5.3.Demonstrate that no elements other than those included in the TDP were introduced in the software build. The vendor or source from which each COTS product was procured must be included in the TDP.*
>
> *5.5.4.Document for future reference the configuration of the system certified.*

5.5.5.Demonstrate that all COTS products are unmodified by requiring the VSTL to independently obtain all COTS products from an outside source.

As part of EAC certification, manufacturers are required to submit system identification tools and procedures that use hashes to prove that the applications installed on a voting system exactly match the certified versions.

The ES&S representative performing the installation during the examination used a method that was not tested by an EAC-accredited voting system test laboratory (VSTL) or certified by the EAC to install the software. When questioned by the Texas SOS representatives, the representative claimed that the installation method was reviewed/approved by the lab as part of their certification. Both SLI (VSTL for EVS 6.0.2.0) and Pro V&V (VSTL for EVS 6.0.3.0) deny that they had reviewed this installation method as part of certification testing.

Texas contracted with Pro V&V to verify ES&S' claim that the SYSLOAD.BMP file was the only change to the certified version. On September 24th, Pro V&V confirmed via source code review that this was the only change to the software. Texas has demanded that ES&S visit all 18 counties impacted by this deviation to perform a clean installation of the software using the certified installation procedure on all ExpressVote 1.0 machines (720 total).

We were under the initial impression that only EVS 6.0.2.0 systems in Texas were impacted. We now know that is not the case but need to fully understand all of the systems that are impacted.

In order to be in compliance with our Testing and Certification Program, we are requesting the following information. We may request additional information, and expect that you will disclose any other information that would assist us in understanding the scope of impact of any ES&S voting system regarding compliance with EAC certification.

1. The total number of jurisdictions throughout the United States affected including the jurisdiction name, contact information, and a list of affected devices including the system version information as well as serial numbers in each jurisdiction and when the installation occurred by ES&S personnel.
2. A detailed document providing a timeline of when this issue was first known and what ES&S is doing to remediate the issue.
3. All communication with the VSTLs regarding this issue.
4. An advisory notice specifying each EAC-certified voting system that uses the ExpressVote 1.0 and the ExpressVote's certified hashes and the mismatched hashes generated from the "update" file that has been installed on fielded devices.
5. All communication to the affected jurisdictions must represent the real facts regarding the circumstances.
6. Submit all documentation that supports your position regarding what you feel occurred.
7. A detailed document describing why ES&S disagrees with some of the statements the Texas Secretary of State's office made in the their letter to ES&S dated September 24, 2020.
8. ES&S' plan to install EAC-certified software on the affected ExpressVotes in Texas.
9. ES&S' plan to install EAC-certified software on affected ExpressVotes as requested by jurisdictions.
10. ES&S' planned resolution, including a documented procedure, to ensure that this does not occur again.

11. ES&S' communication plan and any other documentation (timeline, FAQs) that will be distributed to the affected jurisdictions for review and approval by the EAC.
12. ES&S will communicate directly with the Executive Director or her designated representative and will cease to contact EAC employees throughout the duration of this investigation.

Finally, according to Section 5.15.4 of the Testing and Certification Program Manual, a manufacturer has 15 days from receipt of this letter to comply with the recommended corrective actions. However, due to the urgent nature of this issue and its impact on fielded, EAC-certified voting system 35 days before the 2020 General Election, we are requesting this information by close of business on October 1, 2020. We anticipate you immediately provide a written advisory of the situation to the states and localities impacted by this issue. We are requesting you utilize additional personnel and expend whatever resources necessary to install EAC-certified trusted builds on identified EAC certified voting systems, resolving the issue upon request of the states. The EAC anticipates that we will review and test the "update file" in our accredited VSTLs in the coming days and weeks. We anticipate your cooperation with this matter and working with the states and localities using the identified voting systems.

ES&S needs to be prepared to cooperate with the labs and EAC to provide complete test reports on each of the builds of different versions among the states that have an incorrect hash validation - so we have a complete record of testing results that confirms there is not any impact to accuracy, functionality, use, etc.

Failure to comply will result in the EAC taking immediate required action as it deems appropriate as the system no longer complies with its original certification, including but not limited to initiating decertification actions and/or suspension of manufacturer registration.

We are taking this matter very seriously and understand that ES&S does as well and appreciate a prompt response given the nature of this issue.

Sincerely,

Mona Harrington

Mona Harrington, Executive Director

cc:
Kevin Rayburn, General Counsel
Jerome Lovato Director, Voting System Testing and Certification

U. S. ELECTION ASSISTANCE COMMISSION
VOTING SYSTEM TESTING AND CERTIFICATION PROGRAM
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

October 1, 2020 **Sent via e-mail**

Re: ExpressVote 1.0 Trusted Build

Dear State Election Directors,

On September 23, 2020, the U.S. Election Assistance Commission (EAC) was notified by the Texas Secretary of State's (SOS) office that they discovered a hash value discrepancy with a voting system they were examining for certification, ES&S EVS 6.0.3.0. This hash value discrepancy was discovered on ExpressVote 1.0 when the Texas SOS staff exported the software files from the installation USB drive and the installation files from the trusted build and imported them into a 3rd party software tool, Ubuntu, which compared the two hash values and displayed the mismatched hash value.

It's important to note in this case that the states and their jurisdictions wouldn't have seen an automated hash value error displayed on the screen as there are two separate load processes, which makes it impossible to allow for the system to compare the two hashes and display an error message. Discovering the hash value discrepancy would require a manual process of comparison by reviewing the hash value from the Inno disk (inside the unit) which loads the entirety of the installation (all files), to the hash value from the USB drive (as it only loads the firmware).

Texas SOS representatives and ES&S representatives determined this validation error existed in EVS 6.0.2.0 as well. Both versions are certified by the EAC to VVSG 1.0 and EVS 6.0.2.0 is currently deployed in 43 counties in Texas. 18 of the 43 counties use a configuration of EVS 6.0.2.0 that includes the ExpressVote 1.0.

As part of EAC certification, manufacturers are required to submit system identification tools and procedures that use hashes to prove that the applications installed on a voting system exactly match the certified versions. ES&S explained that only one file was causing the hash validation error, a bitmap image file (SYSLOAD.BMP) with a copyright date that displays on the ExpressVote while booting up. ES&S further explained that the issue occurs only if a USB update method is used to update the version of the ExpressVote unit from a previous version. The reason the update method causes the issue is due to the fact that the USB drive is a quick installation method that is designed to ONLY update firmware, and because the bitmap file is not part of the firmware, the installation via the USB drive method didn't replace the bitmap file and left the old bitmap file on the system resulting in the hash discrepancy.

Texas contracted with the voting system test laboratory (VSTL) Pro V&V to verify ES&S' claim that the SYSLOAD.BMP file was the only change to the certified trusted build. Pro V&V performed a source code comparison of the EVS 6.0.2.0 update image disk file and the EVS 6.0.2.0 production release disk image file. Pro V&V confirmed that the only change was a bitmap file. Pro V&V upgraded an ExpressVote from EVS 5.2.2.0 to EVS 6.0.2.0, received a hash mismatch message as expected, and

performed functional testing on the upgraded ExpressVote. Pro V&V concluded that the hash mismatch error does not impact the functionality of the ExpressVote. Pro V&V's test report is attached to this letter.

Initially, we were under the impression that only EVS 6.0.2.0 systems in Texas were impacted. We requesting information from ES&S to better understand the scope and to date have received information that the states listed in Table 1 have at least one jurisdiction that may be affected. Please note that this information is current as of October 1, 2020. We will provide updated information as soon as it is received.

Table 1

State	# of Units	Status
AL	105	Potentially affected
AR	2072	Potentially affected
AZ	496	Potentially affected
DC	102	Affected
FL	2893	Potentially affected
IA	532	Potentially affected
ID	346	Potentially affected
IN	731	Potentially affected
KS	1742	Potentially affected
KY	400	Affected
MD	3501	Likely unaffected
MI	548	Potentially affected
MO	538	Potentially affected
OH	168	Potentially affected
TN	671	Potentially affected
WA	3	Potentially affected
WI	667	Potentially affected
WY	20	Potentially affected

On September 29, 2020, we sent the following request to ES&S:

"In order to be in compliance with our Testing and Certification Program, we are requesting the following information. We may request additional information, and expect that you will disclose any other information that would assist us in understanding the scope of impact of any ES&S voting system regarding compliance with EAC certification.

1. The total number of jurisdictions throughout the United States affected including the jurisdiction name, contact information, and a list of affected devices including the system version information as well as serial numbers in each jurisdiction and when the installation occurred by ES&S personnel.

2. A detailed document providing a timeline of when this issue was first known and what ES&S is doing to remediate the issue.
3. All communication with the VSTLs regarding this issue.
4. An advisory notice specifying each EAC-certified voting system that uses the ExpressVote 1.0 and the ExpressVote's certified hashes and the mismatched hashes generated from the "update" file that has been installed on fielded devices.
5. All communication to the affected jurisdictions must represent the real facts regarding the circumstances.
6. Submit all documentation that supports your position regarding what you feel occurred.
7. A detailed document describing why ES&S disagrees with some of the statements the Texas Secretary of State's office made in the their letter to ES&S dated September 24, 2020.
8. ES&S' plan to install EAC-certified software on the affected ExpressVotes in Texas.
9. ES&S' plan to install EAC-certified software on affected ExpressVotes as requested by jurisdictions.
10. ES&S' planned resolution, including a documented procedure, to ensure that this does not occur again.
11. ES&S' communication plan and any other documentation (timeline, FAQs) that will be distributed to the affected jurisdictions for review and approval by the EAC.
12. ES&S will communicate directly with the Executive Director or her designated representative and will cease to contact EAC employees throughout the duration of this investigation.

Finally, according to Section 5.15.4 of the Testing and Certification Program Manual, a manufacturer has 15 days from receipt of this letter to comply with the recommended corrective actions. However, due to the urgent nature of this issue and its impact on fielded, EAC-certified voting system 35 days before the 2020 General Election, we are requesting this information by close of business on October 1, 2020. We anticipate you immediately provide a written advisory of the situation to the states and localities impacted by this issue. We are requesting you utilize additional personnel and expend whatever resources necessary to install to provide an appropriate validated hash on identified EAC certified voting systems, resolving the issue upon request of the states. The EAC anticipates that we will review and re-test the software with incorrect hash validation in our accredited laboratories in the coming days and weeks. We anticipate your cooperation with this matter and working with the states and localities using the identified systems.

ES&S needs to be prepared to cooperate with the labs and EAC to provide complete test reports on each of the builds of different versions among the states that have an incorrect hash validation - so we have a complete record of testing results that confirms there is not any impact to accuracy, functionality, use, etc.

Failure to comply will result in the EAC taking immediate required action as it deems appropriate as the system no longer complies with its original certification, including but not limited to initiating decertification actions and/or suspension of manufacturer registration.

We are taking this matter very seriously and understand that ES&S does as well and appreciate a prompt response given the nature of this issue."

We will request that ES&S submit all update image files and voting system configurations to VSTLs for examination via our de minimis change process. Table 2 displays all affected EVS voting systems, firmware versions, and hash values of the production trusted build.

Table 2

EVS Release	FW Version	Copyright YRS	Hash Value
FL EVS 4500v4	1.2.3.0	2011 - 2013	f67dbc52fe9c5e65ad786740ca07388e864fc00aaabcb6e0169b44c485356101
EVS 5200 EVS 5300 EVS 5303 IL EVS 5300 EVS 5201 EVS 5202 EVS 5203 EVS 5204	1.4.0.0	2011 - 2014	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
EVS 5210 EVS 5310	1.4.1.0	2011 - 2015	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
EVS 5211	1.4.1.1	2011 - 2016	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
EVS 5220 EVS 5320	1.4.1.2	2011 - 2016	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
EVS 5321 EVS 5230 EVS 5330	1.4.1.6	2011 - 2017	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
EVS 5240 EVS 5340 EVS 5241 EVS5341	1.4.1.7	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
FL EVS 4520v1	1.4.2.0	2011 - 2015	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
FL EVS 4530v1	1.4.3.0	2011 - 2017	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
FL EVS 4530v2	1.4.3.1	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
EVS 6000 EVS 6010 EVS 6020 EVS 6030	1.5.0.0	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
EVS 6021 EVS 6030	1.5.1.0	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
EVS 6040 EVS 6043	1.5.2.0	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12

EVS 6040 AZ	1.5.2.1	2011 - 2019	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
EVS 6050 EVS 6051	1.5.3.0	2011 - 2019	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

Proposed Plan

We are asking ES&S to place all affected versions with the labs as a de minimus change. According to Section 3.4.2. of the EAC's Testing and Certification Manual, a de minimis change is defined as a change to a certified voting system's hardware, software, TDP, or data, the nature of which will not materially alter the system's reliability, functionality, capability, or operation. Under no circumstance shall a change be considered de minimis if it has reasonable and identifiable potential to impact the system's performance and compliance with the applicable voting Standard.

