Democracy Live
Secure Select 1.0
Security and Telecommunications Test Report

CDL-306-STR-01

Prepared for:

Vendor Name	*Democracy Live*
Vendor System	*Secure Select 1.0*

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
8.24.2017	1.0	*J. Peterson*	Initial Release
8.28.2017	2.0	*M. Santos*	Updated for CASOS comments
8.29.2017	2.1	*M. Santos*	Updates for CASOS comments

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

Overview

This report discusses the results of the Security and Telecommunications testing of the **Democracy Live Secure Select 1.0** remote accessible vote by mail system (RAVBMS).

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

The testing was divided into three (3) phases.

- **Phase I** – **Documentation Review.** This included a review of all pertinent documents for appropriate processes and procedures for implementing a secure system. This included review of the system design and architecture.
- **Phase II – Functional Security Testing**. This phase included testing of relevant software, operating systems and hardware configurations.
- **Phase III – Telecommunications and Data Transmission Testing.** The phase included testing of all telecommunications aspects of the system.

The California Voting Systems Standards (CVSS) were written in such a way to be applicable to a wide variety of voting technology. Therefore, the relevant portions of the CVSS are reviewed as they relate to the Remote Accessible Vote by Mail System (RAVBMS) for purposes of this report. The use of "voting system" shall apply to the RAVBMS.

Phase I – Documentation Review

In this phase, **Democracy Live Secure Select 1.0** documentation was reviewed to verify and validate the following relevant requirements:

- 5.5 Vote Secrecy on Direct Recording Electronic (DRE) and Electronic Ballot Marking (EBM) Systems
- 6.1.2 Data Transmissions
- 6.2 Design, Construction, and Maintenance Requirements
- 6.2.1 Confirmation
- 7.2 Access control
- 7.2.1 General Access Control
- 7.2.2 General Access Control
- 7.4.5 Software Reference Information

- 7.4.6 Software Setup Validation

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

5.5 Vote Secrecy on Direct Recording Electronic (DRE) and Electronic Ballot Marking (EBM) Systems

a. Immediately after the ballot is recorded to persistent electronic storage or printed, erasing the selections from the device's display, working memory, and all other storage, including all forms of temporary storage

b. Immediately after the voter chooses to cancel his or her ballot, erasing the selections from the display and all other storage, including buffers and other temporary storage

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

6.1.2 Data Transmissions

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.

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

6.2 Design, Construction, and Maintenance Requirements

Design, construction, and maintenance requirements for telecommunications represent the operational capability of both system hardware and software. These capabilities **shall** be considered basic to all data transmissions.

Review of the Technical Data Package (TDP) 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.

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

7.1.1 Elements of Security Outside Manufacturers Control

The requirements of this section apply to the capabilities of a voting system that must be provided by the manufacturer. However, an effective security program requires well defined security practices by the purchasing jurisdiction and the personnel managing and operating the system. These practices include:

- Administrative and management controls including access controls
- Internal security procedures
- Adherence to, and enforcement of, operational procedures (e.g., effective password management)
- Security of physical facilities
- Organizational responsibilities and personnel screening

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

7.2 Access Control

Access controls are procedures and system capabilities that detect or limit access to system components in order to guard against loss of system integrity, availability, confidentiality, and accountability. Access controls provide reasonable assurance that system resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized operation, modification, disclosure, loss or impairment. Unauthorized operations include modification of compiled or interpreted code, run-time alteration of flow control logic or of data, and abstraction of raw or processed voting data in any form other than a standard output report by an authorized operator.

Access controls may include physical controls, such as keeping computers in locked rooms to limit physical access, and technical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. The access controls described in this section are limited to those controls required to be provided by system manufacturers.

Review of the Technical Data Package (TDP) validated that the requirement was satisfactorily 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 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.

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

7.2.2 General Access Control

Identification requirements provide controls for accountability when operating and administering a voting system.

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.

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

7.4.5 Software Reference Information

a) The manufacturer **shall** provide the National Software Reference Library (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.

b) 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.

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

Review of the Technical Data Package (TDP) 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.

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

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.

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.

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.).

