WYLE REPORT NO. T56285-01

APPENDIX A.4

SECURITY

TEST CASE PROCEDURE SPECIFICATION (T56285-60)

50 pages including cover page

wyle

7800 Highway 20 West
Huntsville, Alabama 35806
Phone (256) 837-4411
Fax (256) 721-0144
www.wyle.com

SECURITY
TEST CASE PROCEDURE SPECIFICATION
FOR
UNISYN VOTING SOLUTIONS, INC.
OPENELECT VOTING SYSTEM, VERSION 1.0

Prepared by:

Jack Cobb 12-29-09

Jack Cobb, Senior Project Engineer

TABLE OF CONTENTS

ATTACHMENTS

1.0 INTRODUCTION

The purpose of the Security Test Case Procedure Specification is to document the "Security" functionality of the Unisyn OpenElect Voting System (OVS), version 1.0. Wyle must verify that the OVS performs as documented in the Unisyn supplied Technical Data Package submitted to Wyle for the test campaign. Wyle must also validate that the OVS meets the requirements of the 2005 EAC Voluntary Voting Systems Guidelines (VVSG). Wyle qualified personnel will use this document as the procedure to execute the "Security" test.

1.1 Scope

The scope of this procedure will focus on the security technologies used in the Unisyn OpenElect Voting System (OVS). The OVS uses security technologies to secure the hardware, software, telecommunications, and storage media during pre-voting, voting, and post voting activities. Capabilities shall be provided to ensure that the OVS is protected against unauthorized activity, potential threats and intentional manipulation. All telecommunication transmissions used by OVS employ Hypertext Transfer Protocol over Secure Socket Layer (https) on a closed private Local Area Network (LAN). Public networks are not used as part of the OVS system. The specific applications of the OVS used in this test suite are:

- Election Server (ES)
- Election Manager (EM)
- Ballot Layout Manager (BLM)
- Software Server (SS)
- Tabulator Client (TC)
- Tabulator
- OpenElect Voting Central Scan (OVCS)
- OpenElect Voting Optical Scan (OVO)
- OpenElect Voting Interface (OVI)

1.2 References

The documents listed below were used in the development of the Test Plan and are utilized to perform certification testing.

- Election Assistance Commission 2005 Voluntary Voting System Guidelines, Volume I, Version 1.0, "Voting System Performance Guidelines", and Volume II, Version 1.0, "National Certification Testing Guidelines", dated December 2005
- Election Assistance Commission Testing and Certification Program Manual, Version 1.0, effective date January 1, 2007
- Election Assistance Commission Voting System Test laboratory Program Manual, Version 1.0, effective date July 2008
- National Voluntary Laboratory Accreditation Program NIST Handbook 150, 2006 Edition, "NVLAP Procedures and General Requirements (NIST Handbook 150)", dated February 2006
- National Voluntary Laboratory Accreditation Program NIST Handbook 150-22, 2008 Edition, "Voting System Testing (NIST Handbook 150-22)", dated May 2008

1.0 INTRODUCTION (continued)

1.2 References (continued)

- United States 107th Congress Help America Vote Act (HAVA) of 2002 (Public Law 107-252), dated October 2002
- Wyle Laboratories' Quality Assurance Program Manual, Revision 4
- ANSI/NCSL Z540-1, "Calibration Laboratories and Measuring and Test Equipment, General Requirements"
- ISO 10012-1, "Quality Assurance Requirements for Measuring Equipment"
- EAC Requests for Interpretation (listed on www.eac.gov)
- EAC Notices of Clarification (listed on www.eac.gov)

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
Commercial Off the Shelf	COTS	---
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 Management System	EMS	Within the OpenElect system, the EMS equivalent is OCS.
Election Server	ES	A component of the OCS, the ES updates the system clock and downloads new Election data to the voting devices prior to each election, typically at the warehouse.
Equipment Under Test	EUT	---
OpenElect Central Suite	OCS	Set of applications supplied by Unisyn to run at the Election Headquarters to support elections on the OVO, OVI, and OVCS systems. Includes: Ballot Layout Manager, Election Manager, Election Server, Tabulator Client, Tabulator Server and Tabulator Reports. In addition, the OCS includes the Software Server (SS) system for updating and validating OVO and OVI (voting device) software.
OpenElect Voting Device	OVD	OVD refers to the OVO, OVI, and OVCS hardware components of the OpenElect Voting System.
OpenElect Voting Interface	OVI	The OVI is an accessible voting device designed to accommodate voters with disabilities, and may also be used for Early Voting.
OpenElect Voting Optical Scan	OVO	The OVO is a ballot scanning and tabulation device which is located at a precinct and may also be used for Early Voting purposes.
OpenElect Voting System	OVS	The OVS is a voting system which is comprised of the OVS suite of software applications, and the OVO and OVI client machines used by voters to produce and cast ballots.