The bitmap file is "minor in nature and effect" and qualifies under section 3.4.1 for a change order.

The VSTLS will perform a thorough review of all source code in all affected versions and the EAC will receive reports on all versions.

The de mimimus process will allow for election officials to have full assurance that the labs have thoroughly reviewed and compared all affected versions to the trusted build as part of the de mimimus review.

We are requesting this effort be performed in an expedited manner and within a two week time frame. We will share our findings with you and keep you updated throughout the process.

In weighing the merits, we believe this is the most optimal solution given the non-substantive impact of the bitmap file issue that is causing the hash mismatch. This process will also allow for verification that the bitmap file is in fact the only change and will result in compliance with EAC's certification program.

This effort doesn't impact the state's/jurisdiction's ability to request ES&S to perform a clean full installation which would also resolve the hash value issue. Given the short time window left until the election, we wanted to implement a solution that resolves the issue for all while simultaneously allowing you to focus on all the hard work you are doing to run safe and secure elections.

Finally, this proposed plan is based on the information the EAC has right now. Should we learn new material information, we will modify the plan and take whatever steps are appropriate.

Sincerely,

Mona Harrington
Mona Harrington, Executive Director

cc:
Kevin Rayburn, General Counsel
Jerome Lovato Director, Voting System Testing and Certification

Election Systems & Software
MAINTAINING VOTER CONFIDENCE. ENHANCING THE VOTING EXPERIENCE.
EXPERIENCE
RELIABILITY
SECURITY
INNOVATION
11208 John Galt Boulevard · Omaha, NE 68137 USA
Phone: 402.593.0101 · Toll-Free: 1.800.247.8683 · Fax: 402.593.8107
www.essvote.com

October 1, 2020

VIA ELECTRONIC MAIL: mharrington@eac.gov
AND OVERNIGHT COURIER

Mona Harrington
Executive Director
U.S. Election Assistance Commission
Voting System Testing and Certification Program
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

RE: ExpressVote 1.0 Trusted Build

Dear Ms. Harrington:

I am in receipt of your letter dated September 29, 2020, regarding the above-referenced matter. Thank you, Jerome and Kevin very much for taking time yesterday to allow us to further explain the issue and discuss potential options for resolution of the same.

In response to the twelve (12) enumerated requests set forth in your letter, please know that numerous ES&S personnel are working diligently to provide you with complete and timely responses as soon as possible. As you know, yesterday we provided additional information respecting EVS versions, copyright years and corresponding hash values, as well as potentially affected jurisdictions and numbers of ExpressVote units within each. We have also included herewith additional materials and information responsive to your requests which have been assembled and completed to date. The enclosed materials have been labeled to identify the corresponding request number in your letter. As we committed, we will continue to supplement this response with additional information and materials as soon as their preparation is complete.

We greatly appreciate the EAC's oversight and dedication to working with ES&S toward a satisfactory resolution of this matter. As you and your staff review the materials and responses provided by ES&S, please do not hesitate to contact me if anyone has any additional questions. Thank you.

Sincerely,

Steve Pearson, Sr. Vice President, Certification

Enclosures
cc: Thomas E. Burt, Chief Executive Officer, ES&S
Eric A. Anderson, Vice President and General Counsel, ES&S
Kathy Rogers, Senior Vice President, ES&S

ES&S RESPONSE NO. 1 - JURISDICTIONS

Jurisdiction	State	Is Copyright Correct/Incorrect?
Montgomery County, Alabama	AL	Potentially Affected
Arkansas County, Arkansas	AR	Potentially Affected
Benton County, Arkansas	AR	Potentially Affected
Carroll County, Arkansas	AR	Potentially Affected
Cross County, Arkansas	AR	Potentially Affected
Faulkner County, Arkansas	AR	Potentially Affected
Garland County, Arkansas	AR	Potentially Affected
Miller County, Arkansas	AR	Potentially Affected
Pike County, Arkansas	AR	Potentially Affected
Polk County, Arkansas	AR	Potentially Affected
Sebastian County, Arkansas	AR	Potentially Affected
Sevier County, Arkansas	AR	Potentially Affected
Boone County, Arkansas	AR	Potentially Affected
Columbia County, Arkansas	AR	Potentially Affected
Garland County, Arkansas	AR	Potentially Affected
Sebastian County, Arkansas	AR	Potentially Affected
Yell County, Arkansas	AR	Potentially Affected
Chicot County, Arkansas	AR	Potentially Affected
Cleveland County, Arkansas	AR	Potentially Affected
Arkansas County, Arkansas	AR	Potentially Affected
Jackson County, Arkansas	AR	Potentially Affected
Randolph County, Arkansas	AR	Potentially Affected
Washington County, Arkansas	AR	Potentially Affected
White County, Arkansas	AR	Potentially Affected
Apache County, Arizona	AZ	Potentially Affected
Cochise County, Arizona	AZ	Potentially Affected
Gila County, Arizona	AZ	Potentially Affected
Graham County, Arizona	AZ	Potentially Affected
Greenlee County, Arizona	AZ	Potentially Affected
La Paz County, Arizona	AZ	Potentially Affected
Mohave County, Arizona	AZ	Potentially Affected
Navajo County Elections	AZ	Potentially Affected
Pima County, Arizona	AZ	Potentially Affected
Tucson, City of, Arizona	AZ	Potentially Affected
Yuma County, Arizona	AZ	Potentially Affected
DC Board of Elections	DC	Incorrect
Bay County, Florida	FL	Potentially Affected

Broward County, Florida	FL	Potentially Affected
Calhoun County, Florida	FL	Potentially Affected
Charlotte County, Florida	FL	Potentially Affected
Citrus County, Florida	FL	Potentially Affected
Clay County, Florida	FL	Potentially Affected
Collier County, Florida	FL	Potentially Affected
Escambia County, Florida	FL	Potentially Affected
Flagler County, Florida	FL	Potentially Affected
Indian River County, Florida	FL	Potentially Affected
Lafayette County, Florida	FL	Potentially Affected
Lake County, Florida	FL	Potentially Affected
Lee County, Florida	FL	Potentially Affected
Manatee County, Florida	FL	Potentially Affected
Marion County, Florida	FL	Potentially Affected
Martin County, Florida	FL	Potentially Affected
Orange County, Florida	FL	Potentially Affected
Osceola County, Florida	FL	Potentially Affected
Pasco County, Florida	FL	Potentially Affected
Polk County, Florida	FL	Potentially Affected
Seminole County, Florida	FL	Potentially Affected
St Johns County, Florida	FL	Potentially Affected
Sumter County, Florida	FL	Potentially Affected
Volusia County, Florida Warehouse	FL	Potentially Affected
Washington County, Florida	FL	Potentially Affected
Black Hawk County, Iowa	IA	Potentially Affected
Clayton County, Iowa	IA	Potentially Affected
Clinton County, Iowa	IA	Potentially Affected
Delaware County, Iowa	IA	Potentially Affected
Jasper County, Iowa	IA	Potentially Affected
Johnson County, Iowa	IA	Potentially Affected
Jones County, Iowa	IA	Potentially Affected
Kossuth County, Iowa	IA	Potentially Affected
Lee County, Iowa	IA	Potentially Affected
Linn County, Iowa	IA	Potentially Affected
Muscatine County, Iowa	IA	Potentially Affected
Palo Alto County, Iowa	IA	Potentially Affected
Pottawattamie County, Iowa	IA	Potentially Affected
Scott County, Iowa	IA	Potentially Affected
Wapello County, Iowa	IA	Potentially Affected
Adams County, Idaho	ID	Potentially Affected
Bannock County, Idaho	ID	Potentially Affected

Bear Lake County, Idaho	ID	Potentially Affected
Bingham County, Idaho	ID	Potentially Affected
Blaine County, Idaho	ID	Potentially Affected
Boundary County, Idaho	ID	Potentially Affected
Camas County, Idaho	ID	Potentially Affected
Cassia County, Idaho	ID	Potentially Affected
Fremont County, Idaho	ID	Potentially Affected
Gem County, Idaho	ID	Potentially Affected
Jerome County, Idaho	ID	Potentially Affected
Latah County, Idaho	ID	Potentially Affected
Madison County, Idaho	ID	Potentially Affected
Minidoka County, Idaho	ID	Potentially Affected
Nez Perce County, Idaho	ID	Potentially Affected
Oneida County, Idaho	ID	Potentially Affected
Owyhee County, Idaho	ID	Potentially Affected
Payette County, Idaho	ID	Potentially Affected
Power County, Idaho	ID	Potentially Affected
Teton County, Idaho	ID	Potentially Affected
Twin Falls County, Idaho	ID	Potentially Affected
Washington County, Idaho	ID	Potentially Affected
Brown County, Illinois	IL	Correct
Pulaski County, Illinois	IL	Correct
Carroll County, Indiana	IN	Potentially Affected
Hancock County, Indiana	IN	Potentially Affected
Henry County, Indiana	IN	Potentially Affected
Marion County, Indiana	IN	Incorrect
Martin County, Indiana	IN	Potentially Affected
Union County, Indiana	IN	Potentially Affected
Allen County, Kansas	KS	Potentially Affected
Atchison County, Kansas	KS	Potentially Affected
Brown County, Kansas	KS	Potentially Affected
Chautauqua County, Kansas	KS	Potentially Affected
Cloud County, Kansas	KS	Potentially Affected
Cowley County, Kansas	KS	Potentially Affected
Doniphan County, Kansas	KS	Potentially Affected
Ellsworth County, Kansas	KS	Potentially Affected
Finney County, Kansas	KS	Potentially Affected
Jewell County, Kansas	KS	Potentially Affected
Labette County, Kansas	KS	Potentially Affected
Leavenworth County, Kansas	KS	Potentially Affected
Linn County, Kansas	KS	Potentially Affected

Lyon County, Kansas	KS	Potentially Affected
Marion County, Kansas	KS	Potentially Affected
McPherson County, Kansas	KS	Potentially Affected
Mitchell County, Kansas	KS	Potentially Affected
Nemaha County, Kansas	KS	Potentially Affected
Ness County, Kansas	KS	Potentially Affected
Norton County, Kansas	KS	Potentially Affected
Osage County, Kansas	KS	Potentially Affected
Republic County, Kansas	KS	Potentially Affected
Saline County, Kansas	KS	Potentially Affected
Sedgwick County, Kansas	KS	Potentially Affected
Shawnee County, Kansas	KS	Potentially Affected
Sherman County, Kansas	KS	Potentially Affected
Smith County, Kansas	KS	Potentially Affected
Trego County, Kansas	KS	Potentially Affected
Washington County, Kansas	KS	Potentially Affected
Wichita County, Kansas	KS	Potentially Affected
Wyandotte County, Kansas	KS	Potentially Affected
Jefferson County, Kentucky	KY	Incorrect
Madison County, Kentucky	KY	Incorrect
State of Maryland	MD	Correct
Grand Traverse County, Michigan	MI	Potentially Affected
Kalamazoo County, Michigan	MI	Potentially Affected
Mason County, Michigan	MI	Potentially Affected
Macomb County, Michigan	MI	Potentially Affected
Roscommon County, Michigan	MI	Potentially Affected
Bay County, Michigan	MI	Potentially Affected
Emmet County, Michigan	MI	Potentially Affected
Boone County Clerk's Annex	MO	Potentially Affected
Greene County, Missouri	MO	Potentially Affected
Johnson County, Missouri	MO	Potentially Affected
Kansas City, City of, Missouri	MO	Potentially Affected
Laclede County, Missouri	MO	Potentially Affected
Lincoln County, Missouri	MO	Potentially Affected
Vernon County, MIssouri	MO	Potentially Affected
Harrison County Election	MS	Correct
Lauderdale County, Mississippi	MS	Correct
Madison County, Mississippi	MS	Correct
Carson City County, Nevada	NV	Correct
Knox County, Ohio	OH	Incorrect
Portage County, Ohio	OH	Incorrect