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

7.8 Testing – Security

The S-ATA **shall** design and perform test procedures that test the security capabilities of the voting system against the requirements. These procedures **shall** focus on the ability of the system to detect, prevent, log, and recover from the broad range of security risks identified. These procedures **shall** also examine system capabilities and safeguards claimed by the manufacturer in the TDP to go beyond these risks. The range of risks tested is determined by the design of the system and potential exposure to risk. Regardless of system design and risk profile, all systems **shall** be tested for effective access control and physical data security.

The S-ATA may meet these testing requirements by confirming proper implementation of proven commercial security software. In this case, the manufacturer must provide the published standards and methods used by the U.S.

Government to test and accept this software, or it may provide references to free, publicly available publications of these standards and methods, such as government web sites.

At its discretion, the S-ATA may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities.

Review of the Technical Data Package (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. 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:

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

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

Phase II - Functional Security Testing

In this phase, functional tests were exercised in order to verify and validate the following requirements:

- 5.5 Vote Secrecy on DRE and EBM Systems
- 7.2.1 General Access Control
- 7.2.2 Access Control Identification
- 7.2.4 Access Control Authorization
- 7.4.5 Software Reference Information
- 7.4.6 Software Setup Validation

- 7.6 Telecommunications and Data Transmission
- 7.8 Testing – Security
- 7.8.1 Access Control
- 7.8.2 Data Interception and Disruption

5.5 Vote Secrecy on Direct Recording Electronic (DRE) and Electronic Ballot Marking (EBM) Systems

a) Immediately after the ballot is recorded to persistent electronic storage or printed, erasing the selections from the device's display, working memory, and all other storage, including all forms of temporary storage

b) Immediately after the voter chooses to cancel his or her ballot, erasing the selections from the display and all other storage, including buffers and other temporary storage

Testing performed: Testing was performed to verify how the system handled a ballot being printed and the browser closed, as well as when the ballot is closed prior to being printed. Attempts were made to resume a ballot, as well as to determine if any ballot information resided in history or cache.

Secure Select 1.0 performed as expected and the requirement is met.

7.2.1 General Access Control

General requirements address the high-level functionality of a voting system. These are the fundamental access control requirements upon which other requirements in this section are based.

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.

Testing performed: Testing was performed of multiple server setups which included an unrestricted test setup, and a data domain whitelist protected system to verify that the whitelisting of JavaScript Object Notation (JSON) domains successfully blocks load of JSON files from an invalid domain.

Secure Select 1.0 performed as expected and the requirement was met.

7.2.2 Access Control Identification

Identification requirements provide controls for accountability when operating and administering a voting system.

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.

Testing performed: Testing was performed to verify the system's ability to correctly process invalid data domain white listings. Two different test systems were tested in order to verify that an open system accepts JavaScript Object Notation (JSON) ballot definition files from anywhere, and that the locked down SS-CA application successfully blocks non-whitelisted domains.

Secure Select 1.0 performed as expected and the requirement was met.

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.

Testing performed: Testing was performed to verify the system's invalid data domain whitelisting. Two different test systems were used to verify that an open system accepts JSON ballot definition files from anywhere, and that the locked down SS-CA application successfully blocks non-whitelisted domains.

Secure Select 1.0 performed as expected and the requirement was met.

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 another designated repository.

Testing performed: Testing was performed to confirm that the **Secure Select 1.0** system contains a Verification URL that contains a hash code value that can be checked to verify if the source code has been modified.

Secure Select 1.0 performed as expected and the requirement was met.

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.

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.

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.

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.).

Testing performed: Testing was performed to confirm that the **Secure Select 1.0** system contains a Verification URL that contains a hash code value that can be checked to verify if the source code has been modified.

Secure Select 1.0 performed as expected and the requirement was met.

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.

Testing performed: Tests were performed to verify that if the system utilizes electrical or optical transmission, that the ballot was sent via SSL, and no receipt is utilized to verify. What is sent is a blank ballot that does not contain any voter data or voting selections.

Secure Select 1.0 performed as expected with regard to usage of SSL, and no receipt is utilized to verify the transaction. For a RAVBMS that is only delivering a blank ballot, this may be considered acceptable, and the requirement is met.