1.0 INTRODUCTION (continued)

1.3 Terms and Abbreviations (continued)

Table 1-1 Terms and Abbreviations (continued)

Software Server	SS	The SS application is used for the updating and validation of Certified Software Releases which are installed on OVS client machines.
OpenElect Voting Central Scan	OVCS	The OVCS is a COTS ballot scanning device that uses proprietary software to capture ballot images.
Tabulator Client	TC	The TC is a software application that retrieves vote files from the TM and transfers the files to the Tabulator.
Tabulator		Tabulator is a software application that receives uploaded voting data.
Ballot Layout Manager	BML	Unisyn OVS application used to layout ballot information.
Election Manager	EM	Utilizes the election definition file from the Ballot Layout Manager, adds jurisdiction voting device specific options and produces the CD used to load the election onto the voting devices and OVCS.

1.4 Relationship to Other Procedures

The Security Test Case Procedure Specification is a stand alone 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 OVS and individual test cases that will be run in to facilitate security testing.

Table 2-1 Security Requirements

Section		Requirement
VI-7.2.1		Unisyn 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		Unisyn 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.

2.0 DETAILS (continued)

Table 2-1 Security Requirements (continued)

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		Unisyn 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, Unisyn 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		Unisyn 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, Unisyn 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		OVS 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	Unisyn shall document all software including OVS software, third party software (such as operating systems and drivers) to be installed on the OVS, and installation programs.

2.0 DETAILS (continued)

Table 2-1 Security Requirements (continued)

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 OVS software performed by Unisyn.
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 OVS software • the certification application number of the OVS • 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 OVS software • the certification number of the OVS • 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	Unisyn shall provide the NSRL and any repository designated by a state with a copy of the software installation disk, which Unisyn will distribute to purchasers--including the executable binary images of all third party software.
V1-7.4.4	d i	All OVS software, installation programs and third party software (such as operating systems and drivers) used to install or to be installed on the OVS equipment shall be distributed using unalterable storage media.
V1-7.4.4	d ii	Unisyn 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 OVS equipment shall be designed to allow the OVS 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	Unisyn and Wyle shall document to whom they provide the OVS software.

2.0 DETAILS (continued)

Table 2-1 Security Requirements (continued)

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	Uniysn 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 OVS.
V1-7.4.6	b ii	Unisyn shall document the process used to verify software on the OVS equipment.
V1-7.4.6	b iii	The process shall not modify the OVS software on the OVS during the verification process.
V1-7.4.6	c	Unisyn shall provide a method to comprehensively list all software files that are installed on the OVS.
V1-7.4.6	d	The verification process should be able to be performed using COTS software and hardware available from sources other than Unisyn.
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	OVS equipment shall provide a means to ensure that the OVS 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 OVS 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	Unisyn should provide a method to query the OVS 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	Unisyn 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		OVS uses telecommunications to communicate between system components so it is subject to the same security requirements governing access to any other system hardware, software, and data function.
V1-7.5.1	a	Voting systems that use electrical or optical transmission of data shall ensure the receipt of valid vote records is verified at the receiving station. This should include standard transmission error detection and correction methods such as checksums or message digest hashes. Verification of correct transmission shall occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.
V1-7.5.1	b	OVS uses telecommunications to communicate between system components before the polling place is officially closed shall:
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.

2.0 DETAILS (continued)

Table 2-1 Security Requirements (continued)

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 OVS
- All passwords for all access control levels generated by the OVS 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. These WoPs are attached in Appendix B.

2.3 Automated Source Code Analysis

As a pre-test activity, the OVS source code suite will be scanned using Fortify SCA. A complete report will be transmitted to Unisyn for review and remediation before the discovery phase of security testing will be started. These reports are attached in Appendix C.

