WYLE REPORT NO. T59087.01

Appendix A.4

Security

TEST CASE PROCEDURE SPECIFICATION

ES&S EVS 5.0.0.0
(T59087.01)

TABLE OF CONTENTS

Page No.

1.0 INTRODUCTION……..……..……2

1.1. Scope ……..….2
1.2. References ……..…….2
1.3. Terms and Abbreviations ……..…..3
1.4. Relationship to Other Procedures .....……..……..…..3

2.0 DETAILS ……..……...……3

2.1. Inputs, Outputs, and Special Requirements…..……..….7
2.2. WOP 6 Test Suite ……..…..7
2.3. Discovery & Exploratory Functional Security Testing ……..….7

ATTACHMENTS

ATTACHMENT A – SECURITY TEST MATRIX…….....8

ATTACHMENT B – 2005 VVSG REQUIREMENTS CHECKLIST.....9

1.0 INTRODUCTION

The purpose of the Security Test Case Procedure Specification is to document the "Security" functionality of the ES&S EVS 5.0.0.0 Voting System. Wyle verified that the ES&S EVS 5.0.0.0 performed as documented in the ES&S supplied Technical Data Package submitted to Wyle for the test campaign. Wyle also validated that the EVS 5.0.0.0 met the requirements of the 2005 EAC Voluntary Voting Systems Guidelines (VVSG). Wyle qualified personnel used this document as the procedure to execute the "Security" test.

1.1 Scope

The scope of this procedure was to focus on the security technologies used in the ES&S EVS 5.0.0.0 voting system. The EVS 5.0.0.0 used security technologies to secure the hardware, software, and storage media during pre-voting, voting, and post voting activities. Capabilities were provided to ensure that the EVS 5.0.0.0 was protected against unauthorized activity, potential threats, and intentional manipulation. Public networks are not used as part of the EVS 5.0.0.0 system. The specific applications of the EVS 5.0.0.0 used in this test suite are:

- EVS5000 System (as a whole)
- EMS PC applications and peripherals
- DS200 Precinct Voting Devices
- DS850 Central Count Voting Device
- Network Cable Run
- Transport Media (TM) (USB & CF)
- Ballot Boxes & (DS200) (AutoMark)
- Ballot Tote Bin
- AutoMARK (A100, A200 & A300)

1.2 References

The media listed below were utilized as part of this test:

- Parikh, Clay U., CEH, CHFI, CISSP. Wyle Security Test Summary of ES&S Voting System Version 3400. Letter. May 21, 2012. Print.
- Parikh, Clay U., CEH, CHFI, CISSP. Wyle Security Test Summary of ES&S Voting System Version 5.0.0.0 (EVS5000). Letter. May 15, 2012. Print.
- United States Election Assistance Commission. 2005 Voluntary Voting System Guidelines, Volume I, Version 1.0. New York, Washington D.C., 2005, Print
- United States Election Assistance Commission. 2005 Voluntary Voting System Guidelines, Volume II, Version 1.0. New York, Washington D.C., 2005. Print
- United States Election Assistance Commission. Testing and Certification Program Manual, Version 1.0. New York, Washington, January 1, 2007. Print
- United States Election Assistance Commission. Voting System Test Laboratory Program Manual, Version 1.0, New York, Washington, effective date July 2008. Print
- United States Department of Commerce, National Institute of Standards and Technology. National Voluntary Laboratory Accreditation Program, NIST Handbook 150, 2006 Edition, NVLAP, Washington, February 2006. Print
- United States Department of Commerce, National Institute of Standards and Technology. National Voluntary Laboratory Accreditation Program, NIST Handbook 150-22, 2008 Edition, NVLAP, Washington, May 2008. Print
- Help America Vote Act (HAVA) of 2002, Pub. L. no. 107-252. October 2002. Web
- Wyle Laboratories. Quality Assurance Program Manual, Revision 4. Print
- ANSI/NCSL Z540-3, Calibration Laboratories and Measuring and Test Equipment, General Requirements. Web

- United States Election Assistance Commission. Notices of Clarification. Web, EAC.gov
- United States Election Assistance Commission. Requests for Interpretation. Web, EAC.gov
- NIST Standards for Security Categorization of Federal Information and Information Systems, FIPS PUB 199, February 2004

1.3 Terms and Abbreviations

The terms and abbreviations relevant to the test campaign are described in Table 1-1, below.

