ES&S EVS 6.0.4.2
Source Code Review Test Report

ESS-18S52059-CSTR-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
6/13/2019	1.0	D. George	Initial Release
7/16/2019	1.1	D. George	Updates based on comments from CASOS
8/16/2019	1.2	D. George	Additional edits
8/20/2019	1.3	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

Introduction

This report outlines the test approach SLI Compliance (SLI) followed when performing Software Testing on the **ES&S EVS 6.0.4.2** voting system against the California Voting System Standards (CVSS).

References

- California Voting System Standards (CVSS)

System Overview

Voting System Scope

This section provides a description of the **ES&S EVS 6.0.4.2** voting system components:

- DS200 HW 1.3/ 2.20.0.0
- DS450 HW 1.0/ 3.3.0.0
- DS850 HW 1.0/ 3.3.0.0
- ExpressVote HW 2.1/ 2.5.0.0
- ExpressVote XL / 1.2.0.0
- Electionware (EMS) 5.3.0.0

The EVS 6.0.4.2 Election Management System (Electionware, PaperBallot) represents a set of N-Tier software applications (EMS, RTR, Adjudication) for pre-voting and post-voting election project activities that are applicable to jurisdictions of various sizes and geo-political complexities.

The EVS 6.0.4.2 DS450 and DS850 central, high-speed, optical scan ballot counters (tabulators) and are used for processing absentee ballots (such as vote by mail). This ballot counter unit is based on commercial off the shelf (COTS) hardware coupled with custom-made ballot processing application software. It is used for high-speed, accurate, and reliable centralized scanning and counting of paper ballots.

The EVS 6.0.4.2 DS200 system employs a precinct-level optical scan ballot counter (tabulator) in conjunction with an external ballot box. This tabulator is designed to scan paper ballots, interpret voting marks, and deposit the ballots into the secure ballot box.

The EVS 6.0.4.2 ExpressVote and ExpressVote XL ballot marking platforms are solutions used for creation of paper ballots. These ballots are later scanned and tabulated by the DS200, DS850 and DS450 optical ballot counters.

Review Specifications

The following are the specifications for source code testing conducted on the ES&S 6.0.4.2 voting system.

Source Code Review

The ES&S EVS 6.0.4.2 voting system includes proprietary software and firmware. The EVS 6.0.4.2 voting system code base was tested to the applicable CVSS requirements.

Review of the code included:

- Adherence to the applicable standards in sections 5 and 7 of the CVSS.
- Adherence to other applicable coding format conventions and standards including best practices for the coding language used.
  - ESSSYS_1'0_P_CodingStandards.pdf

    Note: This is the standard selected and provided by ES&S that is used in development as allowed by the CVSS Requirements
- Analysis of the program logic and branching structure.
- Evaluate whether the system is designed in a way that allows meaningful analysis, including:
  - Whether the architecture and code is amenable to an external review.
  - Whether code analysis tools can be usefully applied.
  - Whether the code complexity is at a level that obfuscates its logic.

Security considerations reviewed against the code base included:

- Search for exposures to commonly exploited vulnerabilities.
- Evaluate the use and correct implementation of cryptography and key management.
- Analysis of error and exception handling.
- Evaluate the likelihood of security failures being detected:
  - Evaluate whether audit mechanisms are reliable and tamper resistant.
  - Evaluate whether data that might be subject to tampering is properly validated and authenticated.
- Evaluate the risk that a user can escalate his or her capabilities beyond those authorized.
- Evaluate the design and implementation to ensure that sound, generally accepted engineering practices are followed, checking to verify that code is defensively written against:
  - Bad data.
  - Errors in other modules.

- Changes in environment.
- User errors.
- Other adverse conditions.

- Evaluate for embedded, exploitable code (such as “Easter eggs”) that can be triggered to affect the system.
- Evaluate the code for dynamic memory access features which would permit the replacement of certificated executable code or control data or insertion of exploitable code or data.
- Evaluate the code for use of runtime scripts, instructions, or other control data that can affect the operation of security relevant functions or the integrity of the data.

Components and coding languages involved in ES&S’s applications are shown in Table 1.