2.0 DETAILS (continued)

2.4 Discovery and Exploratory Functional Security Testing

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

ATTACHMENT A

SECURITY TEST CASES

Security Test Case

<table>
<tr><td colspan="4">**Test Case:** Security Testing for Unisyn OVS.</td></tr>
<tr><td colspan="2">**VVSG Requirements**</td><td colspan="2">V1-7.2, 7.3, 7.4, 7.5</td></tr>
<tr><td colspan="3">**Test Objective:**</td><td>**Test Configuration:**</td></tr>
<tr><td colspan="3">This test the security of the OVS. A scanning laptop will be used to the scan the security of EM, ES, and Tab. Scanning will be performed (leveraged- passwords generated by the OCS are used) and (unleveraged- passwords generated by the OCS are not used)</td><td>Machine with preconfigured OCS and election loaded. A separate laptop with special scanning software will be used to verify security in the OCS.</td></tr>
<tr><td colspan="2">**Devices & Tools Utilized:**</td><td colspan="2">Preconfigured OVS with election loaded on the system.
Scanning laptop
Nessus client v4.0.1 (build 4G1045_Q), Nmap 5.00 and Zenmap 5.00 (Nmap’s GUI)
Unisyn policy for Nessus configured by a certified security professional.</td></tr>
<tr><td colspan="2">**Special Requirements**</td><td colspan="2">A preconfigured OVS with a test election and all the necessary passwords will be needed for this test.</td></tr>
<tr><td colspan="2">**Assumptions**</td><td colspan="2">This test case will not have detailed step by step procedures for security testing. It is assumed the test case will be a general procedure. This test will be performed under the guidance of a certified security professional. All data gathered will be validated by a certified security professional.</td></tr>
<tr><td>**Step**</td><td colspan="3">**Procedure**</td></tr>
<tr><td>**0**</td><td colspan="3">Record the election version being used on the OCS.</td></tr>
<tr><td>**10000**</td><td colspan="3">Record date and time of the test start. Record test operator.</td></tr>
<tr><td>**10010**</td><td colspan="3">**NMAP (unleveraged)**
Scan the EM, ES, and Tab with Nmap 5.00 using standard connect scan. (Hub IP depedant)
• Connect scan laptop to system and scan OR Connect scan laptop, startup system, scan (if ports really do shutdown after server check)
• Configure system if needed, re scan
• Run Zenmap with credentials, if needed (if showing remote connection ports)
Nessus (unleveraged)
Scan the EM, ES and Tab with Nessus client v4.0.1, using Unisyn policy. Save the report with “unlev” in the name.
Nessus (leveraged)
Scan the EM, ES and Tab with Nessus client v4.0.1, using Unisyn policy. Save the report with “lev” in the name.</td></tr>
<tr><td>**10020**</td><td colspan="3">**Scans (OVI, OVO)**
Start scans for the OVI and OVO as in step **10010,** except as noted below.
• (Nmap) Connect scan laptop, startup system, scan
• (Nessus) Enter maintenance mode, configure, scan</td></tr>
<tr><td>**10030**</td><td colspan="3">**Group 1 tests (EM, ES, Tab)**
This step should start the same time as step **10020** above. Perform the group 1 tests listed below for the EM, ES, Tab:
• File permission checks on critical files/apps/directories
• Account checks (privileges, passwords)
• Bios – order change, backdoor, potential MBR attacks, on crypto
• Xwindows – bypass/short cut desktop
• Password policy enforcement
• Injection attacks (overflows)</td></tr>
<tr><td>**10040**</td><td colspan="3">**Group 1 tests (OVI, OVO)**
Perform the Group 1 test in the above step **10030** for the OVI and OVO, expect for the Xwindows test.</td></tr>
</table>

Security Test Case (continued)

<table>
<tr><td><b>10050</b></td><td><b>TM and Group 2 tests</b>
Perform the TM tests and perform the group 2 tests for the appropriate system, as listed on security test spreadsheet
TM tests:
• Only Unisyn type hardware
• Clean or cleared
Group 2 tests:
• Attacks from key – TM
• File manipulation
• OCS installer</td></tr>
<tr><td></td><td><b>Other Tests</b>
Finish the rest of tests listed on security test spreadsheet on the appropriate system. These tests involve setup or running election scenarios.
• Test verification process
• Election Day network connectivity
• Hardware connections (USB, LAN)
• Data corruption – view other election
• Data validation – absentee ballots check
• EM to OVCS control
• Build on check, OS
• Hidden key check</td></tr>
<tr><td colspan="2"><b>Criteria for Evaluation of the Test Results</b>
The results of this test will be accepted if the scan files from Nmap and Nessus are verified by the certified security professional for analysis and no security changes are required by Unisyn.   Any recommended security changes to the system need to be logged and analyzed by Wyle qualified personnel.</td></tr>
</table>

