# ES&S EVS 6.0.4.2
# Security and Telecommunications Test Report

*ESS-18S52059-S/TTR-01*

| | |
|---|---|
| **Vendor Name** | *Election Systems & Software (ES&S)* |
| **Vendor System** | *EVS 6.0.4.2* |

Prepared by:


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

Accredited by the Election Assistance Commission (EAC) for VSTL status.

# Revision History

| Date | Release | Author | Revision Summary |
|---|---|---|---|
| 8/14/2019 | 1.0 | J. Peterson, J. Panek | Initial Release |
| 8/16/2019 | 1.1 | D. George | Updated based on comments |
| 8/19/2019 | 1.2 | D. George | Additional edits |
| 8/20/2019 | 1.3 | D. George | Additional edits |
| 8/21/2019 | 1.4 | D. George | Final edits |

## 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; 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

# Overview

This test report provides results for the security and telecommunications testing of the **ES&S EVS 6.0.4.2 Voting System**.

Security and telecommunications testing covered:

- Top-level system design and architecture
- System documentation and procedures
- Testing of relevant software and operating system configuration for pertinent vulnerabilities
- Testing of hardware, including examination of unused hardware ports and security measures applied to those ports
- Testing of system communications, including encryption of data as well as protocols and procedures for access authorization

Testing was implemented without any prior knowledge of the source code.

The testing was divided into three phases:

- Phase I included the following areas of focus:
  - Review of all pertinent documents for appropriate processes and procedures for implementing a secure system
  - Review of the system design and architecture
- Phase II included the following areas of focus:
  - Testing of relevant software, operating systems and hardware configurations
- Phase III included the following areas of focus:
  - Testing of all telecommunications aspects of the system

# Phase I – Documentation Review

During Phase I testing, documentation was reviewed to verify and validate:

- Top-level system design and architecture
- System documentation and procedures

The documentation was also reviewed against the following California Voting System Standards (CVSS) requirements:

- 7.2.2 Access Control Identification
- 7.3.1 Polling Place Security
- 7.3.2 Central Count Location Security
- 7.4.1 Software and Firmware Installation
- 7.4.2 Protection Against Malicious Software
- 7.4.3 Software distribution and setup validation
- 7.4.4 Software Distribution
- 7.4.5 Software Reference Information
- 7.4.6 Software Setup Validation
- 7.8.1 Access Control
- 7.8.2 Data Interception and Disruption
- 9.6 System Security Specification

Please see the applicable section below for more details on these requirements and the review results.

During Phase I testing, an issue log of any errors and omissions found in the documentation or anomalies encountered was maintained.

## 7.2.2 Access Control Identification

a. The voting system **shall** identify users and processes to which access is granted and the specific functions and data to which each entity holds authorized access.

b. Voting system equipment that implements role-based access control **shall** support the recommendations for Core RBAC in the ANSI INCITS 359-2004 American National Standard for Information Technology Role Based Access Control document.

c. Voting system equipment **shall** allow the administrator group or role to configure the permissions and functionality for each identity, group, or role to include account and group/role creation, modification, and deletion.

**Results**: Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily covered.

## 7.3.1 Polling Place Security

For polling place operations, manufacturers **shall** develop and provide detailed documentation of measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences.

The measures **shall** allow the immediate detection of tampering with vote casting devices and precinct ballot counters.

**Results**: Review of the TDP validated that the requirement was satisfactorily covered.

## 7.3.2 Central Count Location Security

Manufacturers **shall** develop and document in detail the measures to be taken in a central counting environment. These measures **shall** include physical and procedural controls related to the handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.

**Results**: Review of the TDP validated that the requirement was satisfactorily covered.

## 7.4.1 Software and Firmware Installation

The system **shall** meet the following requirements for installation of software, including hardware with embedded firmware.

a. Air Gap Architecture

   i. Every voting system **shall** be capable of being deployed in a segregated dual-installation architecture to protect against propagation of viruses. The architecture **shall** allow elections officials to use one or more, permanent server(s) and set of central-office voting devices, known to be running unaltered, certified software and firmware to create memory cards before each election and to use another, physically separate “sacrificial” server and set of voting devices after the election to tabulate results and generate reports. The architecture **shall** allow transfer of the election definition and tally database from the permanent server(s) to the sacrificial server using a write-once medium, such as a CD-R. The voting system architecture **shall** allow each installation to use its own Ethernet network, port server, and central-office vote-recording units, including any DRE and optical scan units, permitting the two installations to be segregated and air-gapped to ensure that there are

no cross connections. An air gap is established by keeping two installations/networks physically separate and seeing that no device attached to the sacrificial installation/network is connected (directly or indirectly) to the first network, ensuring that data cannot flow from one installation/network to the other.

ii. The TDP for the voting system **shall** provide full procedures and instructions, to be incorporated into the Official Use Procedures for the voting system, to implement the segregated dual-installation architecture.

b. Voting and Tabulating Unit

i. If software is resident in the system as firmware, the manufacturer **shall** require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations.

ii. To prevent alteration of executable code, no software **shall** be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.

iii. The voting system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote counting program, and its associated exception handlers.

iv. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.

v. After initiation of Election Day testing, no source code or compilers or assemblers **shall** be resident or accessible.

**Results**: Review of the TDP validated that the requirement was satisfactorily covered.

## 7.4.2 Protection against Malicious Software

Voting systems **shall** deploy commercial-off-the-shelf (COTS) protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs.