Table 1-1 Terms and Abbreviations

Term	Abbreviation	Definition
United States Election Assistance Commission	EAC	Commission created per the Help America Vote Act of 2002, assigned the responsibility for setting voting system standards and providing for the voluntary testing and certification of voting systems.
Election Manager System	EMS	The Election Management System (EMS) is a set of applications responsible for all pre-voting and post-voting activities in the process of defining and managing elections. The complete EMS software platform consists of client (end-user) and server (back-end) applications.
Equipment Under Test	EUT	The components of the voting system being tested.
Personal Computer	PC	The EMS Windows Operating System (OS) desktop computer and peripherals.
Technical Data Package	TDP	The documents necessary to define the product and its method of operation; to provide technical and test data supporting the vendor's claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance.
Transport Media	TM	Universal Serial Bus (USB) Disc Drives and Compact Flash (CF) Cards used by the system to transport election data.
Voluntary Voting System Guidelines	VVSG	---

1.4 Relationship to Other Procedures

The Security Test Case Procedure Specification is a standalone procedure. No other test procedures need to be run concurrent with this procedure.

2.0 DETAILS

The following sections describe the requirements that are applicable to the EVS5.0.0.0 and individual test cases that will be run in to facilitate security testing.

Table 2-1 Security Requirements

Section		Requirement
VI-7.2.1		ES&S shall specify the general features and capabilities of the access control policy recommended to provide effective voting system security.
VI-7.2.1	a	Software access controls
VI-7.2.1	b	Hardware access controls
VI-7.2.1	c	Communications
VI-7.2.1	d	Effective password management
VI-7.2.1	e	Protection abilities of a particular operating system
VI-7.2.1	f	General characteristics of supervisory access privileges
VI-7.2.1	g	Segregation of duties
VI-7.2.1	h	Any additional relevant character

V1-7.2.1.1		ES&S shall provide individual access privileges
V1-7.2.1.1	a	Identify each person, to whom access is granted, and the specific functions and data to which each person holds authorized access.
V1-7.2.1.1	b	Specify whether an individual's authorization is limited to a specific time, time interval, or phase of the voting or counting operations.
V1-7.2.1.1	c	Permit the voter to cast a ballot expeditiously, but preclude voter access to all aspects of the vote-counting processes
V1-7.2.1.2		Provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include.
V1-7.2.1.2	a	Use of data and user authorization.
V1-7.2.1.2	b	Program unit ownership and other regional boundaries.
V1-7.2.1.2	c	One-end or two-end port protection devices.
V1-7.2.1.2	d	Security kernels.
V1-7.2.1.2	e	Computer-generated password keys.
V1-7.2.1.2	f	Special protocols.
V1-7.2.1.2	g	Message encryption.
V1-7.2.1.2	h	Controlled access security.
V1-7.2.1.2		ES&S also shall define and provide a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself.
V1-7.3.1		For polling place operations, ES&S shall develop and provide a detailed documentation of measures to enable poll workers to physically protect and perform orderly shutdown of the voting equipment to counteract vandalism civil disobedience, and similar occurrence. • Allow the immediate detection of tampering with vote casting devices and precinct ballot counters. • Control physical access to a telecommunications link if such a link is used.
V1-7.3.2		ES&S 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: • Handling of ballot boxes. • Preparing of ballots for counting. • Counting operations. • Reporting data.
V1-7.4		Provide specific security requirements for the installation of software and for the protection against malicious software. Provide security requirements for hardware with embedded firmware.
V1-7.4.1	a	If software is resident in the system as firmware, ES&S 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.
V1-7.4.1	b	No software shall be permanently installed or resident in the 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.
V1-7.4.1	c	The 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.
V1-7.4.1	d	The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as computer chip) other than the component on which the operating system resides.
V1-7.4.1	e	After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.
V1-7.4.2		EVS5.0.0.0 shall deploy 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. Vendors shall develop and document the procedures to be followed to ensure that such protection is maintained in a current status.