Security Test Spreadsheet

Unisyn OVS Security Tests						
complete	**TEST**	**EM/ES**	**Tab Cluster**	**OVI**	**OVO**	**TM**
	Ports, Protocols, Services Scan w/ Nmap	x	x	x	x	
	Ports, Protocols, Services Scan w/ Nmap (leveraged)	x	x	x	x	
	Vulnerability Scan w/Nessus	x	x	x	x	
	Vulnerability Scan w/Nessus (leveraged)	x	x	x	x	
	File permission checks on critical files/apps/directories	x	x	x	x	
	Account checks (*privileges, password*)	x	x	x	x	
	Test Verification Process	x	x	x	x	
	Attacks from key - TM	x	x	x	x	
	File manipulation	x	x			x
	OS Tests					
	Bios - order change, backdoor, potential mbr attack on crypto	x	x	x	x	
	Xwindows - bypass/short cut desktop	x	x			
	password policy enforcement	x	x	x	x	
	election day network connectivity			x	x	
	Hardware connections (usb, lan)	x	x	x	x	
	Application Tests					
	Injection attacks (overflows)	x	x	x	x	
	OCS Installer	x	x			
	Data corruption - view other election	x	x			
	Data validation - Absentee ballots check -?	x				
	EM to OVCS control	x				
	Build on check, OS	x	x			
	Hidden key check			x	x	
	TM Tests					
	Only Unisyn type					x
	Clean or cleared					x

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

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:	**X**
i	Implement an encryption standard currently documented and validated for use by an agency of the U.S. government	**X**
ii	Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System	**X**
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:	
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	**X**
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:	**X**
i	The output file or database has no provision for write access back to the system	**X**
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	**X**
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.	**X**

ATTACHMENT C

SECURITY WOP SUITES

VOLUME I **SECTION 7** **Security Requirements**	**VOTING SYSTEMS GUIDELINES** **2005 (Ver. 1)**	**Vendor:** **Job Number:** **Date:**

Test Title: Security Requirements

Requirements Reference: VVSG Volume I, Sections 7 Security Requirements and Section 2.1.4 h. Integrity

Test Description: The objectives of the security standards for voting systems are:

- To protect critical elements of the voting system
- To establish and maintain controls to minimize errors
- To protect the system from intentional manipulation, fraud and malicious mischief
- To identify fraudulent or erroneous changes to the voting system
- To protect secrecy in the voting process

Maintenance of a permanent record of original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g., during the canvassing process).

Applicability: Security requirements apply to the system's hardware, software, communications and documentation. The requirements apply to the broad range of hardware, software, communications components, and documentation that comprises a voting system. These requirements apply to those components that are:

- Provided by the voting system vendor and the vendor's suppliers
- Furnished by an external provider (i.e., providers of personal computers and COTS operating systems) where the components are capable of being used during voting system operation
- Developed by a voting jurisdiction

The requirements apply to all software used in any manner to support any voting-related activity, regardless of the ownership of the software or the ownership and location of the hardware on which the software is installed or operated. These requirements apply to software that operates on:

- Voting devices and vote counting devices installed at polling places under the control or authority of the voting jurisdiction
- Ballot printers, vote counting devices, and other hardware typically installed at central or precinct locations (including contractor facilities)

Acceptance Criteria: The voting system must successfully guard against the following risks:

- Unauthorized changes to system capabilities for:
  - — Defining ballot formats
  - — Casting and recording votes
  - — Calculating vote totals consistent with defined ballot formats
  - — Reporting vote totals
- Alteration of voting system audit trails
- Changing, or preventing the recording of, a vote
- Introducing data for a vote not cast by a registered voter
- Changing calculated vote totals
- Preventing access to vote data--including individual votes and vote totals—by unauthorized individuals
- Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes
- Requirements for software distribution to purchasing jurisdictions

- Generation of reference information to validate software
- Validation of software using the reference information
- Requirements regarding the use of wireless communications
- Requirements for DREs with voter verifiable paper trail components

Verification of security measures for telecommunication and data transmission, including access control, data integrity, detection and prevention of data interception, and protection against external threats.

Test Data Required: Test Plan, Receiving Inventory, TDP, WoP 6a - WoP 6d.

Test Requirement/Procedure:

Instructions:
Complete the following table:

Provide a reason where shown for all test steps marked N/A.