Tuscarawas County, Ohio	OH	Incorrect
Aurora County, South Dakota	SD	Correct
Beadle County, South Dakota	SD	Correct
Bon Homme County, South Dakota	SD	Correct
Brookings County, South Dakota	SD	Correct
Brown County, South Dakota	SD	Correct
Campbell County, South Dakota	SD	Correct
Clay County, South Dakota	SD	Correct
Codington County, South Dakota	SD	Correct
Corson County, South Dakota	SD	Correct
Davison County, South Dakota	SD	Correct
Deuel County, South Dakota	SD	Correct
Grant County, South Dakota	SD	Correct
Haakon County, South Dakota	SD	Correct
Harding County, South Dakota	SD	Correct
Jerauld County, South Dakota	SD	Correct
Kingsbury County, South Dakota	SD	Correct
Lincoln County, South Dakota	SD	Correct
Lyman County, South Dakota	SD	Correct
Marshall County, South Dakota	SD	Correct
Meade County, South Dakota	SD	Correct
Mellette County, South Dakota	SD	Correct
Minnehaha County, South Dakota	SD	Correct
Pennington County, South Dakota	SD	Correct
Perkins County, South Dakota	SD	Correct
Sanborn County, South Dakota	SD	Correct
State of South Dakota	SD	Correct
Marshall County, South Dakota	SD	Correct
Haakon County, South Dakota	SD	Correct
Pennington County, South Dakota	SD	Correct
Todd County, South Dakota	SD	Correct
Tripp County, South Dakota	SD	Correct
Turner County, South Dakota	SD	Correct
Walworth County, South Dakota	SD	Correct
Ziebach County, South Dakota	SD	Correct
Coffee County, Tennessee	TN	Correct
Decatur County, Tennessee	TN	Correct
Hardin County, Tennessee	TN	Incorrect – In progress of correcting
Lincoln County, Tennessee	TN	Correct
McNairy County, Tennessee	TN	Incorrect – In progress of correcting
Pickett County, Tennessee	TN	Incorrect – In progress of correcting

Weakley County, Tennessee	TN	Incorrect – In progress of correcting
Tennessee College of Applied Technology	TN	Incorrect – In progress of correcting
Blanco County, Texas	TX	Corrected
Bowie County, Texas	TX	Corrected
Brewster County, Texas	TX	Corrected
Carson County, Texas	TX	Corrected
Childress County, Texas	TX	Corrected
Clay County, Texas	TX	Corrected
Erath County, Texas	TX	Corrected
Franklin County, Texas	TX	Corrected
Hemphill County, Texas	TX	Corrected
Hockley County, Texas	TX	Corrected
Jackson County, Texas	TX	Corrected
Kaufman County, Texas	TX	Corrected
Kinney County, Texas	TX	Corrected
McAllen, City of, Texas (Hidalgo)	TX	Corrected
Navarro County, Texas	TX	Corrected
Nolan County, Texas	TX	Corrected
Presidio County, Texas	TX	Corrected
Rockwall County, Texas	TX	Corrected
Sutton County, Texas	TX	Corrected
Appomattox County, Virginia	VA	Correct
Bath County, Virginia	VA	Correct
Bland County, Virginia	VA	Correct
Botetourt County, Virginia	VA	Correct
Buckingham County, Virginia	VA	Correct
Carroll County, Virginia	VA	Correct
Chesterfield County, Virginia	VA	Correct
Clarke County, Virginia	VA	Correct
Colonial Heights, City of, Virginia	VA	Correct
York County, Virginia	VA	Correct
Printelect	VA	Correct
Culpeper County Voter Registration	VA	Correct
Emporia, City of, Virginia	VA	Correct

Fairfax County, Virginia	VA	Correct
Fauquier County, Virginia	VA	Correct
Franklin, City of, Virginia	VA	Correct
Frederick County, Virginia	VA	Correct
Giles County, Virginia	VA	Correct
Goochland County, Virginia	VA	Correct
Grayson County, Virginia	VA	Correct
Hampton, City of, Virginia	VA	Correct
Printelect	VA	Correct
Henrico County, Virginia	VA	Correct
Hopewell, City of, Virginia	VA	Correct
Printelect	VA	Correct
King William County, Virginia	VA	Correct
Lunenburg County, Virginia	VA	Correct
PrintElect	VA	Correct
Newport News, City of, Virginia	VA	Correct
Norton, City of, Virginia	VA	Correct
Printelect	VA	Correct
Poquoson, City of, Virginia	VA	Correct
Portsmouth, City of, Virginia	VA	Correct
Printelect	VA	Correct
Printelect	VA	Correct
Pulaski County, Virginia	VA	Correct
Richmond, City of, Virginia	VA	Correct
Southampton County, Virginia	VA	Correct
Stafford County, Virginia	VA	Correct
Surry County, Virginia	VA	Correct
Tazewell County, VA Voter Registrar	VA	Correct
Virginia Beach, City of, Virginia	VA	Correct
Printelect	VA	Correct
Wise County, Virginia	VA	Correct
Wythe County, Virginia	VA	Correct
Elections System of the Virgin Islands	VI	Correct
Adams County, Washington	WA	Incorrect
Walla Walla County, Washington	WA	Correct
Brown County	WI	Potentially Affected
Calumet County	WI	Potentially Affected
Clark County	WI	Potentially Affected
Columbia County	WI	Potentially Affected
Dane County	WI	Potentially Affected
Dodge County	WI	Potentially Affected

Douglas County	WI	Potentially Affected
Eau Claire County	WI	Potentially Affected
Iowa County	WI	Potentially Affected
Jefferson County	WI	Potentially Affected
Kenosha County	WI	Potentially Affected
Manitowoc County	WI	Potentially Affected
Milwaukee County	WI	Potentially Affected
Outagamie County	WI	Potentially Affected
Pierce County	WI	Potentially Affected
Rock County	WI	Potentially Affected
Sauk County	WI	Potentially Affected
St. Croix County	WI	Potentially Affected
Taylor County	WI	Potentially Affected
Waukesha County	WI	Potentially Affected
Barbour County, West Virginia	WV	Correct
Doddridge County, West Virginia	WV	Correct
Fayette County, West Virginia	WV	Correct
Harrison County, West Virginia	WV	Correct
Jefferson County, West Virginia	WV	Correct
Kanawha County, West Virginia	WV	Correct
Monongalia County, West Virginia	WV	Correct
Nicholas County, West Virginia	WV	Correct
Ohio County, West Virginia	WV	Correct
Putnam County, West Virginia	WV	Correct
Ritchie County, West Virginia	WV	Correct
Taylor County, West Virginia	WV	Correct
Tyler County, West Virginia	WV	Correct
Upshur County, West Virginia	WV	Correct
Sublette County, Wyoming	WY	Potentially Affected
Teton County, Wyoming	WY	Potentially Affected

ES&S RESPONSE NO. 2 – TIMELINE

As it relates to this matter, ES&S became aware of this issue during its September 4, 2020 EVS 6.0.3.0 certification event in the State of Texas. During the certification event, ES&S upgraded its ExpressVote 1.0 version utilizing the USB flash drive method. The examiner for the State of Texas completed a hash verification on the ExpressVote version 1.0 unit and identified a hash mismatch identifying the sysload.bmp copyright image file as not matching the trusted build sent by the EAC. ES&S is conducting a review of its files to determine if any additional information is available regarding this matter.

In order to correct this matter, ES&S has prepared a Software Engineering Change Order ("ECO") for immediate submission under the EAC Testing & Certification Program to remediate the issue for all affected ExpressVote HW v1.0 releases. The foregoing ECO request is subject to approval by the EAC.

In addition, we are in discussion with each individual state to determine their plan for upgrading their ExpressVote 1.0 units (Example – Texas has upgraded all its affected units and Tennessee is upgrading its affected units this weekend).

ES&S RESPONSE NO. 3 – VSTL COMMUNICATIONS

Attached are email exchanges between ES&S and Pro V&V regarding ES&S' request for an independent assessment regarding this matter. If additional files are identified we will provide them to the EAC.

From:	Pearson, Steve
To:	Hallett, Tim
Subject:	FW: Scope of Work
Date:	Thursday, October 1, 2020 6:00:13 PM
Attachments:	image001.png

From: Jack Cobb (b) (6)
Sent: Thursday, September 24, 2020 1:27 PM
To: McKay, Sue (b) (6) Pearson, Steve (b) (6)
Subject: Scope of Work

Pro V&V will perform an independent analysis for the "Update" product used to install the EV v1.0 firmware in Texas. Pro V&V will examine the "Update" product and compare it with the "prod_release" product that is the "Trusted Build" and perform addition comparison as necessary. When completed Pro V&V will prepare a report of their findings. This project is a time and material project (b) (4) per hour not to exceed 32 hours without written request and approval from ES&S.

Jack Cobb
6705 Odyssey Drive
Suite C
Huntsville, AL 35806
Office: (b) (6)
Fax: (b) (6)
Cell: (b) (6)

email logo

From: Pearson, Steve
To: Hallett, Tim
Subject: FW: Scope of Work
Date: Thursday, October 1, 2020 6:00:32 PM
Attachments: image001.png

From: Pearson, Steve
Sent: Thursday, September 24, 2020 4:19 PM
To: 'Jack Cobb' (b) (6)
Cc: McKay, Sue (b) (6)
Subject: RE: Scope of Work

Please proceed.

Thanks,
Steve

From: Jack Cobb (b) (6)
Sent: Thursday, September 24, 2020 1:27 PM
To: McKay, Sue (b) (6) Pearson, Steve (b) (6)
Subject: Scope of Work

Pro V&V will perform an independent analysis for the "Update" product used to install the EV v1.0 firmware in Texas. Pro V&V will examine the "Update" product and compare it with the "prod_release" product that is the "Trusted Build" and perform addition comparison as necessary. When completed Pro V&V will prepare a report of their findings. This project is a time and material project (b) (4) per hour not to exceed 32 hours without written request and approval from ES&S.

Jack Cobb
6705 Odyssey Drive
Suite C
Huntsville, AL 35806
Office: (b) (6)
Fax: (b) (6)
Cell: (b) (6)
email logo

Letter Report

To: Steve Pearson, Sue McKay – Election Systems & Software, LLC (ES&S)

From: Wendy Owens - Pro V&V, Inc.

CC: Jack Cobb, Stephen Han - Pro V&V, Inc.

Date: October 1, 2020

Subject: ES&S ExpressVote Hardware Version 1.0, Firmware Version 1.5.0.0 Update Process

---

Dear ES&S:

Pro V&V is providing this letter to report the results of the evaluation effort on the ES&S ExpressVote® hardware version 1.0, (ExpressVote HW1.0) firmware version 1.5.0.0 update process. An examination was performed to confirm that the update process utilized during the state evaluation contains identical executable files as those found in the trusted build and the process does not add any additional software to the ExpressVote HW1.0.

Background

Pro V&V was contacted by ES&S to analyze an anomaly that occurred during a Texas state evaluation of the ExpressVote HW1.0 running firmware version 1.5.0.0. Pro V&V has also been in contact with the U.S. Election Assistance Commission (EAC) and Texas Secretary of State regarding this evaluation. During the evaluation, the "Update" process was attempted and a hash value mismatch error was displayed for the sysload.bmp file.

Test Summary

Pro V&V compared the update disk image file to the prod_release disk image file from the Trusted Build to ensure the update disk image file contained the same files from the Trusted Build. Pro V&V used the ExamDiff Pro application with the PESnoop 2.0 plug-in to compare all files. Three files were found to be in the update disk image that were not in the prod_release disk image file. These files are listed below:

- InputOutputBoard.S19
- ScannerPrinterEngine.S19
- startup.exe

Pro V&V then compared the InputOutputBoard.S19 and ScannerPrinterEngine.S19 to the Trusted Build for EVS 6.0.0.0 where these artifacts were originally created. The SHA-256 hash values were the same as the files in the update disk image file. The startup.exe file was also hashed from EVS 6.0.0.0 and produced the following SHA-256 hash value:

startup.exe - 85f8d210ca9ad2433c4dbe154aee31f9d75968f908dc114e91adc26fd0f85731

Pro V&V then retrieved the sysload.bmp from EVS 5.2.2.0, as presented in Photograph 1.

Photograph 1: EVS 5.2.2.0 sysload.bmp

This file produces a SHA-256 value of the following:

sysload.bmp - b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3

The sysload.bmp file from EVS 6.0.2.0 was retrieved, as depicted in Photograph 2.

Photograph 2: EVS 6.0.2.0 sysload.bmp

This file produces a SHA-256 value of the following:

sysload.bmp - 07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12

In addition, Pro V&V upgraded a production EVS 5.2.2.0 ExpressVote HW1.0 device using an EVS 6.0.2.0 USB update image. Pro V&V followed the validation procedures detailed in the *Verification Procedure: ExpressVote Hardware 1.0* document to verify the hash values of all software on the device, noting the sysload.bmp verification was a mismatch. It was observed to have no impact on functionality.