Manufacturers **shall** develop and document the procedures to be followed to ensure that such protection is maintained in a current status. Virus and malware

protection software and updates **shall** be installed using transportable portable media only and **shall not** be installed by download from the Internet.

**Results**: Review of the TDP validated that the requirement was satisfactorily covered.

## 7.4.3 Software Distribution and Setup Validation

Subsections 7.4.4, 7.4.5 and 7.4.6 specify requirements for the distribution of voting system software and the setup validation performed on voting system equipment. These requirements are applicable to voting systems that have completed certification testing.

## 7.4.4 Software Distribution

The manufacturer **shall** document all software including voting system software, third party software (such as operating systems and drivers) to be installed on the certified voting system, and installation programs.

a. The documentation **shall** have a unique identifier (such as a serial number or part number) for the following set of information: documentation, software manufacturer name, product name, version, the certification application number of the voting system, file names and paths or other location information (such as storage addresses) of the software.

b. The documentation **shall** designate all software files as static, semi-static or dynamic.

**Results**: Review of the TDP validated that the requirement was satisfactorily covered.

## Pertinent Excerpt(s) from: 7.4.5 Software Reference Information

a. The manufacturer **shall** provide the NSRL, any California certified escrow facility, pursuant to Title 2, Division 7, Chapter 6 of the California Code of Regulation, and the Office of the Secretary of State with a copy of the software installation disk, including the executable binary images of all third party software. Further, the manufacturer **shall** deposit the source code, tools, and documentation, to allow the complete and successful compilation of a system in its production/operation environment.

   i. The manufacturer **shall** document that the process used to verify the software distributed on unalterable storage media is the certified software by using the reference information provided by the NSRL or other designated repository before installing the software.

c. The manufacturers **shall** document to whom they provide voting system software.

**Results**: Review of the TDP validated that the requirement was satisfactorily covered.

## Pertinent Excerpt(s) from: 7.4.6 Software Setup Validation

g. Setup validation methods **shall** verify the contents of all system storage locations (e.g., system registers, variables, files, etc.) containing election specific information (e.g., ballot style, candidate registers, measure registers, etc.).

   i. The manufacturer **shall** document the default values of all system storage locations that hold election specific information.

**Results**: Review of the TDP validated that the requirement was satisfactorily covered.

## 7.8.1 Access Control

The accredited testing laboratory **shall** conduct tests of system capabilities and **review** the access control policies and procedures submitted by the manufacturer to identify and verify the access control features implemented as a function of the system.

Specific activities to be conducted by the S-ATA **shall** include:

a. A review of the manufacturer's access control policies, procedures and system capabilities to confirm that all requirements have been addressed completely.

**Results**: Review of the TDP validated that the requirement was satisfactorily covered.

## 7.8.2 Data Interception and Disruption

For systems that use telecommunications, as provided for in section 6 of the Standards and consistent with California law, to transmit official voting data, the S-ATA **shall** review, and conduct tests of, the data interception and prevention safeguards specified by the manufacturer in its TDP. The S-ATA **shall** evaluate safeguards provided by the manufacturer to ensure their proper operation, including the proper response to the detection of efforts to monitor data or otherwise compromise the system.

**Results**: Review of the TDP validated that the requirement was satisfactorily covered.

### 9.6 System Security Specification

Manufacturers shall Document in the TDP all aspects of the system design, development and proper usage that are relevant to system security. This includes but is not limited to the following:

- System security specification that Addresses the security requirements.
- The means used to keep the security capabilities of the system current to respond to evolving threats.
- Specific security risks addressed by the system.
- All hardware and software security mechanisms.
- Development procedures employed to ensure absence of malicious code.
- Initialization, usage, and maintenance procedures necessary to secure operation.
- All attacks the system is designed to resist or detect.
- Any security vulnerabilities known to the manufacturer.

**Results**: Review of the TDP validated that the requirement was satisfactorily covered.

## Phase II – Functional Security Testing

During Phase II testing of the **ES&S EVS 6.0.4.2** system, functional tests were exercised in order to:

- Test relevant software and operating system configurations for pertinent vulnerabilities
- Test hardware, including examination of unused hardware ports and security measures applied to those ports

The functional security testing of the ES&S EVS 6.0.4.2 system was evaluated against the following CVSS requirements:

- 5.4.3 In-process Audit Records
- 7.2.1 General Access Control
- 7.2.2 Access Control Identification
- 7.2.3 Access Control Authentication
- 7.2.4 Access Control Authorization
- 7.3 Physical Security Measures

- 7.3.1 Polling Place Security
- 7.3.2 Central Count Location Security
- 7.4.1 Software and Firmware Installation
- 7.4.2 Protection Against Malicious Software
- 7.4.3 Software distribution and setup validation
- 7.4.5 Software Reference Information
- 7.4.6 Software Setup Validation
- 7.6 Telecommunications and Data Transmission
- 7.6.1 Maintaining Data Integrity
- 7.6.2 Election Returns
- 7.8.1 Access Control
- 7.8.2 Data Interception and Disruption

Please see the applicable section below for more details on these requirements and the review results.

## Pertinent Excerpt(s) from: 5.4.3 In-process Audit Records

iv. Notification of system login or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing.

**Testing Performed**: During the examination, the auditing capabilities were reviewed to determine the systems auditing capabilities. The examination included:

- Attempts to modify or corrupt audit logs / records.
- Attempts to disable or turn off audit logging capabilities.
- Attempts to Falsify audit logs located on removable election media.