Section A: System Identification

Vendor Name: ______________________	**System Name:** ______________________ **Version submitted for Test certification:** ______________________
Security Test Method conducted in period: ***enter dates***	**From:** ___/___/___ **To:** ___/___/___
Test Location(s):	______________________
Project Engineer:	______________________

For each test step in the following table (Section B), check the appropriate status box. The status definitions indicate the Pass/Fail status of each test step and are specifically defined as follows:

1. **P** - The test step has Passed or is satisfactorily complete.
2. **F** - The test step has Failed or a non-conformance to the expected result has occurred.
3. **NA** - This test step is Not Applicable – *indicate briefly the reason under Comments.*
4. **U** - This test was not executed. *(Enter explanation under Comments when the test procedure has been executed)*

Section B: General Security Checks

STEP #	ACTION	Pass (or Complete) / Fail / NA / Untested	Comments / Data and Ref. to Anomalies
1a	*Configuration Baseline - Hardware*	P□ F□ NA□ U□	

- Examine all Customer Furnished Equipment (CFE) to be used in testing.
- Check WoP 3 results to ensure TDP passed or did not have any issues concerning hardware.
- Review the vendor TDP.
- Compare hardware with that documented in TDP.
    - If no issues then Pass this test step.
    - Review issues with PM/Vendor.

Record test equipment Hardware Products, Model #'s, Serial Numbers in table below.

1a.1 *Hardware (Vendor proprietary – tabulators, voting devices...):*

1. Product:______________________ Model: ____________ Serial #:__________
2. Product:______________________ Model: ____________ Serial #:__________
3. Product:______________________ Model: ____________ Serial #:__________
4. Product:______________________ Model: ____________ Serial #:__________
5. Product:______________________ Model: ____________ Serial #:__________
6. Product:______________________ Model: ____________ Serial #:__________
7. Product:______________________ Model: ____________ Serial #:__________
8. Product:______________________ Model: ____________ Serial #:__________
9. Product:______________________ Model: ____________ Serial #:__________
10. Product:______________________ Model: ____________ Serial #:__________

Check if List is continued on additional pages: □ *Total Number of Items listed:* ______

1a.2 *Hardware (COTS – laptop computers, storage devices etc.):*

1. Product:______________________ Model: ____________ Serial #:__________
2. Product:______________________ Model: ____________ Serial #:__________
3. Product:______________________ Model: ____________ Serial #:__________
4. Product:______________________ Model: ____________ Serial #:__________
5. Product:______________________ Model: ____________ Serial #:__________
6. Product:______________________ Model: ____________ Serial #:__________
7. Product:______________________ Model: ____________ Serial #:__________
8. Product:______________________ Model: ____________ Serial #:__________
9. Product:______________________ Model: ____________ Serial #:__________
10. Product:______________________ Model: ____________ Serial #:__________

Check if List is continued on additional pages: □ *Total Number of Items listed:* ______

1a.3 *Software (Proprietary e.g. EMS components – Ballot Generation, Tally...)*

1. Product:________________________ Model: ______________ Serial #:____________
2. Product:________________________ Model: ______________ Serial #:____________
3. Product:________________________ Model: ______________ Serial #:____________
4. Product:________________________ Model: ______________ Serial #:____________
5. Product:________________________ Model: ______________ Serial #:____________
6. Product:________________________ Model: ______________ Serial #:____________
7. Product:________________________ Model: ______________ Serial #:____________
8. Product:________________________ Model: ______________ Serial #:____________
9. Product:________________________ Model: ______________ Serial #:____________
10. Product:________________________ Model: ______________ Serial #:____________

Check if List is continued on additional pages: □ *Total Number of Items listed:* ______

Software (COTS e.g. Windows OS, ...)

1. Product:________________________ Model: ______________ Serial #:____________
2. Product:________________________ Model: ______________ Serial #:____________
3. Product:________________________ Model: ______________ Serial #:____________
4. Product:________________________ Model: ______________ Serial #:____________
5. Product:________________________ Model: ______________ Serial #:____________
6. Product:________________________ Model: ______________ Serial #:____________
7. Product:________________________ Model: ______________ Serial #:____________
8. Product:________________________ Model: ______________ Serial #:____________
9. Product:________________________ Model: ______________ Serial #:____________
10. Product:________________________ Model: ______________ Serial #:____________

Check if List is continued on additional pages: □ *Total Number of Items listed:* ______