After conducting this verification, Pro V&V loaded the EVS 6.0.2.0 prod_release image onto an additional ExpressVote HW1.0 device via an Innodisk. Pro V&V then performed the same validation procedures outlined previously and noted there were no verification discrepancies.

Conclusion

Based on the testing performed and the results obtained, it was verified that the only difference in the two products was the sysload.bmp file and no additional software was placed on the devices during the update process.

Should you require additional information or would like to discuss this matter further, please contact me at (b) (6).

Sincerely,

Wendy Owens

Wendy Owens
VSTL Program Manager
(b) (6)

From:	McKay, Sue
To:	Hallett, Tim
Subject:	FW: Texas ExpressVote Review Final Letter Report
Date:	Thursday, October 1, 2020 8:35:33 AM
Attachments:	ESS EV Letter Report-FINAL.pdf

From: Michael Walker (b) (6)
Sent: Thursday, October 01, 2020 8:07 AM
To: Pearson, Steve (b) (6) McKay, Sue (b) (6)
Cc: Jack Cobb (b) (6) Wendy Owens (b) (6)
Stephen Han (b) (6)
Subject: Texas ExpressVote Review Final Letter Report

Good morning,

Please find attached the final letter report for the ExpressVote Texas review. Please let us know if you have any questions or concerns. Thank you

Michael L. Walker
Pro V&V
6705 Odyssey Drive
Suite C
Huntsville, AL 35806
Office: (b) (6)
Fax: (b) (6)
Cell: (b) (6)

From:	McKay, Sue
To:	Hallett, Tim
Subject:	FW: Scope of Work
Date:	Thursday, October 1, 2020 4:56:33 PM
Attachments:	image001.png

From: Jack Cobb (b) (6)
Sent: Thursday, September 24, 2020 1:27 PM
To: McKay, Sue (b) (6) Pearson, Steve (b) (6)
Subject: Scope of Work

Pro V&V will perform an independent analysis for the "Update" product used to install the EV v1.0 firmware in Texas. Pro V&V will examine the "Update" product and compare it with the "prod_release" product that is the "Trusted Build" and perform addition comparison as necessary. When completed Pro V&V will prepare a report of their findings. This project is a time and material project (b) (4) per hour not to exceed 32 hours without written request and approval from ES&S.

Jack Cobb
6705 Odyssey Drive
Suite C
Huntsville, AL 35806
Office: (b) (6)
Fax: (b) (6)
Cell: (b) (6)

email logo

ES&S RESPONSE NO 4 - ADVISORY NOTICE

ExpressVote Copyright Bitmap Image Update

Product Advisory

Document ID:	FYIEXV20272
Product:	ExpressVote HW1.0
Versions Affected:	EVS 52XX, 53XX, 60XX, FLEVS 45XX
Publication Date:	October 2020
Distribution:	External

Scenario:

Some versions of ExpressVote hardware version 1.0 display an incorrect copyright image on the ExpressVote splash screen.

This copyright image has no impact to the performance and accuracy of the voting system.

Discussion:

Q: What is the effect of an incorrect copyright image?

Units which have the incorrect copyright (a bitmap image that indicates an incorrect year) will not provide a 100% match during hash validation.

Q: How did the wrong copyright image get there?

During either the initial installation process or subsequent update, a single copyright file (a bitmap image) did not transfer correctly to some ExpressVote HW1.0 units that were upgraded using the USB flash drive method.

Q: What does this mean in terms of the accuracy and performance of these units?

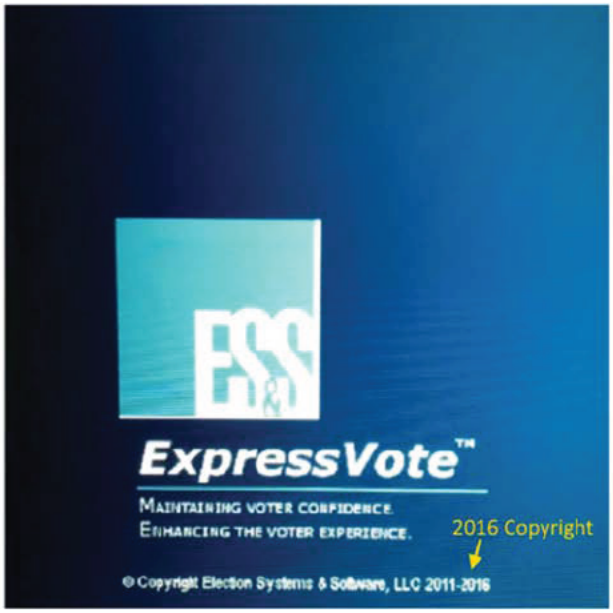
This issue has no impact on any accuracy, security or performance.

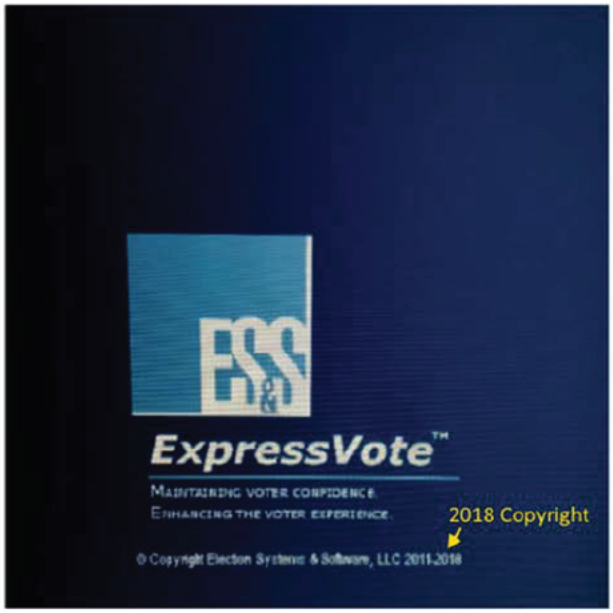
Q: How do I determine if my ExpressVote has the correct copyright image?

See a sample of two images below. The photo on the left shows an older copyright image, and the photo on the right shows a current copyright image. At the bottom of this advisory is a list of the correct copyright images for each version of the ExpressVote HW1.0. You should power on your ExpressVote and compare the copyright image on the screen to the list below to determine if the image displayed is correct for your certified software.

Note

If you need assistance with verifying if your copyright image is current for your version of software, please reach out to Technical Support or your Account Manager.





Q: If the copyright image is not correct what should I do?

For the ExpressVote to operate as expected, this does not need to be corrected. However, ES&S is working with each State election authority to determine when and how the copyright image will be corrected.

Q: How will corrections be put in place?

A firmware update will be applied to each identified unit to place the correct and latest copyright image onto your unit.

Q: Were any previous elections impacted or compromised by having the incorrect copyright screen?

No. The incorrect copyright image file has no impact on any previous elections, nor does it affect future elections.

Table 1-1: ExpressVote HW1.0 Copyright Information

EVS Voting System	Firmware Version	Correct Copyright Years
FL EVS 4500v4	1.2.3.0	2011 - 2013
EVS 5200 EVS 5300 EVS 5300 (IL) EVS 5303 EVS 5201 EVS 5202 EVS 5203 EVS 5204	1.4.0.0	2011 - 2014
EVS 5210 EVS 5310	1.4.1.0	2011 - 2015
EVS 5211	1.4.1.1	2011 - 2016
EVS 5220 EVS 5320	1.4.1.2	2011 - 2016
EVS 5321 EVS 5230 EVS 5330	1.4.1.6	2011 - 2017
EVS 5240 EVS 5340 EVS 5241 EVS 5341	1.4.1.7	2011 - 2018
FL EVS 4520v1	1.4.2.0	2011 - 2015
FL EVS 4530v1	1.4.3.0	2011 - 2017
FL EVS 4530v2	1.4.3.1	2011 - 2018
EVS 6000 EVS 6010 EVS 6020 EVS 6030	1.5.0.0	2011 - 2018
EVS 6021 EVS 6030	1.5.1.0	2011 - 2018
EVS 6040 EVS 6043	1.5.2.0	2011 - 2018

Table 1-1: ExpressVote HW1.0 Copyright Information (Continued)

EVS Voting System	Firmware Version	Correct Copyright Years
EVS 6040 AZ	1.5.2.1	2011 - 2019
EVS 6050 EVS 6051	1.5.3.0	2011 - 2019

Technical Support

For additional technical support, contact ES&S.

Telephone: (b) (6)
Fax: (b) (6)
Email: (b) (6)

Support representatives are available Monday through Friday, between 7:00 a.m. and 7:00 p.m. Central Time.

ES&S support services are subject to the prices, terms, and conditions in place at the time of service.

ES&S RESPONSE NO. 4

ExpressVote HW1.0 Copyright Information

EVS Release	FW Version	Copyright YRS	Hash Value
FL EVS 4500v4	1.2.3.0	2011 - 2013	f67dbc52fe9c5e65ad786740ca07388e864fc00aaabcb6e0169b44c485356101
EVS 5200 EVS 5300 EVS 5303 EVS 5300 (IL) EVS 5201 EVS 5202 EVS 5203 EVS 5204	1.4.0.0	2011 - 2014	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
EVS 5210 EVS 5310	1.4.1.0	2011 - 2015	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
EVS 5211	1.4.1.1	2011 - 2016	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
EVS 5220 EVS 5320	1.4.1.2	2011 - 2016	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
EVS 5321 EVS 5230 EVS 5330	1.4.1.6	2011 - 2017	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
EVS 5240 EVS 5340 EVS 5241 EVS5341	1.4.1.7	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
FL EVS 4520v1	1.4.2.0	2011 - 2015	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
FL EVS 4530v1	1.4.3.0	2011 - 2017	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
FL EVS 4530v2	1.4.3.1	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
EVS 6000 EVS 6010 EVS 6020 EVS 6030	1.5.0.0	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
EVS 6021 EVS 6030	1.5.1.0	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
EVS 6040 EVS 6043	1.5.2.0	2011 - 2018	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
EVS 6040 AZ	1.5.2.1	2011 - 2019	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
EVS 6050 EVS 6051	1.5.3.0	2011 - 2019	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

ES&S RESPONSE NO. 5 - COMMUNICATION TO AFFECTED JURISDICTIONS

FAQ Regarding the ExpressVote Copyright BitMap Image Update
Revised Oct 1, 2020

Q: What is the situation?

Some ExpressVote 1.0 ballot marking devices display a copyright image with the wrong date on the splash screen when the unit is powered up. ***This does not, has not, and will not impact any function of the machine, which has been proven to be and will continue to be secure, accurate and reliable.*** This copyright image is meaningless in regard to unit performance.

Q: What is the effect of an incorrect copyright image?

Units which have the incorrect copyright – a bitmap image that simply indicates an incorrect year - will not provide a 100% firmware hash validation match.

Every ExpressVote unit operates as designed and tested. The security, accuracy and reliability of the system are proven and documented through numerous EAC federal certifications and extensive post-election audits. The incorrect copyright bitmap file image is cosmetic in nature.

Q: I've heard the term hash validation —what does that mean?

A hash validation is designed to ensure data integrity. It is an independent check and validation which verifies that the firmware on the unit matches the version of the firmware that was federally, and state tested and approved.

Q: How did the wrong copyright image get there?

When some ExpressVote 1.0 units were last updated with the latest firmware, one file —the file containing the copyright image—did not correctly update.

Q: Why did it not correctly update?

During either the initial installation process or subsequent upgrade, a single copyright file (a bitmap photo) did not correctly transfer to some ExpressVote 1.0 units that were upgraded via a USB drive.

Q: How do we know this is the only thing that didn't correctly update?

ES&S commissioned an independent analysis by a NIST-accredited Voting System Test Laboratory (VSTL) to confirm the root cause of the hash validation mismatch stems from the incorrect copyright image photo. The analysis will further confirm that the incorrect copyright image has zero impact on the operation of the voting system and that all system files – with the exception if the copyright image - match exactly. The report will be made available to customers upon receipt.

Q: What does this mean in terms of the accuracy and performance of these units?

This issue has zero impact on any accuracy, security, or performance.

Q: Does this need to be corrected?

For the ExpressVote to operate as expected, this does not need to be corrected, however ES&S will work with each State Election Authority to determine the State's requirements as it relates to the timing of applying the correct bitmap image. The current file image has zero impact on the performance, accuracy, or security of the units.

Q: Were any previous elections impacted or compromised by having the incorrect copyright screen?

No. The incorrect copyright image file has no impact on any previous elections, nor does it affect future elections.