**Applicable to**: Electionware, ExpressVote, ExpressVote XL, DS200, DS450, DS850.

**Results**:

- It was determined that with the exception of the ExpressVote XL, much of the ES&S EVS 6.0.4.2 system does not provide electronic monitoring or logging of physical security violations. While the EVS 6.0.4.2 system doesn't have electronic monitoring of all physical security violations the system compensates with physical tamper evident security seals and lock / key combinations. The ExpressVote XL indicates that the election media compartment panel is open. This is indicated using both audio and visual means, as well as on screen prompts to notify an election official.

- All attempts to circumvent modify, or disable in-process audit logs or capabilities were unsuccessful.
- Based on the results from attempting to circumvent the audit logs, the requirement for in-process audit records was sufficiently covered.

## 7.2.1 General Access Control

a. Voting system equipment **shall** provide access control mechanisms designed to permit authorized access to the voting system and to prevent unauthorized access to the voting system.

   i. Access control mechanisms on the Election Management System (EMS) shall be capable of identifying and authenticating individuals permitted to perform operations on the EMS.

b. Voting system equipment shall provide controls that permit or deny access to the device's software and files.

c. The default access control permissions shall implement the minimum permissions needed for each role or group identified by a device.

d. The voting device shall prevent a lower-privileged process from modifying a higher-privileged process.

e. An administrator of voting system equipment shall authorize privileged operations.

f. Voting system equipment shall prevent modification to or tampering with software or firmware through any means other than the documented procedure for software upgrades.

**Testing performed**:

- System wide authentication checks, including both positive and negative testing to verify that the systems under examination allowed authorized users the ability to complete tasks while preventing all unauthorized users from accessing critical controls or processes.
- Attempts to access systems files or software via an unauthorized method or process.
- System wide permission checks to determine if user accounts and passcodes only allowed the appropriate levels of permission / roles to perform the task at hand.
- Examined Solution specific users and roles to confirm permissions and task / actions.
- Attempts to escalate privileges from a lower privileged account in an attempt to perform or access roles or tasks not specifically assigned to users.

- Examined the system to determine if the software or firmware could be tampered with or modified through other means besides the documented procedure.
- Enumerated each system as able, pulling audit logs, firewall rules, running processes, network configurations, user lists, and security settings.

**Applicable to**: Electionware, ExpressVote, ExpressVote XL, DS200, DS450, DS850.

Results:

- During the examination of the Electionware Client and Standalone configurations, it was determined that many of the programs on the start menu were disabled from direct launching from the start menu. The user, either restricted or administrative, was able to successfully run a command prompt and execute the programs that were disabled on the start menu. Restricted users were still restricted from running elevated commands or programs. The restricted user account for the Windows Electionware systems is able to succesfully enumerate the system, basic common privilege escalation attempts were unsuccessful.
- During testing it was determined that it is possible to modify or tamper with the software installed on the Electionware systems. Access control mechanisms were in place to prevent unauthorized access to the system.
- During testing all the OKI printers were configured with default DHCP enabled active ethernet ports. This also included the default username and passwords for the printer in both local and network configuration. No active mitigation was observed for this issue.
- Review of the results from testing the system validated that the requirement was partially covered. The ability for an unauthorized user to modify Electionware software is prevented by operating system roles and access control methods.

  The following items were not sufficiently mitigated:

  - The restricted user is still able to access the CMD prompt and enumerate the system.
  - The OKI printers were still configured with active DHCP enable ethernet ports, and the printer was configured with default user credentials.

## Pertinent Excerpt(s) from: 7.2.2 Access Control Identification

a. The voting system **shall** identify users and processes to which access is granted and the specific functions and data to which each entity holds authorized access.

b. Voting system equipment that implements role-based access control **shall** support the recommendations for Core RBAC in the ANSI INCITS 359-2004 American National Standard for Information Technology Role Based Access Control document.

c. Voting system equipment **shall** allow the administrator group or role to configure the permissions and functionality for each identity, group, or role to include account and group/role creation, modification, and deletion.

**Testing performed**:

- Confirmation that the documented users and roles are included in the TDP.
- Confirmation of all Electionware roles and responsibilities.
- Confirmation of Administrative groups roles and permissions.

**Applicable to**: Electionware, ExpressVote, ExpressVote XL, DS200, DS450, DS850.

- **Results**: Review of the results from testing the system validated that the requirement was covered.

## 7.2.3 Access Control Authentication

The following authentication requirements apply to all voting system equipment.

a. Voting system equipment **shall** authenticate users prior to granting them access to system functions or data.

b. When private or secret authentication data is stored in voting system equipment, the data **shall** be protected to ensure that the confidentiality and integrity of the data is not violated.

c. Voting system equipment **shall** allow the administrator group or role to set and change passwords, pass phrases, and keys.

d. Voting system equipment **shall** allow privileged groups or roles to be disabled and allow new individual privileged groups or roles to be created.

e. Voting system equipment **shall** lock out groups, roles, or individuals after a specified number of consecutive failed authentication attempts within a predefined time period.

f. Voting systems **shall** allow the administrator group or role to configure the account lock out policy, including the time period within which failed attempts must occur, the number of consecutive failed access attempts allowed before lock out, and the length of time the account is locked out.

g. If the voting system uses a user name and password authentication method, the voting system **shall** allow the administrator to enforce password strength, histories, and expiration.

h. The voting system **shall** allow the administrator group or role to specify password strength for all accounts, including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters.

i. The voting system **shall** enforce password histories and allow the administrator to configure the history length.

j. Voting system equipment **shall** ensure that the username is not used in the password.

k. Voting systems **shall** provide a means to automatically expire passwords in accordance with the voting jurisdiction's policies.