STEP #	ACTION	Pass (or Complete) / Fail / NA / Untested	Comments / Data and Ref. to Anomalies
2	Risk: Unauthorized changes to the system capabilities for defining ballot formats.		Reference the TDP section addressing this test step.
	Review the vendor's TDP *(esp. system capabilities and safeguards).*		____________________ ____________________
	Verify that the TDP documents how the system is able to...		
	a. Detect the unauthorized change.	a. P□ F□ NA□ U□	*a.* ____________________
	b. Prevent the unauthorized change.	b. P□ F□ NA□ U□	*b.* ____________________
	c. Log the unauthorized change.	c. P□ F□ NA□ U□	*c.* ____________________
	d. Recover from the unauthorized change to ballot definitions.	d. P□ F□ NA□ U□	*d.* ____________________
3	Risk: Unauthorized changes to the system capabilities for Casting and recovering votes		Reference the TDP section addressing this test step.
	Review the vendor's TDP *(esp. system capabilities and safeguards).*		____________________ ____________________
	Verify that the TDP documents how the system is able to...		
	a. Detect the unauthorized change.	a. P□ F□ NA□ U□	*a.* ____________________
	b. Prevent the unauthorized change.	b. P□ F□ NA□ U□	*b.* ____________________
	c. Log the unauthorized change.	c. P□ F□ NA□ U□	*c.* ____________________
	d. Recover from the unauthorized change affecting Casting and recovering votes.	d. P□ F□ NA□ U□	*d.* ____________________

4	<u>Risk: Unauthorized changes to the system capabilities for Calculating vote totals consistent with defined ballot formats</u>		Reference the TDP section addressing this test step.
	Review the vendor's TDP *(esp. system capabilities and safeguards).*		________________ ________________
	Verify that the TDP documents how the system is able to...		
	a. Detect the unauthorized change.	a. P□ F□ NA□ U□	*a.* ________________
	b. Prevent the unauthorized change.	b. P□ F□ NA□ U□	*b.* ________________
	c. Log the unauthorized change.	c. P□ F□ NA□ U□	*c.* ________________
	d. Recover from the unauthorized change affecting calculation of vote totals.	d. P□ F□ NA□ U□	*d.* ________________
5	<u>Risk: Unauthorized changes to the system capabilities for Reporting vote totals</u>		Reference the TDP section addressing this test step.
	Review the vendor's TDP *(esp. system capabilities and safeguards).*		________________ ________________
	Verify that the TDP documents how the system is able to...		
	a. Detect the unauthorized change.	a. P□ F□ NA□ U□	*a.* ________________
	b. Prevent the unauthorized change.	b. P□ F□ NA□ U□	*b.* ________________
	c. Log the unauthorized change.	c. P□ F□ NA□ U□	*c.* ________________
	d. Recover from the unauthorized change affecting the Reporting of vote totals.	d. P□ F□ NA□ U□	*d.* ________________

4	Risk: Unauthorized changes to the system capabilities for Calculating vote totals consistent with defined ballot formats		Reference the TDP section addressing this test step.
	Review the vendor's TDP *(esp. system capabilities and safeguards).*		____________________ ____________________
	Verify that the TDP documents how the system is able to...		
	a. Detect the unauthorized change.	a. P□ F□ NA□ U□	*a.* ____________________
	b. Prevent the unauthorized change.	b. P□ F□ NA□ U□	*b.* ____________________
	c. Log the unauthorized change.	c. P□ F□ NA□ U□	*c.* ____________________
	d. Recover from the unauthorized change affecting calculation of vote totals.	d. P□ F□ NA□ U□	*d.* ____________________
5	Risk: Unauthorized changes to the system capabilities for Reporting vote totals		Reference the TDP section addressing this test step.
	Review the vendor's TDP *(esp. system capabilities and safeguards).*		____________________ ____________________
	Verify that the TDP documents how the system is able to...		
	a. Detect the unauthorized change.	a. P□ F□ NA□ U□	*a.* ____________________
	b. Prevent the unauthorized change.	b. P□ F□ NA□ U□	*b.* ____________________
	c. Log the unauthorized change.	c. P□ F□ NA□ U□	*c.* ____________________
	d. Recover from the unauthorized change affecting the Reporting of vote totals.	d. P□ F□ NA□ U□	*d.* ____________________

6 Risk: Alteration of voting audit trails.

Reference the TDP section addressing this test step.

____
____

Review the vendor's TDP *(esp. system capabilities and safeguards).*

Verify that the TDP documents how the system is able to...

a. Detect the alteration of the voting audit trail. a. P□ F□ NA□ U□ *a.* ______________________

b. Prevent the alteration of the voting audit trail. b. P□ F□ NA□ U□ *b.* ______________________

c. Log the alteration of the voting audit trail. c. P□ F□ NA□ U□ *c.* ______________________

d. Recover from the alteration of the voting audit trail. d. P□ F□ NA□ U□ *d.* ______________________

7 Risk: Changing, or preventing the recording of, a vote.

Reference the TDP section addressing this test step.