V1-7.4.4	a	ES&S shall document all software including EVS5.0.0.0 software, third party software (such as operating systems and drivers) to be installed on the EVS5.0.0.0, and installation
V1-7.4.4	a i	The documentation shall have a unique identifier (such as a serial number or part number) for the following set of information: • documentation • software vendor name • product name, version • the certification application number of the voting system • file names • paths or other location information(such as storage addresses) of the software
V1-7.4.4	a ii	The documentation shall designate all software files as static, semi-static or dynamic.
V1-7.4.4	b	Wyle shall witness the final build of the executable version of the EVS5.0.0.0 software performed by ES&S.
V1-7.4.4	b i	Wyle shall create a complete record of the build that includes: • a unique identifier (such as a serial number) for the complete record • a list of unique identifiers of unalterable storage media associated with the record • the time, date, location, names and signatures of all people present • the source code and resulting executable file names • the version of EVS5.0.0.0 software • the certification application number of the EVS5.0.0.0 • the name and versions of all (including third party) libraries • the name, version, and configuration files of the development environment used for the build
V1-7.4.4	b ii	The record of the source code and executable files shall be made on unalterable storage media. Each piece of media shall have a unique identifier.
V1-7.4.4	b iii	Wyle shall retain this record until notified by the EAC that it can be archived.
V1-7.4.4	c	After EAC certification has been granted, Wyle shall create a subset of the complete record of the build that includes: • a unique identifier (such as a serial number) of the subset • the unique identifier of the complete record • a list of unique identifiers of unalterable storage media associated with the subset • the vendor and product name • the version of EVS5.0.0.0 software • the certification number of the EVS5.0.0.0 • all the files that resulted from the build and binary images of all installation programs
V1-7.4.4	c i	The record of the software shall be made on unalterable storage media. Each piece of media shall have a unique identifier.
V1-7.4.4	c ii	Wyle shall retain a copy, send a copy to the vendor, and send a copy to the NIST National Software Reference Library (NSRL) and/or to any repository designated by a State.
V1-7.4.4	c iii	The NSRL shall retain this software until notified by the EAC that it can be archived.
V1-7.4.4	d	ES&S shall provide the NSRL and any repository designated by a state with a copy of the software installation disk, which ES&S will distribute to purchasers--including the executable binary images of all third party software.
V1-7.4.4	d i	All EVS5.0.0.0 software, installation programs and third party software (such as operating systems and drivers) used to install or to be installed on the EVS5.0.0.0 equipment shall be distributed using unalterable storage media.
V1-7.4.4	d ii	ES&S 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.
V1-7.4.4	e	The EVS5.0.0.0 equipment shall be designed to allow the EVS5.0.0.0 administrator to verify that the software is the certified software by comparing it to reference information produced by the NSRL or other designated repository.
V1-7.4.4	f	ES&S and Wyle shall document to whom they provide the EVS5.0.0.0 software.
V1-7.4.6	a	Setup validation methods shall verify that no unauthorized software is present on the voting equipment.