**Testing performed**:

- Attempts to access system functions and resources without successful authentication to the operating system or **ES&S EVS 6.0.4.2** system.
- Attempts to find and extra authentication data from system storage, including compact flash cards, hard drives, USB sticks, and CFast storage.
- Verification that the system equipment allows the administrator to change all passwords, pass phrases, and keys, if applicable.
- Verification that the system(s) have the ability to lockout accounts after a specified number of failed authentication attempts.
- Confirmation and testing of the system's password complexity, strength, lockout, history, length, and expiration requirements.

**Applicable to**: Electionware, ExpressVote, ExpressVote XL, DS200, DS450, DS850.

**Results**:

- A shadowed password file recovered from the ExpressVote XL has two users: ess and root, of which both of the password hashes were cracked. All attempts to utilize the credentials to login to the device were unsuccessful. The ability to access the ExpressVote XL internal storage media is prevented by physical security measures including: security torx screws, wire security seals, and a locked compartment door.

- A boot-loader password file was successfully extracted from a DS450 tabulation device. The boot-loader password hash was sufficiently complex that attempts to crack the password hash were unsuccessful after two days of attempting to brute force the value. The passwords were of sufficient complexity to resist brute force password cracking attempts.
- An exploration of the Electionware systems indicated that there were password hashes stored in the Secure File Transfer Protocol (SFTP) server XML configuration files. Attempts to brute force these password hashes were unsuccessful. The Electionware systems are access controlled systems that prevent unauthorized users from logging into the operating system.
- Review of the results from testing the system validated that the requirement was partially covered. While the finding above were mitigated either by physical or electronic access control mechanisms, the ability to gain access to the internal storage and pull password hashes is a vulnerability, and given enough time the hashes may be brute forced.

### 7.2.4 Access Control Authorization

a. Voting systems **shall** ensure that only authorized roles, groups, or individuals have access to election data.

b. Voting systems **shall** explicitly authorize subject's access based on access control lists or policies.

c. Voting systems **shall** explicitly deny subject's access based on access control lists or policies.

During the examination, the access control authorization capabilities of all the systems were reviewed to determine if the systems provided sufficient controls for authorization.

**Testing performed**:

- Verification that the system only allows authorized roles, groups, and individuals access to election data.
- Verification that the system has access levels based upon roles, control lists, or policies.
- Verification that the system successfully denies access to the system based upon roles, lists, or policies.

**Applicable to**: Electionware, ExpressVote, ExpressVote XL, DS200, DS450, DS850.

**Results**:

- During testing, it was determined that the Electionware systems restrict access to programs or features of the operating system based on software restriction policies; however, there was the potential to circumvent some or all of the policies by launching operating system level components via a command prompt.
    - The built-in windows shortcut key commands were not restricted and allowed the user to utilize the run functionality. This allows the user to bring up a command prompt or run commands directly through the run interface. In the case of the restricted user, this only allowed them to bypass the start menu restrictions for application launching. All basic attempts to escalate privileges on the restricted user for operating system accounts were unsuccessful. The built-in Electionware access control role restrictions were also examined and all attempts to elevate from a restricted access role to a non-restricted one were unsuccessful.
    - In the client/server configuration for the Electionware product, the authentication successfully prevents the restricted user account from accessing sensitive OS functionality. It is also noted that non-administrative users are unable to login to the Electionware server that serves as the SFTP server for results transmission from the central count scanners, and as the Electionware Results database.
    - The standalone configuration combines the roles of the client / server Electionware component and removes the networking capability of the system. Similar to the client / server configuration, all user roles are able to utilize windows shortcut keys to circumvent the start menu application launch restrictions. As an administrative user, this is a low risk observation as the privileged user of the system has administrative privileges and would be able to totally remove/circumvent the in-place hardening.
- All the systems successfully protected the system BIOS settings from tampering which prevented all attempts to boot from unauthorized devices, as well as changing system configuration settings at a BIOS level.
- Per the requirement the requirement the review of the results from testing the system validated that the requirement was partially covered. The restricted user can perform actions that were intended to be restricted including but not limited to:
    - The ability for restricted user to utilize windows shortcut keys to circumvent start menu restrictions was not mitigated.
    - The ability to launch a command prompt and access restricted programs and system files.

## 7.3 Physical Security Measures

a. Any unauthorized physical access **shall** leave physical evidence that an unauthorized event has taken place.

b. Voting systems **shall** only have physical ports and access points that are essential to voting operations and to voting system testing and auditing.

c. An event log entry that identifies the name of the affected device **shall** be generated if a component connected to a piece of voting system equipment is disconnected while polls are open.

d. Ports disabled while polls are open **shall** only be re-enabled by authorized administrators.

e. Access points, such as covers and panels, **shall** be secured by locks or tamper evident seals or tamper resistant countermeasures **shall** be implemented so that system owners can monitor access to voting system components through these points.

f. Ballot boxes **shall** be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.

During the examination of the physical security measures, all the systems were physically secured as they normally would be during a live election.

**Testing performed**:

- Attempts to circumvent all physical security features, including picking of locks, attempts to circumvent or bypass security seals, and security screws
- Examination and testing of all ports and connectors.
- Disconnection of devices and examination of audit logs, as applicable, to determine if auditing of device disconnection was present.
- Identification and examination of every cover, panel, and access compartment.
- Attempts to circumvent all ballot boxes to add, remove, or destroy paper ballots.