Review the vendor's TDP *(esp. system capabilities and safeguards).*

____
____

Verify that the TDP documents how the system is able to...

a. Detect this risk. a. P□ F□ NA□ U□ *a.* ______________________

b. Prevent this risk. b. P□ F□ NA□ U□ *b.* ______________________

c. Log this risk. c. P□ F□ NA□ U□ *c.* ______________________

d. Recover from the attempt to change or prevention of the recording of a vote. d. P□ F□ NA□ U□ *d.* ______________________

8	Risk: Introducing data for vote not cast by a register voter.		Reference the TDP section addressing this test step.
	Review the vendor's TDP *(esp. system capabilities and safeguards).*		____________________ ____________________
	Verify that the TDP documents how the system is able to...		
	a. Detect this risk.	a. P□ F□ NA□ U□	*a.* ____________________
	b. Prevent this risk.	b. P□ F□ NA□ U□	*b.* ____________________
	c. Log this risk.	c. P□ F□ NA□ U□	*c.* ____________________
	d. Recover from the attempt to introduce data for a vote not cast by a register voter.	d. P□ F□ NA□ U□	*d.* ____________________
9	Risk: Changing calculated vote totals.		Reference the TDP section addressing this test step.
	Review the vendor's TDP *(esp. system capabilities and safeguards).*		____________________ ____________________
	Verify that the TDP documents how the system is able to...		
	a. Detect a change to the calculated vote totals.	a. P□ F□ NA□ U□	*a.* ____________________
	b. Prevent this risk.	b. P□ F□ NA□ U□	*b.* ____________________
	c. Log this risk.	c. P□ F□ NA□ U□	*c.* ____________________
	d. Recover from the unauthorized attempt to change the calculated vote totals.	d. P□ F□ NA□ U□	*d.* ____________________

10	Risk: Preventing access to vote data including individual votes and vote totals by unauthorized individuals.		Reference the TDP section addressing this test step. ____________________ ____________________
	Review the vendor's TDP *(esp. system capabilities and safeguards).*		
	Verify that the TDP documents how the system is able to…		
	a. Detect this risk.	a. P□ F□ NA□ U□	*a.* ____________________
	b. Prevent this risk.	b. P□ F□ NA□ U□	*b.* ____________________
	c. Log this risk.	c. P□ F□ NA□ U□	*c.* ____________________
	d. Recover from an unauthorized attempt to access vote data, votes and vote totals.	d. P□ F□ NA□ U□	*d.* ____________________
11	Risk: Preventing access to voter identification data and data for votes cast by voter such that an individual can determine the content of specific votes.		Reference the TDP section addressing this test step. ____________________ ____________________
	Review the vendor's TDP *(esp. system capabilities and safeguards).*		
	Verify that the TDP documents how the system is able to…		
	a. Detect this risk.	a. P□ F□ NA□ U□	*a.* ____________________
	b. Prevent this risk.	b. P□ F□ NA□ U□	*b.* ____________________
	c. Log this risk.	c. P□ F□ NA□ U□	*c.* ____________________
	d. Recover from an unauthorized attempt to access voter identification data and data for votes cast by voter such that an individual can determine the content of specific votes.	d. P□ F□ NA□ U□	*d.* ____________________

- Report any discrepancies (indications of Failed test steps) in accordance with accepted anomaly reporting.

Section C: Access Controls Security Testing

STEP #	ACTION	Pass (or Complete) / Fail / NA / Untested	Comments / Data and Ref. to Anomalies
1	Access Controls and system capabilities Review the vendor's TDP *(<u>esp. Access Control Policies</u>)*.		Reference the TDP section addressing this test step. ____________________ ____________________
	From this review verify that the vendor's access control policies, procedures and system capabilities address the following concerns: a) Software access controls b) Hardware access controls c) Communications d) Effective password management e) Protection abilities of a particular operating system. f) General characteristics of supervisory access privileges g) Segregation of duties h) Any additional relevant characteristics. *(Indicate TDP ref. in comments column)*	a. P□ F□ NA□ U□ b. P□ F□ NA□ U□ c. P□ F□ NA□ U□ d. P□ F□ NA□ U□ e. P□ F□ NA□ U□ f. P□ F□ NA□ U□ g. P□ F□ NA□ U□ h. P□ F□ NA□ U□	*a.* ____________________ *b.* ____________________ *c.* ____________________ *d.* ____________________ *e.* ____________________ *f.* ____________________ *g.* ____________________ *h.* ____________________
2	Individual Access Privileges Review the vendor's TDP *(<u>esp. Access Control Policies</u>)*.		Reference the TDP section addressing this test step. ____________________ ____________________
	From this review verify that the vendor's access control policies, procedures and system capabilities are able to: a) Identify each person, to whom access is granted, and the specific functions and data to which each person holds authorized access. b) Specify whether an individual's authorization is limited to a specific time, time interval, or phase of the voting or counting operations. c) Permit the voter to cast a ballot expeditiously, but preclude voter access to all other aspects of the vote-counting processes. *(Indicate TDP ref. in comments column)*	a. P□ F□ NA□ U□ b. P□ F□ NA□ U□ c. P□ F□ NA□ U□	*a.* ____________________ *b.* ____________________ *c.* ____________________