V1-7.4.6	b	ES&S shall have a process to verify that: • the correct software is loaded • there is no unauthorized software • voting system software on voting equipment has not been modified using the reference information from the NSRL or from a State designated repository.
V1-7.4.6	b i	The process used to verify software should be possible to perform without using software installed on the EVS5.0.0.0.
V1-7.4.6	b ii	ES&S shall document the process used to verify software on the EVS5.0.0.0 equipment.
V1-7.4.6	b iii	The process shall not modify the EVS5.0.0.0 software on the EVS5.0.0.0 during the verification process.
V1-7.4.6	c	ES&S shall provide a method to comprehensively list all software files that are installed on the EVS5.0.0.0.
V1-7.4.6	d	The verification process should be able to be performed using COTS software and hardware available from sources other than ES&S.
V1-7.4.6	d i	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.
V1-7.4.6	d ii	The verification process shall either: (a) use reference information on unalterable storage media received from a repository, or (b) verify the digital signature of the reference information on any other media.
V1-7.4.6	e	EVS5.0.0.0 equipment shall provide a means to ensure that the EVS5.0.0.0 software can be verified through a trusted external interface, such as a read-only external interface, or by other means.
V1-7.4.6	e i	The external interface system shall be protected using tamper evident techniques.
V1-7.4.6	e ii	The external interface shall have a physical indicator showing when the interface is enabled and disabled.
V1-7.4.6	e iii	The external interface shall be disabled during voting.
V1-7.4.6	e iv	The external interface should provide a direct read-only access to the location of the EVS5.0.0.0 software without the use of installed software.
V1-7.4.6	f	Setup validation methods shall verify that the registers and variables of the voting system equipment contain the proper static and initial values.
V1-7.4.6	f i	ES&S should provide a method to query the EVS5.0.0.0 to determine the values of all static and dynamic registers and variables including the values that jurisdictions are required to modify to conduct a specific election.
V1-7.4.6	f ii	ES&S shall document the values of all static registers and variable, and the initial starting values of all dynamic registers and variables listed for voting system software, except for the values set to conduct a specific election.
V1-7.5.1	b i	Implement an encryption standard currently documented and validated for use by an agency of the U.S. Federal Government.
V1-7.5.1	b ii	Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System.
V1-7.5.5	a	For equipment that operates in a central counting environment, be designed to provide external access to incomplete election returns only if that access for these purposes is authorized by the statutes and regulations of the using agency. 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.
V1-7.5.5	b	Design voting system software and its security environment designed 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, namely, that:
V1-7.5.5	b i	The output file or database has no provision for write-access back to the system.
V1-7.5.5	b 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.

V1-7.8.1		Independent (IV) systems are electronic voting systems that produce multiple independent cast vote records of voter ballot selections, which can be audited to a high level of precision. For this to happen, the cast vote records must be handled according to the following protocol: • At least two cast vote records of the voter's selections are produced and one of the records is then stored in a manner that it cannot be modified by the voting system. For example, the voting system creates a record of the voter's selections and then copies it to unalterable storage media. • The voter must be able to verify that both cast vote records are correct and match before leaving the polling place, e.g., verify his or her selections on the voting machine summary screen and also verify the second record on the unalterable storage media. • The verification processes for the two cast vote records must be independent of each other, and at least one of the records must be verified directly by the voter. • The contents of the two cast vote records also can be checked later for consistency through the use of unique identifiers that allow the records to be linked. The cast vote records would be formatted so that at least one set is usable in an efficient counting process by the electronic voting system and the other set is usable in an efficient process of auditing or verifying the agreement between the two sets.

2.1 Inputs, Outputs, and Special Requirements

Inputs used during security testing will be the following:

- Test election loaded on a preconfigured DS200, DS850, AutoMARK, and EMS
- All passwords for all access control levels generated by the EMS software for the test elections.

Special scanning applications will be configured as pre-test activity and provide the platform for all security scans.

2.2 WoP 6 Test Suite Test

As a pre-test activity, WoP 6, WoP 6a, WoP 6b, WoP 6c, and WoP 6d will be completed to gather the necessary documentation for exploratory security testing.

2.3 Discovery and Exploratory Functional Security Testing

The functional security testing was broken into two phases. The first phase was discovery phase. Scans were performed on different components of the EVS 5.0.0.0 at different states targeting initialization, maintenance, and election states. These scans provided information about the ports, protocols, and hardware as well as simulate certain attacks on vulnerable areas of the system. This information was provided to a certified security professional for analysis. The analysis of this data provided the method of attack during the exploratory phase of testing. Exploratory testing was performed by a certified security professional at Wyle's facilities. A complete report of the exploratory testing results was provided to ES&S and Wyle for review. The certified security professional documented any vulnerable areas of the EVS 5.0.0.0 and provide recommended solutions.