Q: How and when was this issue discovered?

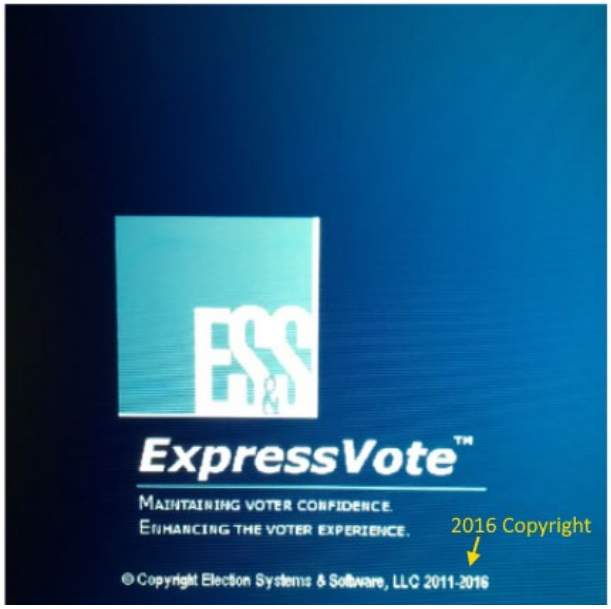
During a recent certification event in Texas, one of the examiners noticed the firmware on some units was not an exact match to standards. ES&S immediately worked to investigate the issue.

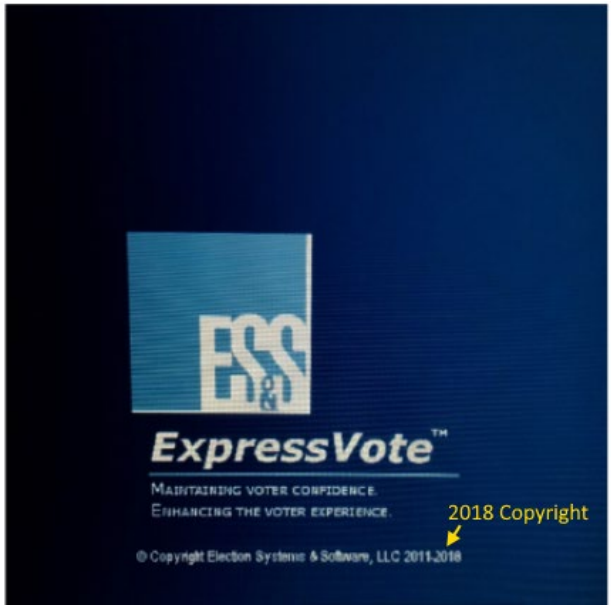
Q: How will corrections be put in place?

A firmware update will be applied to each identified unit to correct the single file image. Following the upgrade, a hash validation will be performed to confirm the correction was applied.

Q: What does this issue look like?

See the two images below. The image on the left shows an older copyright image, and the photo on the right shows a current copyright image.





ES&S appreciates the work that is done by the nation's Election Officials and we pledge to work with our customers to ensure that elections are accurate, secure and fully transparent. If you have any questions regarding the information contained within this FAQ, please don't hesitate to reach out to your ES&S representative.

ES&S RESPONSE NO. 6 – DESCRIPTION OF WHAT OCCURED

During State of Texas certification testing of EVS 6.0.3.0 the hash validation process when performed on the ExpressVote Hardware Version 1.0 reported the copyright bitmap image file as an exception and not matching the hash value of that file created by the VSTL at the time of EAC certification of ExpressVote Hardware Version 1.0 application firmware version 1.5.0.0 as part of the EVS 6.0.3.0 voting system release. ES&S immediately initiated an analysis of this exception condition which has resulted in the findings shown below.

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date, such as 2011 – 2015. When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware during use by a voter during the ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware. The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update the application firmware.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the sysload.bmp file is reported as an exception.

ES&S RESPONSE NO. 7 – TEXAS SOS LETTER

Upon further review and communication with the EAC, ES&S understands the Texas Secretary of State's position set forth in its September 24, 2020 letter.

ES&S RESPONSE NO. 8 – TEXAS INSTALLATION

The following 18 Texas Counties with Version 1 ExpressVote had their inno disks replaced to update the copyright bitmap file. Twenty-one ES&S associates were assigned and completed the work on October 1, 2020.

1. Blanco
2. Kinney
3. Nolan
4. Sutton
5. Childress
6. Hemphill
7. Carson
8. Bowie
9. Navarro
10. Kaufman
11. Franklin
12. Jackson
13. Rockwall
14. Clay
15. Erath
16. Hockley
17. Brewster
18. Presidio

ES&S RESPONSE NO. 9 - OTHER JURISDICTIONS INSTALLATION PLAN

ES&S is sending a team to Tennessee to replace Inno disks in the following counties to resolve the copyright issue. ES&S plans to complete the replacement by October 6, 2020.

Chester County, Tennessee
Hardin County, Tennessee
McNairy County, Tennessee
Pickett County, Tennessee
Weakley County, Tennessee
Wilson County, Tennessee

ES&S RESPONSE NO. 10 – PLANNED RESOLUTION

ES&S will include with all future certification submissions specific detailed validation procedures within its Technical Data Package ("TDP"). These validation procedures will specifically set forth the hash verification process for both the Production Image trusted build and the Update Image trusted build. ES&S will specifically request that the Voting System Test Lab ("VSTL") complete comprehensive hash verification on both trusted builds to ensure all files are correct, match and that each update method may be used upon approval by the EAC. Once the hash verification has been completed for both the Production Image trusted build and the Update Image trusted build, ES&S will request the trusted hashes from the VSTL and include those trusted hashes in the Verification Pack which is a component of the TDP. This Verification Pack which includes all trusted hashes will be sent to the VSTL and the EAC with the final TDP. Once the VSTL provides ES&S with the final trusted build executables for both the Production Image and the Update Image, ES&S will place these files in a secure repository within its Configuration Management Department. ES&S' Configuration Management Department shall be responsible to ensure that only the trusted build executables for both the Production Image and Update Image will be provided when an ES&S customer's voting system is being updated after such version has been approved for use in the applicable jurisdiction.

In addition, ES&S will revise its documentation set forth in its maintenance manual to include installation instructions on how to update its voting system through either the internal solid state drive method or the USB flash drive update method. These instructions will provide step by step processes for each update method.

ES&S RESPONSE NO. 11 – COMMUNICATION PLAN

Monday, September 28 - ES&S began outreach to all State Election Authorities that have certified ExpressVote hardware 1.0 for use. These identified States were informed that jurisdictions in their State who had ExpressVote 1.0 units fielded were either a) not affected or b) likely affected. ES&S provided each State with a written FAQ describing the issue. *The same FAQ was provided to the EAC on September 29.

Monday, September 28 – ES&S began the process of having jurisdictions review the copyright dates to determine if their units were affected. This process is ongoing, and instructions for performing the verification are also included in the Product Advisory Notice. ES&S is documenting the verification information received from each jurisdiction and will make the full, confirmed list available to the EAC upon completion. We will also provide the EAC updates on a regular basis.

Wednesday, September 30 – ES&S completed initial outreach to the State Election Authorities to inform them of the issue.

Thursday, October 1 – ES&S completed a Product Advisory Notice to be provided to all potentially affected customers (Advisory included with this response). The Advisory will be provided to customers immediately upon review and approval of the verbiage by the EAC.

*Please note that the FAQ has been revised and will be re-distributed to State Election Authorities as a replacement to the original version. The revised copy is included in this communication.

ELECTION Systems & Software

Engineering Change Order

ECO#	1100	**Requested by**	Steve Pearson	Date: 10/6/2020
Hardware	EV 1.0	**Product Owner**	Dean Baumert	

Description:

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015. When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware. The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update the application firmware and the two board level firmware: Scanner Printer Engine (SPE) board and Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components. The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote

HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Certification Impact

Impact on hardware configuration, list of tests performed, recommended federal cert strategy, approach to state cert (N.E.W.S).

1. Submit to VSTL: ☑ Yes ☐ No

2. Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

Results when ExpressVote Firmware Hash Does Not Match

Information Sheet

Document ID:	ECO 1100 - Appendix
Product:	ExpressVote HW1.0
Publication Date:	October 7, 2020
Distribution:	External

Description:

During the ExpressVote verification process, when the Firmware Hash File does not match the Trusted Hash File, a difference report is generated.

The name of the difference report fits the form **ExpressVote- Identification_Report.txt**, where "ExpressVote- Identification" is the unique identifier that was supplied when VerifyHash.sh was executed (see ExpressVote Verification Procedures for more information.)

When reviewing the difference report, keep the following item in mind:

- Although every attempt was made to ensure all dynamic files and folders are filtered, it is possible that the difference is caused by the following file/folder types:
  - Report file
  - Log file
  - Bitmap file

Note

If the difference report contains the entries listed below, it is possible that the difference is caused as a result of the firmware being burned on a Windows 10 machine.

/part1/System Volume Information/IndexerVolumeGuid

/part1/System Volume Information/WPSettings.dat

Note

If the difference report contains the entries listed below, these differences may occur during the normal Export operation.

Caution

If it is confirmed that the difference is caused by a static file, the only course of action that can be taken is to restore the ExpressVote by reinstalling the firmware from a trusted source.

Dynamic File Reference

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

Dynamic File History

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

	ENGINEER CHANGE ORDER (ECO) ANALYSIS FORM
Manufacturer:	Election Systems & Software (ES&S)
System:	ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0)
ECO Number:	1100
ECO Description:	Update Process Verification

Overview:
An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build and the process does not add any additional software to the ExpressVote HW1.0.

Components Affected: ExpressVote HW1.0

Affected Systems:
Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043
State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Supporting Documentation:
Original ECO 1100 - EV 1.0 Copyright Information Final 10.6.20.pdf *(ES&S ECO)*
ECO1100_Appendix.pdf *(Results when ExpressVote Firmware Hash Does Not Match)*

Engineering Analysis:
Pro V&V analyzed the system architecture of the ExpressVote HW1.0. The sysload.bmp file is called by the bootloader(BLDR) process in the course of a device booting up. This file can be found in the root of the prod_release.IMG file that is the Trusted Build firmware. The process for installing the prod_release.img for use by the device is to "burn" the prod_release.img image to a Universal Serial Bus Embedded Disk Card (USB EDC). Once the USB EDC is "burnt", the mounting area must be unlocked and the cover must be removed from the device. This USB EDC has to mount on 9 pins on the device. This process requires a screw driver, 5.5 millimeter bit driver, and has to be done carefully to ensure the pins are all mounted and no pin is bent.

USB EDC

An alternative to this method is to run an "Update". This process utilizes a different disk file image. The update.img file that is created during the Trusted Build process can be burnt to a USB flash drive and inserted into the USB ports located on the left side of the device. This process does not update the operating system, but does update the application software and the two firmware components InputOutputBoard.S19 and ScannerPrinterEngine.S19.

It has been discovered that the update process does not update the sysload.bmp. This causes an issue where the last sysload.bmp placed on the USB EDC will remain even if the update process is run for one or more versions.

Engineering Recommendation:
Pro V&V believes because all seven sysload.bmp files have been EAC certified and they are only used to display the copyright information while the device is booting, this should be a De Minimus change. It is Pro V&V's conclusion that the systems listed in this ECO Analysis could remain certified if running any of the following sysload.bmp files:

***Note some of the SHA-256 hashes are the same because the sysload.bmp is used in multiple versions.

EV 1.0 Firmware Version	SHA-256 Hash
1.4.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

Reviewer:	**Approver:**
Jack Cobb	Wendy Owens
Printed Name	Printed Name
Jack Cobb	Wendy Owens
Signature	Signature
10/12/2020	10/12/2020
Date	Date

ELECTION Systems & Software

Engineering Change Order

ECO#	1100	**Requested by**	Steve Pearson	Date: 10/6/2020
Hardware	EV 1.0	**Product Owner**	Dean Baumert	

Description:

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015. When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware. The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update the application firmware and the two board level firmware: Scanner Printer Engine (SPE) board and Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components. The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote

HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Certification Impact

Impact on hardware configuration, list of tests performed, recommended federal cert strategy, approach to state cert (N.E.W.S).

1. Submit to VSTL: ☑ Yes ☐ No

2. Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

Results when ExpressVote Firmware Hash Does Not Match

Information Sheet

Document ID:	ECO 1100 - Appendix
Product:	ExpressVote HW1.0
Publication Date:	October 7, 2020
Distribution:	External

Description:

During the ExpressVote verification process, when the Firmware Hash File does not match the Trusted Hash File, a difference report is generated.