**Applicable to**: Electionware, ExpressVote, ExpressVote XL, DS200, DS450, DS850.

**Results**:

- **ES&S EVS 6.0.4.2** equipment has the same key for every type of device. It is a vulnerability to not rekey all voting systems and devices.
- All ports on the system devices are active; however, physical security measures encountered by SLI during testing prevented casual access to all

ports. The physical mitigation measures included: Security Screws, tamper evident seals, and locking compartment doors.

- OKI printers, the network interface ports are active and not protected, allowing for the ability for the printers to be connected to a network.
- Review of the results from testing the system validated that the requirement was partially covered.

## 7.3.1 Polling Place Security

For polling place operations, manufacturers **shall** develop and provide detailed documentation of measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences.

The measures **shall** allow the immediate detection of tampering with vote casting devices and precinct ballot counters.

**Testing performed**: Tests were performed to verify that the documented measures provide adequate polling place security.

**Applicable to**: ExpressVote, ExpressVote XL, DS200.

**Results**: Review of the results from testing the system validated that the requirement was satisfactorily covered.

## 7.3.2 Central Count Location Security

Manufacturers **shall** develop and document in detail the measures to be taken in a central counting environment. These measures **shall** include physical and procedural controls related to the handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.

**Testing performed**: Tests were performed to verify that the documented measures provide adequate central count location security.

**Applicable to**: Electionware, DS450, DS850.

**Results**: Review of the results from testing the system validated that the requirement was satisfactorily covered.

## Pertinent Excerpt(s) from: 7.4.1 Software and Firmware Installation

The system **shall** meet the following requirements for installation of software, including hardware with embedded firmware:

b. Voting and Tabulating Units

ii. To prevent alteration of executable code, no software **shall** be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.

iii. The voting system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote counting program, and its associated exception handlers.

iv. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.

v. After initiation of Election Day testing, no source code or compilers or assemblers **shall** be resident or accessible.

**Testing performed:**

- Tests were performed to verify that if any software or firmware is installed, unless the documentation details how to protect it, it is inaccessible to activation or control only by authorized means
- Tests were performed to verify that no source code, compilers, or assemblers are resident or accessible after election day testing

**Applicable to**: Electionware, ExpressVote, ExpressVote XL, DS200, DS450, DS850.

**Results**:

- The trusted build process documentation and process were observed by SLI Compliance and it was determined that the process for software creation and installation satisfactorily covered this requirement. With the caveat that in the case of the ExpressVote XL system, the underlying operating system doesn't contain integrity checking of the CFast cards for firmware installation. The open-ended vulnerability testing revealed that it was possible to remove the OS CFast card from the device and read and manipulate the operating system. It should be noted that the ExpressVote XL system contains physical, electronic, and procedural mitigations to detect and prevent this type of modification.
- The DS450, DS850, and DS200 firmware installation processes include the ability to create read-only flash cards which removes the ability for operating system modification after the certified software has been installed on the devices. Processes and procedures for validations of the system

files are detailed by the vendor. This includes creation and comparison of file hashes to certified trusted hashes of the certified software.

- The ExpressVote firmware installation media is able to be modified during the installation phase of the firmware. The USB firmware update media contains no integrity checking of the firmware specific pieces of the system. It should be noted that the examiners were unable to access the internal operating system storage devices due to two factors. 1) The device would have to be totally disassembled, and 2) the internal storage media requires a proprietary connection type to interface with the storage. For this reason, the examination was unable to determine if the OS drive or its contents were protected. Procedures are documented to verify the validity of the loaded software during pre-election activities and again after the election. These validations are completed by extracting the OS media and testing that the system is unmodified by hashing the operating system files and comparing against a trusted hash list from a trusted source.
- In all cases it should be noted that the election specific files such as results, logs, and definitions are all either encrypted and signed or just digitally signed to protect the integrity of the election specific programming.
- Review of the results from testing the system validated that the requirement was satisfactorily covered.
    - The combination of the physical, procedural, electronic and vendor suggestions sufficiently reduce the risk of these vulnerabilities being exploited in the field.
    - The systems are protected by physical tamper evident seals, locking compartment doors, and security screws.
    - The vendor recommends that the systems be properly verified at specific times during the election process.
    - The vendor has procedural recommendations related to the storage and transportation of the devices.
    - The vendor has procedural recommendations for chain of custody, tamper evident seal management, and key management.

## 7.4.2 Protection against Malicious Software

Voting systems **shall** deploy commercial-off-the-shelf (COTS) protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs.

Manufacturers **shall** develop and document the procedures to be followed to ensure that such protection is maintained in a current status. Virus and malware protection software and updates **shall** be installed using transportable portable media only and **shall not** be installed by download from the Internet.

**Testing performed:** Tests were performed to verify that COTS products are implemented to protect against malicious software, as described in voting system manufacturer documentation.

**Applicable to**: Electionware, ExpressVote, ExpressVote XL, DS200, DS450, DS850.

**Results**:

- The Electionware client and server machines are configured with endpoint protection software that successfully detected and cleaned malicious test files and strings. The software; however, didn't detect and remove archived and double archived malicious content until they were extracted.
- The ability to disable the AV protection as an administrative user without requiring a password to do so is considered a vulnerability. The end-point protection software was disabled during the Open Ended Vulnerability Testing so that the testing team was able to verify that there were no vulnerabilities that were hidden behind the protection of the end-point protection software. It is a common practice to restrict the ability to disable or turn off AV / end-point protection software without requiring a password. No mitigation to this issue were observed.
- Malicious software detection and removal software, such as antivirus or anti-malware, was not observed in operation on the DS450, DS850, DS200, ExpressVote, and ExpressVote XL devices. It was determined that in the cases of the DS450, DS850, and the DS200, the operating system storage partitions were created and mounted on read only media, preventing any type of modification or infection of the supporting operating system.
- The examination determined that all malicious and regular executable applications and scripts that were attempted to be launched from the ExpressVote USB media were unsuccessful.
- This requirement was covered satisfactorily with the caveat that it's possible to disable the Electionware server / client Endpoint protection without a password. The ability to disable the Endpoint protection while a vulnerability still requires the ability to access the system, which is restricted by access controls.

