Hart InterCivic Verity Voting 3.1
Voting System Software Test Report
for
California Secretary of State

HRT-19001-CSTR-01

Vendor Name	*Hart InterCivic*
Vendor System	*Verity Voting 3.1*

Prepared by:

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

Accredited by the Election Assistance Commission (EAC) for Selected Voting System Test Methods or Services

Revision History

Date	Release	Author	Revision Summary
October 9, 2019	1.0	*M. Santos*	Initial Release

Disclaimer

The information 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.

Trademarks

- SLI is a registered trademark of SLI Compliance.
- All products and company names are used for identification purposes only and may be trademarks of their respective owners.

TABLE OF CONTENTS

INTRODUCTION

This report outlines the test approach SLI Compliance (SLI) followed when performing Software Testing on the **Hart Verity Voting 3.1** voting system against the California Voting System Standards (CVSS). The purpose of this document is to provide an understanding of the work SLI conducted.

Scope of the Hart InterCivic Verity Voting 3.1 Voting System

This section provides a description of the scope of the following **Hart Verity Voting 3.1** voting system components:

- Verity Data application.
- Verity Build application.
- Verity Count application.
- Verity Central application.
- Verity Election Management.
- Verity Desktop.
- Verity User Manager.
- Verity Scan firmware/hardware.
- Verity Touch Writer with Access firmware/hardware.
- Verity Reader firmware/hardware.
- Verity Print firmware/hardware.

- **Verity Data** provides the user with controls for entering and proofing data and audio. **Verity Data** also performs validation on the exported information to ensure that it will successfully import into **Verity Build**.
- **Verity Build** opens the election to proof data, view reports, and print ballots, and allows for configuring and programming the **Verity Scan** digital scanners, and **Verity Touch Writer** ballot marking devices (BMD), as well as producing the election definition and auditing reports.
- **Verity Count** is an application that tabulates election results and generates reports. **Verity Count** can be used to collect and store all election logs from every Verity component/device used in the election, allowing for complete election audit log reviews.
- **Verity Central** is a high-speed, central digital ballot scanning system used for high-volume processing of ballots (such as vote by mail). The unit is based on commercial-off-the-shelf (COTS) scanning hardware coupled with

the custom **Hart**-developed ballot processing application software which resides on an attached workstation.

- **Verity Election Management** allows users with the Administrator role to import and manage election definitions. Imported election definitions are available through the Elections chevron in Verity Build. Users can also delete, archive, and manage the election definitions.
- **Verity Desktop** enables users, with the correct roles, to set the workstations' date and time, gather Verity application hash codes (in order to validate the correctness of the installed applications), and access to Windows desktop.
- **Verity User Manager** enables users with the correct role and permissions to create and manage user accounts within the Verity Voting system for the local workstation in a standalone configuration, or for the network in a networked configuration.
- **Verity Scan** is a digital scan precinct ballot counter (tabulator) that is used in conjunction with an external ballot box. The unit is designed to scan marked paper ballots, interpret and record voter marks on the paper ballot, and deposit the ballots into the secure ballot box.
- The **Verity Touch Writer** is a standalone precinct level BMD which also includes an Audio Tactile Interface (ATI), which allows voters who cannot complete a paper ballot to generate a machine-readable and human-readable paper ballot, based on vote selections made.
- **Verity Reader** is a voting center ballot reading device for marked paper ballots, that a voter can use to verify how their ballot is being read.
- **Verity Print** is a voting center ballot production device for unmarked paper ballots.

REVIEW SPECIFICATIONS

The following are the specifications for source code testing conducted on the **Hart Verity Voting 3.1** voting system.

Source Code Review

The **Hart Verity Voting 3.1** voting system includes proprietary software and firmware. The 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.

- 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 are 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 the voting system applications are shown in Table 1.

Table 1 – Hart Verity Voting 3.1 Components

Component	Language/s	Lines of Code	Standard
Verity 3.1 Source package	package#	1,375,382	All-In-One Code Framework Coding Standards.pdf
Verity Data	C#	Included in Verity 3.1 Source package count	All-In-One Code Framework Coding Standards.pdf
Verity Build	C#	Included in Verity 3.1 Source package count	All-In-One Code Framework Coding Standards.pdf
Verity Count	C#	Included in previous line count	All-In-One Code Framework Coding Standards.pdf
Verity Central	C#	Included in previous line count	All-In-One Code Framework Coding Standards.pdf
Verity Election Management	C#	Included in previous line count	All-In-One Code Framework Coding Standards.pdf
Verity Desktop	C#	Included in previous line count	All-In-One Code Framework Coding Standards.pdf
Verity User Manager	C#	Included in previous line count	All-In-One Code Framework Coding Standards.pdf
Verity Scan	C#	Included in previous line count	All-In-One Code Framework Coding Standards.pdf
Verity Touch Writer w/ Access	C#	Included in previous line count	All-In-One Code Framework Coding Standards.pdf
Verity Reader	C#	Included in previous line count	All-In-One Code Framework Coding Standards.pdf
Verity Print	C#	Included in previous line count	All-In-One Code Framework Coding Standards.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.
- Examdiff Pro 5: a commercial application used to compare source code deliveries.
- 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.

Verity Data source code review

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

Verity Build source code review

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

Verity Count source code review

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

Verity Central source code review

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

Verity Election Management source code review

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

Verity Desktop source code review

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

Verity User Manager source code review

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

Verity Scan source code review

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

Verity Touch Writer source code review

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

Verity Reader source code review

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

Verity Print source code review

No source code requirements were found to be an issue within the Verity Print 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: 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 the Secretary of State staff.

EMS source code vulnerability review

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

Verity Data source code vulnerability review

No vulnerabilities were found to be an issue within the Verity Data source code base reviewed; as a result, no findings were written against the code base.

Verity Build source code vulnerability review

No vulnerabilities were found to be an issue within the Verity Build source code base reviewed; as a result, no findings were written against the code base.

Verity Count source code vulnerability review

No vulnerabilities were found to be an issue within the Verity Count source code base reviewed; as a result, no findings were written against the code base.

Verity Central source code vulnerability review

No vulnerabilities were found to be an issue within the Verity Central source code base reviewed; as a result, no findings were written against the code base.

Verity Election Management source code vulnerability review

No vulnerabilities were found to be an issue within the Verity Election Management source code base reviewed; as a result, no findings were written against the code base.

Verity Desktop source code vulnerability review

No vulnerabilities were found to be an issue within the Verity Desktop source code base reviewed; as a result, no findings were written against the code base.

Verity User Manager source code vulnerability review

No vulnerabilities were found to be an issue within the Verity User Manager source code base reviewed; as a result, no findings were written against the code base.

Verity Scan source code vulnerability review

No vulnerabilities were found to be an issue within the Verity Scan source code base reviewed; as a result, no findings were written against the code base.

Verity Touch Writer source code vulnerability review

No vulnerabilities were found to be an issue within the Verity Touch Writer source code base reviewed; as a result, no findings were written against the code base.

Verity Reader source code vulnerability review

No vulnerabilities were found to be an issue within the Verity Reader source code base reviewed; as a result, no findings were written against the code base.

Verity Print source code vulnerability review

No vulnerabilities were found to be an issue within the Verity Print source code base reviewed; as a result, no findings were written against the code base.

FINAL REPORT

No discrepancy findings were located within the **Hart Verity Voting 3.1** code base.

No potential vulnerabilities were identified within the **Hart Verity Voting 3.1** code base

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 Software Test Report