The name of the difference report fits the form **ExpressVote- Identification_Report.txt**, where "ExpressVote- Identification" is the unique identifier that was supplied when VerifyHash.sh was executed (see ExpressVote Verification Procedures for more information.)

When reviewing the difference report, keep the following item in mind:

- Although every attempt was made to ensure all dynamic files and folders are filtered, it is possible that the difference is caused by the following file/folder types:
  - Report file
  - Log file
  - Bitmap file

Note

If the difference report contains the entries listed below, it is possible that the difference is caused as a result of the firmware being burned on a Windows 10 machine.

/part1/System Volume Information/IndexerVolumeGuid

/part1/System Volume Information/WPSettings.dat

Note

If the difference report contains the entries listed below, these differences may occur during the normal Export operation.

Caution

If it is confirmed that the difference is caused by a static file, the only course of action that can be taken is to restore the ExpressVote by reinstalling the firmware from a trusted source.

Dynamic File Reference

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

Dynamic File History

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-5200*

ES&S EVS version 5.2.0.0

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***5.2.0.0***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance℠
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 5.2.0.0** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 5.2.0.0** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- 5b465b87ff25679a05490893bb867bf962b488825967a88d3171eea2c611b2ba

The verified SHA-256 hash of the Update Image file is:

- bb226cce225d4a324da7167aa36e0fa8790aadafc218c5ae35cf0d111adb8c2a

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
5.2.0.0	1.4.0.0	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

Of the file(s) noted in "Table 3 – Dynamic Files expected in release" for this release, none were seen during the examination. Given different update paths, the files listed in the table may be seen by a jurisdiction. Note that no associated hash codes are given for dynamic files, as by their nature the file is constantly changing and as a result their hash code is constantly changing.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-5203*

ES&S EVS version 5.2.0.3

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***5.2.0.3***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance[SM]
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Update for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 5.2.0.3** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 5.2.0.3** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- 5b465b87ff25679a05490893bb867bf962b488825967a88d3171eea2c611b2ba

The verified SHA-256 hash of the Update Image file is:

- bb226cce225d4a324da7167aa36e0fa8790aadafc218c5ae35cf0d111adb8c2a

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
5.2.0.3	1.4.0.0	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

Of the file(s) noted in "Table 3 – Dynamic Files expected in release" for this release, none were seen during the examination. Given different update paths, the files listed in the table may be seen by a jurisdiction. Note that no associated hash codes are given for dynamic files, as by their nature the file is constantly changing and as a result their hash code is constantly changing.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-5210*

ES&S EVS version 5.2.1.0

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***5.2.1.0***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance[SM]
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 5.2.1.0** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 5.2.1.0** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\Simg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- 5b465b87ff25679a05490893bb867bf962b488825967a88d3171eea2c611b2ba

The verified SHA-256 hash of the Update Image file is:

- 111e25710cd4658e7e152220b027487e0b23e0816a06694ccfb6e187ece725d5

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
5.2.1.0	1.4.1.0	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

Of the files noted in "Table 3 – Dynamic Files expected in release" for this release only "firstboot.txt" was seen during the examination. Given different update paths, the files listed in the table may be seen by a jurisdiction. Note that no associated hash codes are given for dynamic files, as by their nature the file is constantly changing and as a result their hash code is constantly changing.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-5220*

ES&S EVS version 5.2.2.0

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***5.2.2.0***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance℠
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 5.2.2.0** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 5.2.2.0** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- 4c50d0fd702b94938a39ad9a887668bd1aa50f62aae657bde4b81d984dadbb5f

The verified SHA-256 hash of the Update Image file is:

- 6c8a7ef02c9171bf2c5f1e3ddabd7e0eae2fbdff8909e44dfc1e26253d852ce5

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
5.2.2.0	1.4.1.2	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

Of the file(s) noted in "Table 3 – Dynamic Files expected in release" for this release, none were seen during the examination. Given different update paths, the files listed in the table may be seen by a jurisdiction. Note that no associated hash codes are given for dynamic files, as by their nature the file is constantly changing and as a result their hash code is constantly changing.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-5240*

ES&S EVS version 5.2.4.0

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***5.2.4.0***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance[SM]
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 5.2.4.0** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 5.2.4.0** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- 7c7fddff50ea6cbaefba7646cdaaffe4037b9c0fed3bbb682d092b217e19641e

The verified SHA-256 hash of the Update Image file is:

- 6ef7ef7a523b54151bf156ca7148fb1fa39d08ed17d8ef04325f549bbf9fb9d7

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
5.2.4.0	1.4.1.7	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

No files were listed in "Table 3 – Dynamic Files expected in release" for this release, and none were seen.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-5241*

ES&S EVS version 5.2.4.1

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***5.2.4.1***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance℠
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 5.2.4.1** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 5.2.4.1** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- 7c7fddff50ea6cbaefba7646cdaaffe4037b9c0fed3bbb682d092b217e19641e

The verified SHA-256 hash of the Update Image file is:

- 6ef7ef7a523b54151bf156ca7148fb1fa39d08ed17d8ef04325f549bbf9fb9d7

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
5.2.4.1	1.4.1.7	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

No files were listed in "Table 3 – Dynamic Files expected in release" for this release, and none were seen.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-5320*

ES&S EVS version 5.3.2.0

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***5.3.2.0***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance[SM]
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 5.3.2.0** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 5.3.2.0** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- 4c50d0fd702b94938a39ad9a887668bd1aa50f62aae657bde4b81d984dadbb5f

The verified SHA-256 hash of the Update Image file is:

- 6c8a7ef02c9171bf2c5f1e3ddabd7e0eae2fbdff8909e44dfc1e26253d852ce5

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
5.3.2.0	1.4.1.2	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

Of the file(s) noted in "Table 3 – Dynamic Files expected in release" for this release, none were seen during the examination. Given different update paths, the files listed in the table may be seen by a jurisdiction. Note that no associated hash codes are given for dynamic files, as by their nature the file is constantly changing and as a result their hash code is constantly changing.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-5340*

ES&S EVS version 5.3.4.0

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***5.3.4.0***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance[SM]
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 5.3.4.0** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 5.3.4.0** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- 7c7fddff50ea6cbaefba7646cdaaffe4037b9c0fed3bbb682d092b217e19641e

The verified SHA-256 hash of the Update Image file is:

- 6ef7ef7a523b54151bf156ca7148fb1fa39d08ed17d8ef04325f549bbf9fb9d7

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
5.3.4.0	1.4.1.7	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

No files were listed in "Table 3 – Dynamic Files expected in release" for this release, and none were seen.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-5341*

ES&S EVS version 5.3.4.1

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***5.3.4.1***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance℠
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 5.3.4.1** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 5.3.4.1** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- 7c7fddff50ea6cbaefba7646cdaaffe4037b9c0fed3bbb682d092b217e19641e

The verified SHA-256 hash of the Update Image file is:

- 6ef7ef7a523b54151bf156ca7148fb1fa39d08ed17d8ef04325f549bbf9fb9d7

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
5.3.4.1	1.4.1.7	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

No files were listed in "Table 3 – Dynamic Files expected in release" for this release, and none were seen.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-6000*

ES&S EVS version 6.0.0.0

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***6.0.0.0***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance℠
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 6.0.0.0** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 6.0.0.0** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- d4f7abc7ed486b469d59823d713c6f77c0f83c6b31e067a2bb6654c9a9c78910

The verified SHA-256 hash of the Update Image file is:

- e2f7d671c9a8859a0f275419205ac92e7a3815a27f659a6daa2054c2840121b0

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
6.0.0.0	1.5.0.0	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

Of the file(s) noted in "Table 3 – Dynamic Files expected in release" for this release, none were seen during the examination. Given different update paths, the files listed in the table may be seen by a jurisdiction. Note that no associated hash codes are given for dynamic files, as by their nature the file is constantly changing and as a result their hash code is constantly changing.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-6020*

ES&S EVS version 6.0.2.0

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***6.0.2.0***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance℠
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 6.0.2.0** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 6.0.2.0** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\Simg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
  - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- d4f7abc7ed486b469d59823d713c6f77c0f83c6b31e067a2bb6654c9a9c78910

The verified SHA-256 hash of the Update Image file is:

- e2f7d671c9a8859a0f275419205ac92e7a3815a27f659a6daa2054c2840121b0

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
6.0.2.0	1.5.0.0	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

Of the file(s) noted in "Table 3 – Dynamic Files expected in release" for this release, none were seen during the examination. Given different update paths, the files listed in the table may be seen by a jurisdiction. Note that no associated hash codes are given for dynamic files, as by their nature the file is constantly changing and as a result their hash code is constantly changing.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-6030*

ES&S EVS version 6.0.3.0

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***6.0.3.0***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance℠
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 6.0.3.0** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 6.0.3.0** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\Simg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- d4f7abc7ed486b469d59823d713c6f77c0f83c6b31e067a2bb6654c9a9c78910

The verified SHA-256 hash of the Update Image file is:

- e2f7d671c9a8859a0f275419205ac92e7a3815a27f659a6daa2054c2840121b0

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
6.0.3.0	1.5.0.0	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

Of the file(s) noted in "Table 3 – Dynamic Files expected in release" for this release, none were seen during the examination. Given different update paths, the files listed in the table may be seen by a jurisdiction. Note that no associated hash codes are given for dynamic files, as by their nature the file is constantly changing and as a result their hash code is constantly changing.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-6040*

ES&S EVS version 6.0.4.0

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***6.0.4.0***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance[SM]
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 6.0.4.0** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 6.0.4.0** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
  - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- df9d5106444141a3d21189261e52a844dc0eff4c8f0d945c1bd4b1a382a2613c

The verified SHA-256 hash of the Update Image file is:

- 13ce4df4e5c393885e1f42a84f0392b7f641a56f296d84b1760f4af7bc5e0ef5

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
6.0.4.0	1.5.2.0	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

Of the file(s) noted in "Table 3 – Dynamic Files expected in release" for this release, none were seen during the examination. Given different update paths, the files listed in the table may be seen by a jurisdiction. Note that no associated hash codes are given for dynamic files, as by their nature the file is constantly changing and as a result their hash code is constantly changing.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-6040AZ*

ES&S EVS version 6.0.4.0AZ

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***6.0.4.0AZ***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance[SM]
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 6.0.4.0AZ** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 6.0.4.0AZ** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\Simg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
  - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- a6788abef2d3737a827938c62514991a2346cd6973cb70f51308cfab70aaf652

The verified SHA-256 hash of the Update Image file is:

- 0f8efeebdbc677f72be5683888f74aefc91c5500ba32f9ab49ffadf3ef46a766

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
6.0.4.0AZ	1.5.2.1	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

Of the file(s) noted in "Table 3 – Dynamic Files expected in release" for this release, none were seen during the examination. Given different update paths, the files listed in the table may be seen by a jurisdiction. Note that no associated hash codes are given for dynamic files, as by their nature the file is constantly changing and as a result their hash code is constantly changing.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-6043*

ES&S EVS version 6.0.4.3

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***6.0.4.3***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance[SM]
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 6.0.4.3** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 6.0.4.3** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\Simg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- df9d5106444141a3d21189261e52a844dc0eff4c8f0d945c1bd4b1a382a2613c

The verified SHA-256 hash of the Update Image file is:

- 13ce4df4e5c393885e1f42a84f0392b7f641a56f296d84b1760f4af7bc5e0ef5

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
6.0.4.3	1.5.3.0	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

No files were listed in "Table 3 – Dynamic Files expected in release" for this release, and none were seen.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-6050*

ES&S EVS version 6.0.5.0

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***6.0.5.0***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance℠
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS 6.0.5.0** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS 6.0.5.0** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
  - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- 1314ae73043e6942e46ea5a4716222c499002cf28c777cc37b905115b288472d

The verified SHA-256 hash of the Update Image file is:

- 1c28ef9639cc42b2a543f7721fd2bd48aed5b80810dd4caa50dfc44437b2f6d9

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
6.0.5.0	1.5.3.0	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

No files were listed in "Table 3 – Dynamic Files expected in release" for this release, and none were seen.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-FL4520v1r2*

ES&S EVS version FL4.5.2.0v1r2

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***FL4.5.2.0v1r2***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance℠
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS FL4.5.2.0v1r2** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS FL4.5.2.0v1r2** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\Simg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
  - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only

    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- efc65feba37b21c6e5236ca31c2a6187e63fb31b86cc4f4072047d7842724e72

The verified SHA-256 hash of the Update Image file is:

- 696f672348e6366607b356183c98ad1ca39e700d691824a2376515af9ffefa0b

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
4.5.2.0v1r2 FL	1.4.2.0	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

Of the files noted in "Table 3 – Dynamic Files expected in release" for this release only "firstboot.txt" was seen during the examination. Given different update paths, the files listed in the table may be seen by a jurisdiction. Note that no associated hash codes are given for dynamic files, as by their nature the file is constantly changing and as a result their hash code is constantly changing.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-FL4530v1r2*

ES&S EVS version FL4.5.3.0v1r2

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***FL4.5.3.0v1r2***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance℠
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS FL4.5.3.0v1r2** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS FL4.5.3.0v1r2** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\SImg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
  - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only

    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- 1733d8aaba00395a5e6228b62cd7f817c3d00938fc672333a278f29596d11104

The verified SHA-256 hash of the Update Image file is:

- 7029f19bffed412cbb4fde055817bca1cc0de8d554a08446cb2e066fd7f36264

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
4.5.3.0v1r2 FL	1.4.3.0	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

No files were listed in "Table 3 – Dynamic Files expected in release" for this release, and none were seen.