## 7.4.3 Software Distribution and Setup Validation

Subsections 7.4.4, 7.4.5, and 7.4.6 specify requirements for the distribution of voting system software and the setup validation performed on voting system equipment. These requirements are applicable to voting systems that have completed certification testing.

**Testing performed**: This requirement is met by successful validation of 7.4.5, and 7.4.6.

**Applicable to**: Electionware, ExpressVote, ExpressVote XL, DS200, DS450, DS850.

**Results**: Review of the results from testing the system validated that the requirement was satisfactorily covered.

## 7.4.5 Software Reference Information

a. The voting system equipment **shall** be designed to allow the voting system administrator to verify that the software is the certified software by comparing it to reference information produced by the NSRL or other designated repository.

**Testing performed**: Tests were performed to verify that the software can be verified to meet the National Software Reference Library (NSRL) reference information.

**Applicable to**: Electionware, ExpressVote, ExpressVote XL, DS200, DS450, DS850.

**Results**: Review of the results from testing the system validated that the requirement was satisfactorily covered.

## 7.4.6 Software Setup Validation

a. Setup validation methods **shall** verify that only authorized software is present on the voting equipment. Authorized software is COTS software components needed to run the voting system and voting software components identified by the manufacturer as authorized.

b. The manufacturer **shall** provide a method to comprehensively list all software files that are installed on voting systems.

   i. This method **shall** list version names and numbers for all application software on the voting system.

   ii. This method should list of the date of installation for all application software on the voting system.

c. Setup validation methods **shall** include a software verification method that ensures that the voting system software has not been modified illegitimately.

   i. The voting systems **shall** include any supporting software and hardware necessary to conduct the software verification method.

   ii. The manufacturer **shall** document the process used to conduct the software verification method.

iii. The software verification method **shall** not modify the voting system software on the voting system.

d. Voting systems **shall** include a software verification method that either verifies software prior to installation or a method that verifies software using an external interface. Voting systems may include both software verification methods. Voting systems may provide ancillary setup validation methods, including methods for verifying or identifying installed software, other than those described in this section. There are no specific requirements for ancillary setup validation methods. However, any method intended to serve as the voting system software verification method must meet the requirements outlined in this section.

e. Voting systems which implement a software verification method that verifies software prior to installation **shall** meet the following requirements:

   i. The voting system **shall** contain no more than one method for installing, updating, or removing software on a system.

      - Voting system equipment **shall** prevent processes from installing software except for the one specific software installation process identified by the manufacturer.
      - The voting system manufacturer **shall** document the procedures for installing, updating, and removing voting system software, configuration files, and data files.
      - Voting system equipment **shall** prevent processes from installing, updating or removing software while the polls are open.
      - Voting system equipment **shall** prevent the execution of software not installed using the specified software installation process.

   ii. The voting system **shall** only allow authenticated administrators to install software on voting equipment. The voting system **shall** present the administrator with a description of the software change being performed, including:

      - A list of all applications and/or file names being updated.
      - The type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file).

   iii. Voting system equipment **shall** store the current version identification of all software installed on the voting system equipment.

      - The current version identification **shall** be included as part of reports created by the voting system equipment.
      - The current version identification **shall** be displayed as part of the voting system equipment start up process.

iv. The process for installing, updating and removing software **shall** make software changes based on information contained in software update packages. Software update packages **shall** minimally contain the following information:
    - A unique identifier for the software update package.
    - Names of the applications or files modified during the update process.
    - Version numbers of the applications or files modified during the update process.
    - Any software prerequisites or dependencies for the software involved in the update.
    - A description of the type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file).
    - The binary data of any new or updated files involved in the update process.

v. The software update package **shall** be formatted in a non-restrictive, publicly-available format. Manufacturers **shall** provide a specification describing how they have implemented the format with respect to the manufacturer's specific voting devices and data, including such items as descriptions of elements, attributes, constraints, extensions, syntax and semantics of the format, and definitions for data fields and schemas.

vi. Software update packages **shall** be digitally signed by using a NIST approved algorithm with a security strength of at least 112 bits.

vii. The software installation process **shall** verify digital signatures, software version identification, software prerequisites and dependencies, and manufacturer specific authorization information associated with the software before the software is installed. The software installation process **shall** not install software with invalid digital signatures, version numbers, or manufacturer specific authorization information, and **shall** not install software on systems that do not meet the update requisites.

viii. The voting system **shall** have the capability to prevent the installation of previous versions of applications or files.

ix. The software installation process **shall** result in information being stored in the voting system equipment's log such that altering or deleting log entries or the log was detected.

x. The minimum information to be included in the voting system equipment log **shall** be:

- Success or failure of the software installation process.
- Cause of a failed software installation (such as invalid version identification, digital signature, etc.).
- Application or file name(s), and version number(s);
- A description of the type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file);
- A cryptographic hash of the software update package using FIPS 1402 level 1 or higher validated cryptographic module.