7.8 Testing – Security

The S-ATA shall design and perform test procedures that test the security capabilities of the voting system against the requirements. These procedures shall focus on the ability of the system to detect, prevent, log, and recover from the broad range of security risks identified. These procedures shall also examine system capabilities and safeguards claimed by the manufacturer in the TDP to go beyond these risks. The range of risks tested is determined by the design of the system and potential exposure to risk. Regardless of system design and risk profile, all systems **shall** be tested for effective access control and physical data security.

The S-ATA may meet these testing requirements by confirming proper implementation of proven commercial security software. In this case, the manufacturer must provide the published standards and methods used by the U.S. Government to test and accept this software, or it may provide references to free, publicly available publications of these standards and methods, such as government web sites.

At its discretion, the S-ATA may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities.

Testing performed: Confirmed that **Secure Select 1.0** does not have, nor require, internet access once the ballot has been downloaded. There are no external connections from the ballot to any outside server or service. With the exception of sending the ballot to a connected printer to be printed, there are no external connections to or from the ballot.

Secure Select 1.0 performed as expected and the requirement was met.

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:

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

   Note that sub-requirement "a." is a documentation requirement that is addressed in Phase I above.

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 security environment. These tests **shall** include simulation of attempts to physically destroy components of the voting system in order to validate the 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: Testing was performed to confirm that access control was maintained. Attempts to attack the system included XSS, SQL Injection, Directory listings, and http login pages, as well as SSL certificate information.

Secure Select 1.0 performed as expected and the requirement was met.

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: Verified that this system does not utilize telecommunications for the transmission of official voting data – only the delivery of a blank ballot that does not contain voter data or choice selections.

Secure Select 1.0 performed as expected and the requirement was met.

Phase III – Telecommunications and Data Transmission Testing

In this phase, tests were conducted in order to verify and validate the following requirements:

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

In this phase, tests were exercised to verify and validate the following requirements:

- 6.1.2 Data Transmission
- 6.2 Design, Construction, and Maintenance Requirements
- 6.2.1 Confirmation

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 included transmissions of the **Secure Select 1.0** SPA (Single Page Application) voting ballot that is served from a Hosted webserver, to the voter. Scans were performed to determine if there were any basic web server vulnerabilities in the initial serving of the browser application that houses the **Secure Select 1.0** ballot. None were found.

Secure Select 1.0 performed as expected and the requirement was met.

6.2 Design, Construction, and Maintenance Requirements

Design, construction, and maintenance requirements for telecommunications represent the operational capability of both system hardware and software. These capabilities **shall** be considered basic to all data transmissions.

Testing performed: Verified that **Secure Select 1.0** system consists of a SPA format ballot which is typically used for absentee and mail-in ballot marking. Secure Select 1.0 does not utilize specific telecommunications channels once the ballot has been downloaded and opened on the end voter's machine.

Secure Select 1.0 performed as expected and the requirement was met.

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 included accessing of a ballot from the host and checking for confirmation. This requirement was determined to be not applicable, as the system only allows the voter to mark and confirm marked ballots prior to printing out a ballot summary card. There are no live connections from the application to a remote server. All selections are cleared after browser has been closed.

Secure Select 1.0 performed as expected and the requirement was met.

Potential Vulnerabilities

For any potential 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; and
  - Archiving and storage operations.
- **Vendor Insider**: Possesses 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 security team shall, to the extent possible, be referred to the Secretary of State staff.

7.2.1 General Access Control

- Possible attack vector would be whitelisting a commonly used JavaScript Object Notation (JSON) repository domain. Such domain whitelisting should remain jurisdiction or vendor controlled specific.

For the vulnerability in question, the level of access required to take advantage of this potential vulnerability would be inclusive to the following actors:

- Voter, who could attempt to modify the delivered JSON, or attempt to remotely exploit the web server serving the JSON files.
    - The impact of modifying the delivered JSON file in their own environment would be a local attack, which would only impact that particular voter. The impact is neglible. No mitigation recommended, as what someone does in their own environment is impossible to prevent.
    - The impact of remotely exploiting the server that is serving the JSON files is potentially significant. If the attacker can modify ballots without being detected, they could manipulate voters who utilize the RAVBMS to vote for other than their intended choice. Alternatively if they can at least replace the JSON files with corrupted files, this would serve as a type of denial of service, as when the ballots are marked, printed mailed in and then attempted to be processed, only to be determined to be fraudulent, this could impact many voters such that they are not able to cast their vote. Recommended mitigation is to minimize users and rights to web server, as well as to monitor JSON files and server audit logs as continuously as possible, while the web server is running.
- Election Official Insider, who could attempt to remotely exploit the web server serving the JSON files.
    - The impact of remotely exploiting the server that is serving the JSON files is potentially significant. If the attacker can modify ballots without being detected, they could manipulate voters who utilize the RAVBMS to vote for other than their intended choice. Alternatively if they can at least replace the JSON files with corrupted files, this would serve as a type of denial of service, as when the ballots are marked, printed mailed in and then attempted to be processed, only to be determined to be fraudulent, this could impact many voters such that they are not able to cast their vote. Recommended mitigation is to minimize users and rights to web server, as well as to monitor JSON files and server audit logs as continuously as possible, while the web server is running.
- Vendor Insider, who could attempt to locally exploit the web server serving the JSON files.
    - The impact of remotely exploiting the server that is serving the JSON files is potentially significant. If the attacker can modify ballots without

being detected, they could manipulate voters who utilize the RAVBMS to vote for other than their intended choice. Alternatively if they can at least replace the JSON files with corrupted files, this would serve as a type of denial of service, as when the ballots are marked, printed mailed in and then attempted to be processed, only to be determined to be fraudulent, this could impact many voters such that they are not able to cast their vote. Recommended mitigation is to minimize users and rights to web server, as well as to monitor JSON files and server audit logs as continuously as possible, while the web server is running.

7.4.5 Software Reference Information

Testing did not identify a method of successfully modifying the server code to verify if the protection method was viable. In theory, the functionality is there; however, at this point testing is unable to verify validity.

For the vulnerability in question, the level of access required to take advantage of this potential vulnerability would be inclusive to the following actors:

- Voter, who could attempt to modify the server code remotely.
- Election official insider, who could attempt to modify the server code remotely.
- Vendor Insider, who could attempt to locally modify the server code.

Summary

The **Democracy Live Secure Select 1.0** application is an JSON SPA (Single Page Application), which means that once the initial server call for the application is processed, the entire application runs in the current browser session. Since the SPA doesn't utilize incoming or outgoing connections once the ballot is loaded, this reduces the possibility of interception or manipulation through network attack vectors.

This, however, poses a risk of server side contamination. To help mitigate this, the vendor provides high level documentation about the processes / procedures and security to mitigate these risks. This documentation includes but is not limited to:

- Secure Hosting
- Physical Security of Hosting Sites
- Network Security
- Inventory and Configuration Management

- Access Control
- Monitoring and Logging

It should be noted that security testing of the server side hosting security was not performed beyond review of documentation and attempts to access the provider site. Democracy Live utilizes a commercial cloud based platform to host **Secure Select 1.0**.

Voter privacy is ensured by removing client side storage of marked selections, which allows the voter to verify and print a ballot summary card for use in currently setup jurisdiction absentee / mail-in voting programs.

The ability to tamper with the client side application is always present due to the fact there are no server side verifications or validations in place. In this context, however, the ability to affect large numbers of ballots is reliant upon server side compromise (initial **Secure Select 1.0** ballot launch), and the failure of the Absentee / Mail-in ballot system. The voter is given the ability to proof and confirm ballot selections within the **Secure Select 1.0** interactive ballot system as well as the paper ballot summary. The voter is also required to print, sign and mail the ballot.

For the vulnerability of a malicious actor exploiting the web server serving the JSON ballot files.

The impact of remotely exploiting the server that is serving the JSON files is potentially significant. If the attacker can modify ballots without being detected, they could manipulate voters who utilize the RAVBMS to vote for other than their intended choice. Alternatively if they can at least replace the JSON files with corrupted files, this would serve as a type of denial of service, as when the ballots are marked, printed mailed in and then attempted to be processed, only to be determined to be fraudulent, this could impact many voters such that they are not able to cast their vote. Recommended mitigation is to minimize users and rights to web server, as well as to monitor JSON files and server audit logs as continuously as possible, while the web server is running

No discrepancy findings were identified within the **Democracy Live Secure Select 1.0** RAVBMS.

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

End of Security and Telecommunications Test Report