End of Test Report

ExpressVote HW 1.0 Firmware Update Examination Report

Report Number *ESS-102020-ETR-FL4530v2r3*

ES&S EVS version FL4.5.3.0v2r3

Examination Report version 1.0

October 12th, 2020

Prepared for:

Vendor Name	***Election Systems and Software (ES&S)***
Vendor System	***FL4.5.3.0v2r3***
Vendor Address	***11208 John Galt Boulevard*** ***Omaha, Nebraska 68137***

Prepared by:

SLI Compliance℠
4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

NVLAP TESTING
NVLAP Lab Code 200733-0

Accredited by the National Institute of Standards and Technology (NIST) National Voluntary Lab Accreditation Program (NVLAP), and accredited by the Election Assistance Commission (EAC) for VSTL status.

Revision History

Release	Author	Revisions
v1.0	M. Santos	Initial Release
v2.0	M. Santos	Updated for clarification

Disclaimer

The Certification Test results reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government. Results herein relate only to the items tested.

Trademarks

- SLI is a registered trademark of SLI Compliance, a Division of Gaming Laboratories International, LLC.
- All other products and company names are used for identification purposes only and may be trademarks of their respective owners.

The tests referenced in this document were performed in a controlled environment using specific systems and data sets, and results are related to the specific items tested. Actual results in other environments may vary.

Opinions and Interpretations

There are no SLI opinions or interpretations included in this report.

TABLE OF CONTENTS

1 Introduction

SLI Compliance is submitting this test report as a summary of the examination efforts for the **ES&S EVS FL4.5.3.0v2r3** voting system, for the purpose of examining the ES&S ExpressVote Universal Voting System Hardware 1.0 (ExpressVote HW1.0) application firmware update process. An examination was performed to confirm that the update process documented in ES&S Engineering Change Order (ECO) 1100 results in identical executable files as those found in the trusted build, that the process does not add any additional software to the ExpressVote HW1.0, and that any messages indicating a mismatch of hash codes for any given file, and in particular the "sysload.bmp" file which contains a system copyright, are benign with no unintended or malicious results impacting the voting system.

This effort included examination of the Update Image method, application firmware version (as stated in Table 1 – Sysload.bmp files) of the **EVS FL4.5.3.0v2r3** voting system, which is utilized to perform field updates on the ExpressVote HW 1.0 component**.** ExpressVote HW1.0 is a hybrid paper-based polling place voting device that provides touch screen vote capture that incorporates the printing of the voter's selections as a cast vote record, to be scanned for tabulation in any one of the ES&S precinct or central scanners.

The review and examination were performed at SLI's Wheat Ridge, Colorado facility.

1.1 References

1. Election Assistance Commission Voluntary Voting System Guidelines version 1.0 (EAC VVSG 1.0), Volumes I & II
2. NIST NVLAP Handbook 150: 2016
3. NIST NVLAP Handbook 150-22: 2017
4. EAC Voting System Testing and Certification Program Manual, United States Election Assistance Commission, v 2.0, May 2015
5. EAC Voting System Test Laboratory Program Manual, United States Election Assistance Commission, v 2.0, May 2015
6. SLI VSTL Quality System Manual, v 3.2, prepared by SLI, June 8, 2020

2 Overview

2.1 The Installation Methods for ExpressVote Hardware Version 1.0

There are two methods for updating the system components on the ExpressVote HW1.0.

One method uses the Production Image (prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit.

The Production Image contains the full WinCE operating system, the application firmware and the "sysload.bmp" bit map file. The only items not included in the Production Image are the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files).

Note that this image is populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0 using menu items available only to credentialed users.

The Update Image contains the application firmware, along with the Scanner Printer Engine (SPE) board and the Input Output (IOB) board (represented as .S19 files). Note that the Update Image does not contain the "sysload.bmp" file.

Note that the Production Image method requires the user to remove, reburn and then re-install the internal eUSB device within the unit. This can be a time-consuming process.

The Update Image method is much faster and does not require access to any internal hardware components.

2.2 Engineering Change Order (ECO) 1100

At boot-up, the ExpressVote Hardware Version 1.0 (ExpressVote HW1.0) momentarily displays a copyright bitmap file during the power on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range with two years reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process. At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file as part of the hash validation processes and that reference is only done to generate a hash value of the contents of the file and to initiate a copy of the file to external USB media to facilitate the hash validation process performed external to the ExpressVote HW1.0.

There are two methods for updating the system components on the ExpressVote HW1.0. One method uses the Production Image

(prod_release.img) output during the Trusted Build process and gets loaded directly to the eUSB device that resides internally within the ExpressVote HW1.0 unit. This Production Image contains the full Win CE operating system and the application firmware. This image is also populated with the correct copyright bitmap file (sysload.bmp) for each respective certified version of application firmware.

The second method to update the system components is to use the Update Image (update.img) output during the Trusted Build process. This image is placed on a USB flash drive and then inserted into the ExpressVote HW1.0. By using menu items available only to credentialed users, the Update Image on the USB flash drive can then be used to update

- the application firmware

and the two board level firmware:

- Scanner Printer Engine (SPE) board and
- Input Output (IOB) board represented as .S19 files in the USB Update Image.

The Update Image method, which uses a USB flash drive, is the method most commonly used to update the ExpressVote HW1.0 with new application firmware. This is because the Production Image method requires the user to remove, reburn and then reinstall the internal eUSB device within the unit. The Update Image method is much faster and does not require access to any internal hardware components.

The USB Update Image must be used to update the SPE and IOB firmware if that firmware is updated in any release or the ExpressVote HW1.0 unit needs to be updated with the correct version of SPE or IOB firmware.

The Update Image output does not contain the copyright bitmap file, sysload.bmp. Therefore, ExpressVote HW1.0 units originally updated using the full Production Image method but then later updated using the Update Image method can result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect ***(copyright)*** bitmap file on the eUSB, the sysload.bmp file is reported as an exception. The hash check value of the sysload.bmp resident on the ExpressVote HW1.0 eUSB will validate against one of the seven certified iterations of the sysload.bmp files that have been created during the lifetime of the ExpressVote HW1.0.

In addition, ES&S is providing a list of other known dynamic files and folders which may result as an exception when a hash verification is completed on the ExpressVote HW1.0 units. These dynamic file and folder exceptions are known and do not affect the functionality of the ExpressVote HW1.0 units. A detailed explanation of the dynamic files and folders is provided in the Appendix to this ECO.

ES&S is requesting that all certified iterations of the sysload.bmp files that have been part of previous EAC certification events be deemed as applicable to all certified versions of the ExpressVote HW1.0 application firmware based upon review and approval of this Software ECO. As previously stated, this copyright bitmap file has no functionality in the system other than being briefly displayed on the screen by the BIOS bootloader at power up and is only referenced by the ExpressVote HW1.0 application firmware by credentialed users as part of the hash validation processes.

Affected Systems:

Federal: EVS 5200, EVS 5203, EVS 5210, EVS 5220, EVS 5240, EVS 6000, EVS 6020, EVS 6030, EVS 6040, EVS 6043

State: EVS 5241, EVS 5320, EVS 5340, EVS 5341, EVS 6040 AZ, EVS 6050, FL EVS 4520 v1r2, FL EVS 4530 v1r2, FL EVS 4530 v2r3

Test to: 2005 V 1.0 VVSG Standards

2.3 The Issue

At boot-up, the ExpressVote HW1.0 momentarily displays a copyright bitmap file during the power-on and OS load sequence. This copyright bitmap is represented in a file named sysload.bmp and contains a copyright date range reflecting the original copyright date through the current date of certification, such as 2011 – 2015.

When necessary, this file is updated to reflect new years of applicability. This bitmap image file is displayed on the ExpressVote HW1.0 screen by the BIOS bootloader (BLDR) for a few seconds at the beginning of the ExpressVote HW1.0 boot-up process.

At the end of the boot-up process, the ExpressVote HW1.0 application firmware is initiated.

There is no reference to this copyright bitmap file during the execution of the ExpressVote HW1.0 application firmware for a voter's ballot marking session. The application firmware only references this file during the USB export step of the hash validation process, and that reference is only done to generate a hash value of the contents of the file.

The Update Image output does not contain the (sysload.bmp) file. The sysload.bmp file is included only in the Production Image.

The issue occurs when ExpressVote HW1.0 units were originally updated using the full Production Image method but then later updated using the Update Image method; this may result in the incorrect copyright bitmap file (sysload.bmp) being resident on the internal eUSB. When the hash check validation process is performed on a unit that contains the incorrect bitmap file on the eUSB, the

sysload.bmp file is reported as an exception.

The table below shows the different versions of the (sysload.bmp) file that have been incorporated into the various versions of ExpressVote HW1.0 application firmware.

Table 1 – Sysload.bmp files

Firmware	Copyright YRS	Project(s)	OS Version	IOB	SPE	Sysload.bmp file Hash Value
1.4.0.0	2011 - 2014	5.2.0.0, 5.2.0.3	6.00.14	1.1.0.0	1.1.0.0	e173f1a084bb5fac2e19962aeb4f6ecd529e30cc9b0a64411cda80e4b4089686
1.4.1.0	2011 - 2015	5.2.1.0	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.1.2	2011 - 2016	5.2.2.0, 5.3.2.0	6.00.19	1.1.0.0	1.4.1.0	b3a230dc5ff31311a9f83b5bfee22ac96291c57f0c84abd05852aabf605ebbe3
1.4.1.7	2011 - 2018	5.2.4.0, 5.2.4.1, 5.3.4.0, 5.3.4.1	6.00.19	1.1.0.0	1.4.1.6	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.4.2.0	2011 - 2015	FL 4.5.2.0 V1 R2	6.00.19	1.1.0.0	1.4.1.0	de99ddc620c6260e5e4dd4d26486b82f8a5c2297fc5169b31607b61563f974de
1.4.3.0	2011 - 2017	FL 4.5.3.0 V1 R2	6.00.19	1.1.0.0	1.4.3.0	ff4c1b668dbda1e7b23ba41547c62b53385afc836fd60717bc04739d9383b2aa
1.4.3.1	2011 - 2018	FL 4.5.3.0 V2 R3	6.00.19	1.1.0.0	1.4.3.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.0.0	2011 - 2018	6.0.0.0, 6.0.2.0, 6.0.3.0	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.0	2011 - 2018	6.0.4.0, 6.0.4.3	6.00.19	1.5.0.0	2.4.0.0	07015a3e4d71e8683d3bf21b3d427f007a89b35d236767aedd35c4d94c3d8a12
1.5.2.1	2011 - 2019	6.0.4.0 AZ	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e
1.5.3.0	2011 - 2019	6.0.5.0	6.00.19	1.5.0.0	2.4.0.0	e39d71e88398beb836ee95973be1daec2bdbe091619891d8026fbfa15ae1798e

As an example, a new ExpressVote HW 1.0 device is being deployed, and it is being installed with the application firmware v1.5.2.0 for voting system EVS 6.0.4.3, which was certified in the year 2018. The sysload.bmp file shows a copyright period of 2011-2018.

A year goes by and now that same device needs to be updated to the newer version, EVS 6.0.5.0, which was certified in the year 2019. The sysload.bmp file has a copyright period of 2011-2019. The Update Image (which does not contain the sysload.bmp file) is used to update the device.

When the hash verification is executed, the package used has the hash code for the file with the 2019 copyright, but the sysload.bmp file examined on the ExpressVote HW1.0 device has the 2018 copyright, since it did not get updated by the Update Image installation. As a result, its hash code does not match the 2019 copyright sysload.bmp file's hash code.