f. If software is verified after being installed on the voting system equipment, the voting system equipment **shall** provide an external interface to the location of the voting system software for software verification purposes.
   - i. The external interface:
   - **Shall** be protected using tamper evident techniques,
   - **Shall** have a physical indicator showing when the interface is enabled and disabled
   - **Shall** be disabled during voting
   - Should provide a direct read-only access to the location of the voting system software without the use of installed software ii. The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system manufacturer.
   - If the process uses hashes or digital signatures, then the verification software **shall** use a FIPS 140-2 level 1 or higher validated cryptographic module.
   - The verification process **shall** either (a) use reference information on unalterable storage media received from the repository or (b) verify the digital signature of the reference information on any other media.

g. Setup validation methods **shall** verify the contents of all system storage locations (e.g., system registers, variables, files, etc.) containing election specific information (e.g., ballot style, candidate registers, measure registers, etc.).
   i. The manufacturer should provide a method to query the voting system to determine the value contained in all system storage locations containing election specific information.
   ii. The manufacturer **shall** document the default values of all system storage locations that hold election specific information.

**Results**: The ES&S EVS 6.0.4.2 system allows the jurisdictions to verify that all of the systems in the solution (DS200, DS450, DS850, ExpressVote, and ExpressVote XL) all contain the certified version of the software through a documented hashing and verification process. This process was verified and tested by SLI Compliance as part of the certification effort. As such, the requirement has been satisfactorily covered.

## 7.6 Telecommunications and Data Transmission

There are four areas that must be addressed by telecommunications and data transmission security capabilities: access control, data integrity, detection and prevention of data interception, and protection against external threats.

### 7.6.1 Maintaining Data Integrity

Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function.

a. Voting systems that use electrical or optical transmission of data **shall** ensure the receipt of valid vote records is verified at the receiving station. This should include standard transmission error detection and correction methods such as checksums or message digest hashes. Verification of correct transmission **shall** occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.

    i. Cryptography used to verify the receipt of vote records **shall** use NIST approved algorithms with security strength of at least 112 bits. Message Authentication Code (MAC) keys **shall** have a security strength of at least 112 bits.

**Testing performed**: Tests were performed to verify that data is properly encrypted and that receipt is verified.

**Applicable to**: Electionware, DS450, DS850.

**Results**:

- This requirement was determined to be not applicable. Individual public facing voting components are not networked, nor do they transmit individual voting results. This includes the DS200, the ExpressVote, and the ExpressVote XL, all of which currently have no networking capability to transmit data. This includes examination of wireless and wired network capabilities.

- The only telecommunication capability utilized is an isolated closed network to link the central count scanning devices to the Electionware Client server configuration. The examination reviewed all network traffic between the networked devices and determined that all traffic between the central count scanners utilizes encrypted traffic via the SFTP server. The network communications utilized between the Electionware server and the EMS client also use encryption in the form of TLS / SSL when communicating between the client and the server.
- The examination determined that all results files and relevant election data that is transmitted using these methods is encrypted and digitally signed prior to transmission utilizing ES&S implemented cryptographic methods. This allows the Electionware system to receive, decrypt, and verify that the data has maintained data integrity over the entire transmission process.

## 7.6.2 Election Returns

If the voting system provides access to election returns or interactive inquiries, the system **shall**:

a. Allow authorized administrators the ability to disable or restrict access to election returns (for equipment that operates in a central counting environment). This requirement applies as well to polling place equipment that contains a removable memory module or that may be removed in its entirety to a central place for the consolidation of polling place returns.

b. Design voting system software and its security environment such that data accessible to interactive queries resides in an external file or database created and maintained by the elections software under the restrictions applying to any other output report:

   i. The output file or database has no provision for write access back to the system.

   ii. Persons whose only authorized access is to the file or database are denied write access, both to the file or database, and to the system.

**Testing performed**: Tests were performed to determine that if the system provides access to election returns or interactive queries, then the authorized administrators can disable or restrict access, and that the data resides in an external file or database governed by the voting system.

**Applicable to**: Electionware.

**Results**: Review of the results from testing the system validated that the requirement was satisfactorily covered.

## 7.8.1 Access Control

For those access control features built in as components of the voting system, the S-ATA **shall** design tests to confirm that these security elements work as specified.

Specific activities to be conducted by the S-ATA **shall** include:

b. Specific tests designed by the S-ATA to verify the correct operation of all documented access control procedures and capabilities, including tests designed to circumvent controls provided by the manufacturer. These tests **shall** include:

   i. Performing the activities that the jurisdiction will perform in specific accordance with the manufacturer's access control policy and procedures to create a secure system, including procedures for software and firmware installation.

   ii. Performing tests intended to bypass or otherwise defeat the resulting security environment. These tests **shall** include simulation of attempts to physically destroy components of the voting system in order to validate the correct operation of system redundancy and backup capabilities.

This review applies to the full scope of system functionality. It includes functionality for defining the ballot and other pre-voting functions, as well as functions for casting and storing votes, vote canvassing, vote reporting, and maintenance of the system's audit trail.

**Testing performed**: Tests were performed to verify the documented procedures as well as attempts to defeat the implemented access control security on each system component.

**Applicable to**: Electionware, ExpressVote, ExpressVote XL, DS200, DS450, DS850.

**Results**: Review of the results from testing the system validated that the requirement was satisfactorily covered.

## 7.8.2 Data Interception and Disruption

For systems that use telecommunications, as provided for in section 6 of the Standards and consistent with California law, to transmit official voting data, the S-ATA **shall** review, and conduct tests of, the data interception and prevention safeguards specified by the manufacturer in its TDP. The S-ATA **shall** evaluate safeguards provided by the manufacturer to ensure their proper operation, including the proper response to the detection of efforts to monitor data or otherwise compromise the system.