ATTACHMENT A
SECURITY TEST MATRIX

Component Under Test	HW Access Points	Physical Security	Software Validation	Logical Security
AutoMARK (A100, A200, A300)	Passed	Passed	Passed in Final Build Hash	Tested in FCA
Ballot Holding Bin (plastic)	N/A	Passed by TDP Policy	N/A	N/A
Ballot Holding Bin (card board)	N/A	Passed by TDP Policy	N/A	N/A
DS200	Passed	Passed	Passed in Final Build Hash	Tested in FCA
Ballot Box (plastic)	Passed	Passed	N/A	N/A
Ballot Box (metal)	Passed	Passed	N/A	N/A
DS850	Passed by TDP Policy	Passed by TDP Policy	Passed in Final Build Hash	Passed by TDP Policy
Network	Passed by TDP Policy	Passed by TDP Policy	N/A	N/A
Ballot Box (listed in the TDP but N/A)	N/A	Passed by TDP Policy	N/A	N/A
EMS	Passed	Passed by TDP Policy	Passed	Passed
ElectionWare	Passed	Passed by TDP Policy	Passed	Passed
ERM	Passed	Passed by TDP Policy	Passed	Passed
ULS	Passed	Passed by TDP Policy	Passed	Passed
Network	Passed by TDP Policy	Passed by TDP Policy	Passed	Passed
Transport Media				
USB (DS200 / DS850 EQC)	N/A	Passed by TDP Policy	N/A	Passed
USB (DS200 EMD pre)	N/A	Passed by TDP Policy	N/A	Passed
USB (DS200 EMD post)	N/A	Passed by TDP Policy	N/A	Passed
Flash Cards (DS200)	N/A	Passed by TDP Policy	N/A	VOTE_TC-ESS200-15
Flash Card (AutoMARK)	N/A	Passed by TDP Policy	N/A	Passed
USB (DS850 EMD pre)	N/A	Passed by TDP Policy	N/A	Passed
USB (DS850 EMD post)	N/A	Passed by TDP Policy	N/A	Passed
Flash Card (DS850)	N/A	Passed by TDP Policy	N/A	VOTE_TC-ESS200-15
Tote Box	Passed	Passed by TDP Policy	N/A	N/A
Security Seals (band aide)	N/A	Passed	N/A	N/A

ATTACHMENT B

2005 VVSG REQUIREMENTS CHECKLIST

"X" Requirements were met

VVSG Req. No.	2005 VVSG Volume I Functional Requirement Matrix	REQUIREMENTS MET
Vol. I	**Voting System Performance Guidelines**	
Section 2	**Functional Requirements**	
2.1	**Overall System Capabilities**	
2.1.1	**Security**	
	System security is achieved through a combination of technical capabilities and sound administrative practices. The ensure security, all system shall:	
a	Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.	**X**
b	Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.	**X**
c	Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met.	**X**
d	Provide safeguards in response to system failure to protect against tampering during system repair or interventions in system operations.	**X**
e	Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparations, testing, and operation.	**X**
f	Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled	**X**
g	Provide documentation of mandatory administrative procedures for effective system security	**X**
Section 7	**Security**	
7.2	**Access Control**	
7.2.1	**General Access Control Policy**	
	The vendor shall specify the general features and capabilities of the access control policy recommended to provide effective voting system security. Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for:	
a	Software access controls	**X**
b	Hardware access controls	**X**
c	Communications	**X**
d	Effective password management	**X**
e	Protection abilities of a particular operating system	**X**
f	General characteristics of supervisory access privileges	**X**
g	Segregation of duties	**X**
h	Any additional relevant characteristics	**X**
7.2.1.1	**Individual Access Privileges**	
	Voting system vendors shall:	
a	Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access	**X**
b	Specify whether an individual's authorization is limited to a specific time, time interval or phase of the voting or counting operations	**X**
c	Permit the voter to cast a ballot expeditiously, but preclude voter access to all aspects of the vote counting processes	**X**