2.4 Additional Examination

ES&S has provided a list of other known dynamic files and folders which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units. Note that a Dynamic File, by definition, is a file that is modified often during system operation. As a result, it is to be expected that a hash code will most often not match a previously taken hash code of that same file.

The following table details the "Dynamic File Reference", provides "Firmware Version of Origin" and a "Description" of the file's function.

Table 2 – Dynamic Files

Dynamic File Reference	Firmware Version of Origin	Description
Dynamic Files Filtered Out by the Application Firmware when Creating the USB Export Media		
\ESS\Cache*	1.4.0.0	This folder contains protected key data from the currently EQC'd election and the machine specific private / public keypair. It is deleted and recreated during the EQC process.
\ESS\HashFileOut.lst	1.4.0.0	Text file of file list and hashes generated by the on-unit hashing utility.
\regback	1.4.0.0	This file is created when the application firmware calls the Windows CE RegFlushKey function. This function is OEM (Eurotech) specific and this file contains the modifications made from the Win CE baseline registry contained in nk.bin, the Win CE runtime image. The registry commit most generally occurs upon setting the date / time / time zone and calibrating the touch screen in all releases. As of EV 1.4.1.0, it also occurs on the first boot of our application and coincides with the creation of firstBoot.txt.
\sys.elf \sysstring.elf	1.4.0.0	ExpressVote HW 1.0 system log files.
Dynamic Files that are Created During Typical Use of the ExpressVote HW1.0 when Creating the USB Export Media		
\ESS\firstBoot.txt	1.4.1.0	The Win CE registry needs to be flushed after burning the full eUSB prior to executing our application. This flag file is created by STARTUP.EXE when it performs the flush and reboots the OS. This file is created upon the first execution of the application firmware after updating from either the eUSB prod_release image or USB update image.
\ESS\Simg.bmp	1.4.0.0	This is the bitmap file of the scan image created and displayed when the user executes the Pattern Print and Scan test.
\ESS\lastImage.raw	1.4.1.0	This is a file of the raw image data pulled from the Scanner Printer Engine (SPE) board created by the SPE library. It is most generally created on a successful transfer of the image data of a card on insertion but will also be created in a few other instances of retrieving scan image data.

The following table details the expected outcome of hashing a given release.

Table 3 – Dynamic Files expected in release

EVS Release Name	EV1 Firmware Version	Dynamic Files Not Filtered From Hash Validation
EVS 4.5.2.0 V1 R2	1.4.2.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 4.5.3.0 V1 R2	1.4.3.0	None
EVS 4.5.3.0 V2 R3	1.4.3.1	None
EVS 5.2.0.0	1.4.0.0	SImg.bmp
EVS 5.2.0.3	1.4.0.0	SImg.bmp
EVS 5.2.1.0	1.4.1.0	firstBoot.txt lastImage.raw SImg.bmp
EVS 5.2.2.0	1.4.1.2	lastImage.raw
EVS 5.2.4.0	1.4.1.7	None
EVS 5.2.4.1	1.4.1.7	None
EVS 5.3.2.0	1.4.1.2	lastImage.raw
EVS 5.3.4.0	1.4.1.7	None
EVS 5.3.4.1	1.4.1.7	None
EVS 6.0.0.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.2.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.3.0	1.5.0.0	lastImage.raw SImg.bmp
EVS 6.0.4.0	1.5.2.0	lastImage.raw SImg.bmp
EVS 6.0.4.0 AZ	1.5.2.1	lastImage.raw SImg.bmp
EVS 6.0.4.3	1.5.2.0	None
EVS 6.0.5.0	1.5.3.0	None

3 Examination Performed

This section details the examination methodology as well as the examination performed.

3.1 Examination Methodology

SLI implemented the following methodology in the examination of the Update Image file:

File review:

Step 1.) Generate a SHA-256 hash of the Update Image file.

Step 2.) Compare the generated SHA-256 hash to the SHA-256 hash from the Trusted Build of the system.

Step 3.) Compare the Update Image file to the Production Image file from the Trusted Build to ensure that the Update Image file contains the same files from the Trusted Build (Production Image).

Step 4.) Identify any files that differ between the Update Image and the Production Image.

Step 5.) Compare any differing files against the Trusted Build of the system where these artifacts were originally created. Verify that the files match.

Step 6.) If the files compared in Step 5 differ from those in the trusted build, generate an SHA-256 hash of the files and record the filenames and hash values. Determine the scope and potential impact of the differing files.

Functional Examination:

Step 7.) Update a production ExpressVote HW1.0 device using the USB update image starting at version 1.4.0.0 and generate a verification pack from version to version.

Step 8.) Follow the procedures detailed in the ***Verification Procedure: ExpressVote Hardware 1.0*** document to verify the hash values of all software on the device, noting any verification mismatches. Determine the scope and potential impact of the differing files.

Step 9.) Verify any Dynamic files, as listed in Table 3, which may result in an error message when a hash verification is completed on the ExpressVote HW1.0 units.

3.2 Examination Performed

3.2.1 File Review

The file review portion of the Examination consisted of hashing both the Update Image and Production Image files, then comparing them to the releases trusted build hash codes. Then the files from the Update Image were compared to the files within the Production Image to verify consistency.

3.2.2 Functional Examination

The functional portion of the Examination consisted of five environments that processed a combination of the various EVS releases. Each environment is detailed below.

Updating an ExpressVote with both a Production Image and Update Image represents a full installation. The internal memory (eUSB) is removed from the device and updated to the Production Image (installing the operating system, ExpressVote application firmware and the sysload.bmp file), re-installed into the device, and then updated with the Update Image (Installing the ExpressVote application firmware, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board, but not a new sysload.bmp file).

Each ExpressVote HW1.0 device was configured as it would be for normal field use.

The steps below detail the type of installation performed, the version of the release being installed, the sysload.bmp file associated to the new release, and the result obtained from the hash verification procedure for the sysload.bmp file.

The reader can note that when the device was “Baselined with a Production Image and Update Image”, that the copyright range (in yellow highlight) in the sysload.bmp file is what is on the device, and will be compared to the copyright range in the sysload.bmp file associated with the next version being installed by an “Update Image only” installation.

For example, with Device 1 below,

- First bullet was a Baseline with a 2014 copyright
- Second bullet was a Baseline with a 2015 copyright (no comparison occurred here because it was a baseline)
- Third bullet was an upgrade with a 2017 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.
- Fourth bullet was an upgrade with a 2018 copyright and it was compared to the last Baseline which had the 2015 copyright, with the result that the copyright mismatch was seen.

Device 1 - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.0.0 EVS 5.2.0.0 (non-FL)** (2011-2014 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Baseline with Production Image and Update Image to application firmware **1.4.2.0 for FL EVS 4.5.2.0 V1R2 (first FL release in test)** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.2.0 to 1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 1a - Dedicated to FL release line

- Baseline with a Production Image and Update Image to application firmware **1.4.3.0 for FL EVS 4.5.3.0 V1R2** (2011-2017 copyright) via Update Image only
  - Export Verification Files
- Upgrade from **1.4.3.0 to 1.4.3.1 FL EVS 4.5.3.0 V2R3** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

Device 2

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
  - Serial Number Set
  - Timezone and Date and Time Set
  - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.2.4.0 to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
  - Export Verification Files (**copyright mismatch seen**)

- Upgrade from **1.4.1.7 EVS 5.2.4.1 to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.7 EVS 5.3.4.0 to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**))
- Upgrade from **1.4.1.7 EVS 5.3.4.1 to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.0 to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.2.0 EVS 6.0.4.3 to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

Device 3

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade from **1.4.1.0 to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.2.2.0 to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.4.1.2 for EVS 5.3.2.0 to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.0.0 to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.2.0 to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade from **1.5.0.0 for EVS 6.0.3.0 to 1.5.2.1 for EVS 6.0.4.0 AZ** (2011-2019 copyright) via Update Image only
    - Export Verification File (**copyright mismatch seen**)

DEVICE 4

- Baseline with Production Image and Update Image to application firmware **1.4.1.0 for EVS 5.2.1.0** (2011-2015 copyright) via Production and Update Image
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.2 for EVS 5.3.2.0** (2011-2016 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.2.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.4.1.7 for EVS 5.3.4.1** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.2.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.0.0 for EVS 6.0.3.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.3** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.2.1 for EVS 6.0.4.0AZ** (2011-2019 copyright) via Update Image only

    - Export Verification Files (**copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

DEVICE 5

- Baseline with Production Image and Update Image to application firmware **1.4.1.0** for **EVS 5.2.1.0** (2011-2015 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.2 for EVS 5.2.2.0** (2011-2016 copyright) via Update Image Only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.2** for **EVS 5.2.2.0** (2011-2016 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.4.1.7 for EVS 5.2.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)
- Baseline with Production Image and Update Image media to application firmware **1.4.1.7** for **EVS 5.2.4.0** (2011-2018 copyright)
    - Serial Number Set
    - Timezone and Date and Time Set
    - Export Verification Files
- Upgrade **to 1.5.0.0 for EVS 6.0.0.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (2011-2018 copyright) (**No copyright mismatch seen**)
- Upgrade **to 1.5.2.0 for EVS 6.0.4.0** (2011-2018 copyright) via Update Image only
    - Export Verification Files (**No copyright mismatch seen**)
- Upgrade **to 1.5.3.0 for EVS 6.0.5.0** (2011-2019 copyright) via Update Image only
    - Export Verification Files (**copyright mismatch seen**)

4 Firmware Update Examination Results

4.1 Files Examined

SLI reviewed the Update Image against the Production Image for each of the releases, finding that all common files matched each other and their associated hash codes, as expected. The differentiating files, the Scanner Printer Engine (SPE) board and the Input Output (IOB) board files for the Update Image, and the full WinCE operating system and the "sysload.bmp" bitmap file for the Production Image matched the expected hash codes.

The verified SHA-256 hash of the Production Image file is:

- a520e7779b21060e5a25798f8d9d3a1ef5bd21d68d29922f9f45ea782f0e66c9

The verified SHA-256 hash of the Update Image file is:

- 29749c16ea77bf21e5c47d2a98f02a87d52e7083d0efffc4818a4f98b1591187

Files found on the Update Image but not on the Production Image, as well as file found on the Production Image but not on the Update Image are listed in Table 4 – File Differences between Images below.

Table 4 – File Differences between Images

Software Version	Firmware Version	Files found on the Production Image but not the Update Image	Files found on the Update Image but not the Production Image
4.5.3.0v2r3 FL	1.4.3.1	BOOT.INI	InputOutputBoard.S19
		BLDR	ScannerPrinterEngine.S19
		nk.bin	
		smsc9500.dll	
		sysload.bmp	
		SYSLOAD.REG	
		wdapi1130.dll	
		windrvr6.dll	

Each of these files were found to match files in the Trusted Build.

4.2 Functional Examination Summary

4.2.1 Sysload.bmp file

The functional examination showed that two potential hashing results can occur when updating an ExpressVote HW1.0 device from one release to another using the Update Image, in the context of the sysload.bmp file.

One outcome is that if the version of sysload.bmp file originally on the device has the same copyright period as the sysload.bmp file that is part of the newly installed

release, the verification process will log it as a match and not note anything in the "difference" report. This is expected as the two files are identical.

The other outcome is that if the version of sysload.bmp file originally on the device has a different copyright period from the sysload.bmp file that is part of the newly installed release, the verification process will log it as a difference and will note the two files and their corresponding hash codes in the "difference" report. This is expected as the two files are different.

If this second outcome occurs, the jurisdiction must reference "Table 1 – Sysload.bmp files" above and verify that the sysload.bmp file's hash codes noted in the "difference" report match the corresponding hash codes listed in Table 1. If the hashes match, installation may continue. If the hashes don't match, the jurisdiction must follow ES&S recommendations and perform a Production Image installation on the device.

4.2.2 Dynamic files

No files were listed in "Table 3 – Dynamic Files expected in release" for this release, and none were seen.

End of Test Report

U. S. ELECTION ASSISTANCE COMMISSION
VOTING SYSTEM TESTING AND CERTIFICATION PROGRAM
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

October 14, 2020 **Sent via e-mail**

Sue McKay, Vice President of Federal Certification
Election Systems & Software
11208 John Galt Blvd.
Omaha, NE 69137

Re: ECO 1100

Dear Ms. McKay,

This correspondence is to inform you that ES&S ECO 1100 is approved.

Sincerely,

Jerome Lovato
Director, Voting System Testing and Certification

Cc: Pro V&V
SLI Compliance