**Testing performed**: Testing was performed to verify appropriate encryption, receipt validation and data integrity against any attempts to compromise the system.

**Applicable to**: Electionware, DS450, DS850.

**Results**:

- This requirement was determined to be not applicable for polling place devices. Individual public facing voting components are not networked, nor do they transmit individual voting results. This includes the DS200, ExpressVote and the ExpressVote XL. The only telecommunications in use is in an isolated closed network to link the EMS client / server application, and in the central count scanners (DS450 and DS85) for results transmission to the Electionware server for consolidation. Operating system level and SFTP transmissions provided appropriate encryption, receipt validation, and data integrity.
- Review of the results from testing the system validated that the requirement was satisfactorily covered.

## Phase III – Telecommunications and Data Transmission Testing

During Phase III testing of the ES&S EVS 6.0.4.2 system, functional tests were exercised in order to:

- Test system communications, including encryption of data, as well as protocols and procedures for access authorization.

The functional tests were used to verify and validate the system against the following CVSS telecommunications and data transmission requirements:

- 6.1.2 Data Transmission
- 6.2.1 Confirmation

Please see the applicable section below for more details on these requirements and the test results.

## 6.1.2 Data Transmission

These requirements apply to the use of telecommunications to transmit data for the preparation of the system for an election, the execution of an election, and the preservation of the system data and audit trails during and following an election. While this section does not assume a specific model of voting system operations and does not assume a specific model for the use of telecommunications to

support such operations, it does address the following types of data, where applicable:

**Voter Authentication**: Coded information that confirms the identity of a voter for security purposes for a system that transmits votes individually.

**Ballot Definition**: Information that describes to a voting machine the content and appearance of the ballots to be used in an election.

**Vote Count**: Information representing the tabulation of votes at any level within the control of the jurisdiction, such as the polling place, precinct or central count.

**List of Voters**: A listing of the individual voters who have cast ballots in a specific election

Additional data transmissions used to operate a voting system in the conduct of an election, but not explicitly listed above, are also subject to the requirements of this section.

**Testing performed**:

- Testing was performed to verify appropriate encryption, receipt validation, and data integrity.
- Nessus vulnerability scans were conducted on all equipment that were connected to the private EMS network. These included the Electionware Server, Electionware Client, DS450, and DS850.

**Applicable to**: Electionware, DS450, DS850.

**Results**:

- In all cases the vulnerability scans were completed with no significant vulnerabilities detected.
- In the case of the Electionware server in the EMS networked configuration, the vulnerability scanner detected that the SSH server in relation to the SFTP server is configured to support Cipher Block Chaining (CBC) encryption. This only detects the ability to recover the plaintext message from the ciphertext. All attempts to circumvent the SFTP server encryption were unsuccessful.
- Operating system level transmissions provided appropriate encryption, receipt validation, and data integrity.
- Review of the results from testing the system validated that the requirement was satisfactorily covered.

## 6.2.1 Confirmation

Confirmation occurs when the system notifies the user of the successful or unsuccessful completion of the data transmission, where successful completion is

defined as accurate receipt of the transmitted data. To provide confirmation, the telecommunications components of a voting system shall notify the user of the successful or unsuccessful completion of the data transmission. In the event of unsuccessful transmission, the user shall be notified of the action to be taken.

**Testing performed**:

- Testing was performed to verify appropriate confirmation of data transmission to the user and actions to be taken, if any.
- Nessus vulnerability scans were conducted on all equipment that were connected to the private EMS network. These included the Electionware Server, Electionware Client, DS450, and DS850.

**Applicable to**: Electionware, DS450, DS850.

**Results**:

- Operating system level transmissions provided confirmation.
- Review of the results from testing the system validated that the requirement was satisfactorily covered.

## Final Report

During this CVSS requirements examination, issues were noted related to disabled program access, modification of installed software, passwords, port access, software integrity checking, and anti-virus software.

It should be noted that in most cases where vulnerabilities were observed, there are mitigating controls in place to help protect the **ES&S EVS 6.0.4.2** system as a whole. This includes physical access controls including security seals, security screws, lock/key combinations, and in some cases, electronic compartment monitoring. These controls paired with procedural, access control, and authentication mitigation; provide coverage for all of the detected vulnerabilities. The determining factor for a safe and secure election is that the jurisdiction where the system is used is required to implement the system per the vendor documentation, and to follow all the recommendations that are included.

The Following items were considered unmitigated in the traditional sense however procedures and vendor recommendations reduce the risk of an attacker being able to successfully exploit the vulnerability.

- The OKI printers were still configured with active DHCP enabled ethernet ports, and the printer was configured with default user credentials
- **ES&S EVS 6.0.4.2** equipment has the same key for every type of device. It is a vulnerability to not rekey all voting systems and devices.

- The ability for restricted user to utilize windows shortcut keys to circumvent start menu restrictions was not mitigated.
- The ability to launch a command prompt and access restricted programs and system files.
- the ability to gain access to the internal storage and pull password hashes is a vulnerability and given enough time the hashes can be brute forced.
- The Electionware system does not restrict the ability to disable or turn off AV / end-point protection software without requiring a password. No mitigation to this issue were observed.

As directed by the California Secretary of State, this software testing report does not include any recommendation as to whether or not the system should be approved.

End of Security and Telecommunications Testing Test report