VVSG Req. No.	2005 VVSG Volume I Functional Requirement Matrix	REQUIREMENTS MET
Vol. I	**Voting System Performance Guidelines**	
7.2.1.2	**Access Control Measures**	
	Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include:	
a	Use of data and user authorization	**X**
b	Program unit ownership and other regional boundaries	**X**
c	Communications	**X**
d	Security kernels	**X**
e	Computer-generated password keys	**X**
f	Special protocols	**X**
g	Message encryption	**X**
h	Controlled access security	**X**
	Vendors also shall define and provide a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself.	**X**
7.3	**Physical Security Measures**	
7.3.1	**Polling Place Security**	
	For polling place operations, vendors 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. They also shall control physical access to a telecommunications link if such a link is used.	**X**
7.3.2	**Central Count Location Security**	
	Vendors 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.	**X**
7.4	**Software Security**	
7.4.1	**Software and Firmware Installation**	
	The system shall meet the following requirements for installation of software, including hardware with embedded firmware.	
a	If software is resident in the system as firmware, the vendor 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.	**X**
b	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.	**X**
c	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.	**X**

VVSG Req. No.	2005 VVSG Volume I Functional Requirement Matrix	REQUIREMENTS MET
Vol. I	**Voting System Performance Guidelines**	
7.4	**Software Security**	
7.4.1	**Software and Firmware Installation**	
d	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.	**X**
e	After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.	**X**
7.4.2	**Protection Against Malicious Software**	
	Voting systems shall deploy 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. Vendors shall develop and document the procedures to be followed to ensure that such protection is maintained in a current status.	**X**
7.4.4	**Software Distribution**	
a	The vendor 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.	**X**
i	The documentation shall have a unique identifier (such as a serial number or part number) for the following set of information: documentation, software vendor 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.	**X**
ii	The documentation shall designate all software files as static, semi-static or dynamic. Discussion: Static voting system software such as executable code does not change based on the election being conducted or the voting equipment upon which it is installed. Semi static voting system software contains configuration information for the voting system based on the voting equipment that is installed and the election being conducted. Semi-static software is only modified during the installation of (a) the voting system software on voting equipment or (b) the election-specific software such as ballot formats. Dynamic voting system software changes over time once installed on voting equipment. However, the specific time or value of the change in the dynamic software is usually unknown in advance, making it impossible to create reference information to verify the software.	**X**
b	The EAC accredited testing lab shall witness the final build of the executable version of the certified voting system software performed by the vendor.	**X**
i	The testing lab shall create a complete record of the build that includes: a unique identifier (such as a serial number) for the complete record; a list of unique identifiers of unalterable storage media associated with the record; the time, date, location, names and signatures of all people present; the source code and resulting executable file names; the version of voting system software; the certification application number of the voting system; the name and versions of all (including third party) libraries; and the name, version, and configuration files of the development environment used for the build.	**X**

VVSG Req. No.	2005 VVSG Volume I Functional Requirement Matrix	REQUIREMENTS MET
Vol. I	**Voting System Performance Guidelines**	
7.4	**Software Security**	
7.4.4	**Software Distribution**	
ii	The record of the source code and executable files shall be made on unalterable storage media. Each piece of media shall have a unique identifier. Discussion: Unalterable storage media includes technology such as a CD-R, but not CD-RW. The unique identifiers appear on indelibly printed labels and in a digitally signed file on the unalterable storage media.	**X**
iii	The testing lab shall retain this record until notified by the EAC that it can be archived.	**X**
c	After EAC certification has been granted, the testing lab shall create a subset of the complete record of the build that includes a unique identifier (such as a serial number) of the subset, the unique identifier of the complete record, a list of unique identifiers of unalterable storage media associated with the subset, the vendor and product name, the version of voting system software, the certification number of the voting system, and all the files that resulted from the build and binary images of all installation programs.	**X**
i	The record of the software shall be made on unalterable storage media. Each piece of media shall have a unique identifier.	**X**
ii	The testing lab shall retain a copy, send a copy to the vendor, and send a copy to the NIST National Software Reference Library (NSRL)2 and/or to any repository designated by a State.	**X**
iii	The NSRL shall retain this software until notified by the EAC that it can be archived.	**X**
d	The vendor shall provide the NSRL and any repository designated by a state with a copy of the software installation disk, which the vendor will distribute to purchasers-- including the executable binary images of all third party software.	**X**
i	All voting system software, installation programs and third party software (such as operating systems and drivers) used to install or to be installed on voting system equipment shall be distributed using unalterable storage media.	**X**
ii	The vendor 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.	**X**
e	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.	**X**
f	The vendors and testing labs shall document to whom they provide voting system software.	**X**
7.4.6	**Software Setup Validation**	
a	Setup validation methods shall verify that no unauthorized software is present on the voting equipment.	**X**
b	The vendor shall have a process to verify that the correct software is loaded, that there is no unauthorized software, and that voting system software on voting equipment has not been modified, using the reference information from the NSRL or from a State designated repository.	**X**