Table 1 – EVS 6.0.4.2 Components

Component	Language/s	Lines of Code	Standard
DS450	C/C++	605,251	ESSSYS_1’0_P_CodingStandards.pdf
DS850	C/C++	605,251	ESSSYS_1’0_P_CodingStandards.pdf
DS200	C/C++	626,103	ESSSYS_1’0_P_CodingStandards.pdf
ExpressVoteUVS-v2	C/C++ and VB	318,511	ESSSYS_1’0_P_CodingStandards.pdf
ExpressVote XL	C/C++	318,511	ESSSYS_1’0_P_CodingStandards.pdf
PaperBallot	C/C++	495,000	ESSSYS_1’0_P_CodingStandards.pdf
Electionware	Java	950,000	ESSSYS_1’0_P_CodingStandards.pdf

Source Code Review Tools utilized by SLI included:

- Module Finder: an SLI proprietary application used to parse module names from C/C++, Java and VB code and populate the identified module names into the review documents.
- Understand: a commercial application used to review code to stated requirements.

REVIEW RESULTS

Discrepancies

Discrepancies are reported such that the California Secretary of State is provided with a basis for evaluating the extent to which the source code meets applicable standards.

Electionware source code review

No source code requirements were found to be an issue within the Electionware source code base reviewed, as a result, no discrepancies were written against the code base.

PaperBallot source code review

No source code requirements were found to be an issue within the Electionware source code base reviewed, as a result, no discrepancies were written against the code base.

EpressLink source code review

No source code requirements were found to be an issue within the Electionware source code base reviewed, as a result, no discrepancies were written against the code base.

DS200 source code review

No source code requirements were found to be at issue within the DS200 source code base reviewed, as a result, no discrepancies were written against the code base.

DS450 source code review

No source code requirements were found to be at issue within the DS450 source code base reviewed, as a result, no discrepancies were written against the code base.

DS850 source code review

No source code requirements were found to be at issue within the DS850 source code base reviewed, as a result, no discrepancies were written against the code base.

ExpressVote source code review

No source code requirements were found to be at issue within the ExpressVote source code base reviewed, as a result, no discrepancies were written against the code base.

ExpressVote XL source code review

No source code requirements were found to be at issue within the ExpressVote XL source code base reviewed, as a result, no discrepancies were written against the code base.

Vulnerabilities

For any vulnerabilities discovered, SLI was tasked with identifying the particular standards applicable to each vulnerability.

To the extent possible, reported vulnerabilities include an indication of whether the exploitation of the vulnerability would require access by:

- Voter: Usually has low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine(s) for less than an hour.
- Poll worker: Usually has low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine(s) for up to one week, but all physical security has been put into place before the machines are received.
- Elections official insider: Wide range of knowledge of the voting machine design and configuration. May have unrestricted access to the machine for long periods of time. Their designated activities include:
    - Set up and pre-election procedures.
    - Election operation.
    - Post-election processing of results.
    - Archiving and storage operations.
- Vendor insider: With great knowledge of the voting machine design and configuration. They have unlimited access to the machine before it is delivered to the purchaser and, thereafter, may have unrestricted access when performing warranty and maintenance service, and when providing election administration services.

SLI will not verify or demonstrate exploitability of the vulnerability but the report of the vulnerability will identify factors involved in the exploitation.

Any vulnerability theories developed by the source code review team members shall, to the extent possible, be referred to Secretary of State staff.

Electionware source code vulnerability review

No vulnerabilities were found within the Electionware source code base reviewed, as a result, no findings were written against the code base.

PaperBallot source code vulnerability review

No vulnerabilities were found within the PaperBallot source code base reviewed, as a result, no findings were written against the code base.

ExpressLink source code vulnerability review

No vulnerabilities were found within the ExpressLink source code base reviewed, as a result, no findings were written against the code base.

DS200 source code vulnerability review

No vulnerabilities were found within the DS200 source code base reviewed, as a result, no findings were written against the code base.

DS450 source code vulnerability review

No vulnerabilities were found within the DS450 source code base reviewed, as a result, no findings were written against the code base.

DS850 source code vulnerability review

No vulnerabilities were found within the DS850 source code base reviewed, as a result, no findings were written against the code base.

ExpressVote source code vulnerability review

No vulnerabilities were found within the ExpressVote source code base reviewed, as a result, no findings were written against the code base.

ExpressVote XL source code vulnerability review

No vulnerabilities were found within the ExpressVote XL source code base reviewed, as a result, no findings were written against the code base.

Final Report

No discrepancy findings were located within the ES&S EVS 6.0.4.2 code base.

No potential vulnerabilities were identified within the ES&S EVS 6.0.4.2 code base.

As per the direction given 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 Software Test Report