VVSG Req. No.	2005 VVSG Volume I Functional Requirement Matrix	REQUIREMENTS MET
Vol. I	**Voting System Performance Guidelines**	
7.4	**Software Security**	
7.4.6	**Software Setup Validation**	
i	The process used to verify software should be possible to perform without using software installed on the voting system.	**X**
ii	The vendor shall document the process used to verify software on voting equipment.	**X**
iii	The process shall not modify the voting system software on the voting system during the verification process.	**X**
c	The vendor shall provide a method to comprehensively list all software files that are installed on voting systems.	**X**
d	The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system vendor.	**X**
i	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.	**X**
ii	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.	**X**
e	Voting system equipment shall provide a means to ensure that the system software can be verified through a trusted external interface, such as a read-only external interface, or by other means.	**X**
i	The external interface shall be protected using tamper evident techniques	**X**
ii	The external interface shall have a physical indicator showing when the Interface is enabled and disabled	**X**
iii	The external interface shall have a physical indicator showing when the Interface is enabled and disabled	**X**
iv	The external interface should provide a direct read-only access to the location of the voting system software without the use of installed software	**X**
f	Setup validation methods shall verify that registers and variables of the voting system equipment contain the proper static and initial values.	**X**
i	The vendor should provide a method to query the voting system to determine the values of all static and dynamic registers and variables including the values that jurisdictions are required to modify to conduct a specific election.	**X**
ii	The vendor shall document the values of all static registers and variables, and the initial starting values of all dynamic registers and variables listed for voting system software, except for the values set to conduct a specific election.	**X**
7.5	**Telecommunications and Data Transmission**	
7.5.1	**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.	**N/A**

VVSG Req. No.	2005 VVSG Volume I Functional Requirement Matrix	REQUIREMENTS MET
Vol. I	**Voting System Performance Guidelines**	
7.5	**Telecommunications and Data Transmission**	
7.5.1	**Maintaining Data Integrity**	
b	Voting systems that use telecommunications to communicate between system components and locations before the polling place is officially closed shall:	**N/A**
i	Implement an encryption standard currently documented and validated for use by an agency of the U.S. government	**N/A**
ii	Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System	**N/A**
7.5.5	**Incomplete Election Returns**	
	If the voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, the system shall:	**N/A**
a	Be designed to provide external access to incomplete election returns (for equipment that operates in a central counting environment), only if that access for these purposes is authorized by the statutes and regulations of the using agency. 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	**N/A**
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:	**N/A**
i	The output file or database has no provision for write access back to the system	**N/A**
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	**N/A**
7.8	**Independent Verification Systems**	
7.8.1	**Overview**	
	Independent verification (IV) systems are electronic voting systems that produce multiple independent cast vote records of voter ballot selections, which can be audited to a high level of precision. For this to happen, the cast vote records must be handled according to the following protocol: • At least two cast vote records of the voter's selections are produced and one of the records is then stored in a manner that it cannot be modified by the voting system. For example, the voting system creates a record of the voter's selections and then copies it to unalterable storage media. • The voter must be able to verify that both cast vote records are correct and match before leaving the polling place, e.g., verify his or her selections on the voting machine summary screen and also verify the second record on the unalterable storage media. • The verification processes for the two cast vote records must be independent of each other, and at least one of the records must be verified directly by the voter. • The contents of the two cast vote records also can be checked later for consistency through the use of unique identifiers that allow the records to be linked. The cast vote records would be formatted so that at least one set is usable in an efficient counting process by the electronic voting system and the other set is usable in an efficient process of auditing or verifying the agreement between the two sets.	**N/A**