3 Access Control Measures
Review the vendor's TDP *(esp. Access Control Policies and Measures)*.

Reference the TDP section addressing this test step.

____
____

From this review verify that the vendor's access control measures are designed to permit authorized access to the system and prevent unauthorized access in the following areas:

a) Use of data and user authorization;
b) Program unit ownership and other regional boundaries;
c) One-end or two-end port protection devices;
d) Security kernels;
e) Computer-generated password keys;
f) Special protocols;
g) Message encryption; and
h) Controlled access security.

(Indicate TDP ref. in comments column)

a. P□ F□ NA□ U□ *a.* ______________________
b. P□ F□ NA□ U□ *b.* ______________________
c. P□ F□ NA□ U□ *c.* ______________________
d. P□ F□ NA□ U□ *d.* ______________________
e. P□ F□ NA□ U□ *e.* ______________________
f. P□ F□ NA□ U□ *f.* ______________________
g. P□ F□ NA□ U□ *g.* ______________________
h. P□ F□ NA□ U□ *h.* ______________________

4 Actual test and Verification

List any specific findings from WoP 6a.

Conduct WoP 6a to help verify that the previous steps are indeed implemented within the voting system.

P□ F□ NA□ U□ ______________________
____

Section D: Physical Security Testing

STEP #	ACTION	Pass (or Complete) / Fail / NA / Untested	Comments / Data and Ref. to Anomalies
1	Polling Place Security Review the vendor's TDP *(esp. in regard to Polling Place security measures)*.		Reference the TDP section addressing this test step. ________________ ________________
	From this review verify that the vendor addresses issues and measures to:		
	a) Allow the immediate detection of tampering with vote casting devices and precinct ballot counters; and	a. P□ F□ NA□ U□	*a.* ________________
	b) Control physical access to a telecommunications link *if* such a link is used.	b. P□ F□ NA□ U□	*b.* ________________
	(Indicate TDP ref. in comments column)		
2	Central Count Location Security Review the vendor's TDP *(esp. in regard to the Central Count environment)*.		Reference the TDP section addressing this test step. ________________ ________________
	From this review verify that the vendor addresses issues and measures relating to:		
	a) Handling of ballot boxes;	a. P□ F□ NA□ U□	*a.* ________________
	b) Preparing of ballots for counting;	b. P□ F□ NA□ U□	*b.* ________________
	c) Counting operations; and	c. P□ F□ NA□ U□	*c.* ________________
	d) Reporting data.	d. P□ F□ NA□ U□	*d.* ________________
	(Indicate TDP ref. in comments column)		
3	Actual test and Verification		List any specific findings from WoP 6b.
	Conduct WoP 6b to help verify that the previous steps are indeed implemented within the voting system.	P□ F□ NA□ U□	________________ ________________

Section E: Software Security Testing

STEP # 	ACTION	Pass (or Complete) / Fail / NA / Untested	Comments / Data and Ref. to Anomalies
1	(REF 7.4.1) Software and Firmware Installation Review the vendor's TDP *(esp. Software and Firmware Installation)*		Reference the TDP section addressing this test step. __________________ __________________
	From this review verify that the vendor's software and installation documentation states that:		
	a) Every device is to be retested to validate each ROM prior to the start of elections operations *(for software resident in the system as firmware)*	a. P□ F□ NA□ U□	*a.* __________________
	b) To prevent alteration of executable code, 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;	b. P□ F□ NA□ U□	*b.* __________________
	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;	c. P□ F□ NA□ U□	*c.* __________________
	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; and	d. P□ F□ NA□ U□	*d.* __________________
	e) After initiation of Election Day testing, no source code or compilers or assemblers shall be resident or accessible.	e. P□ F□ NA□ U□	*e.* __________________
	(Indicate TDP ref. in comments column)		

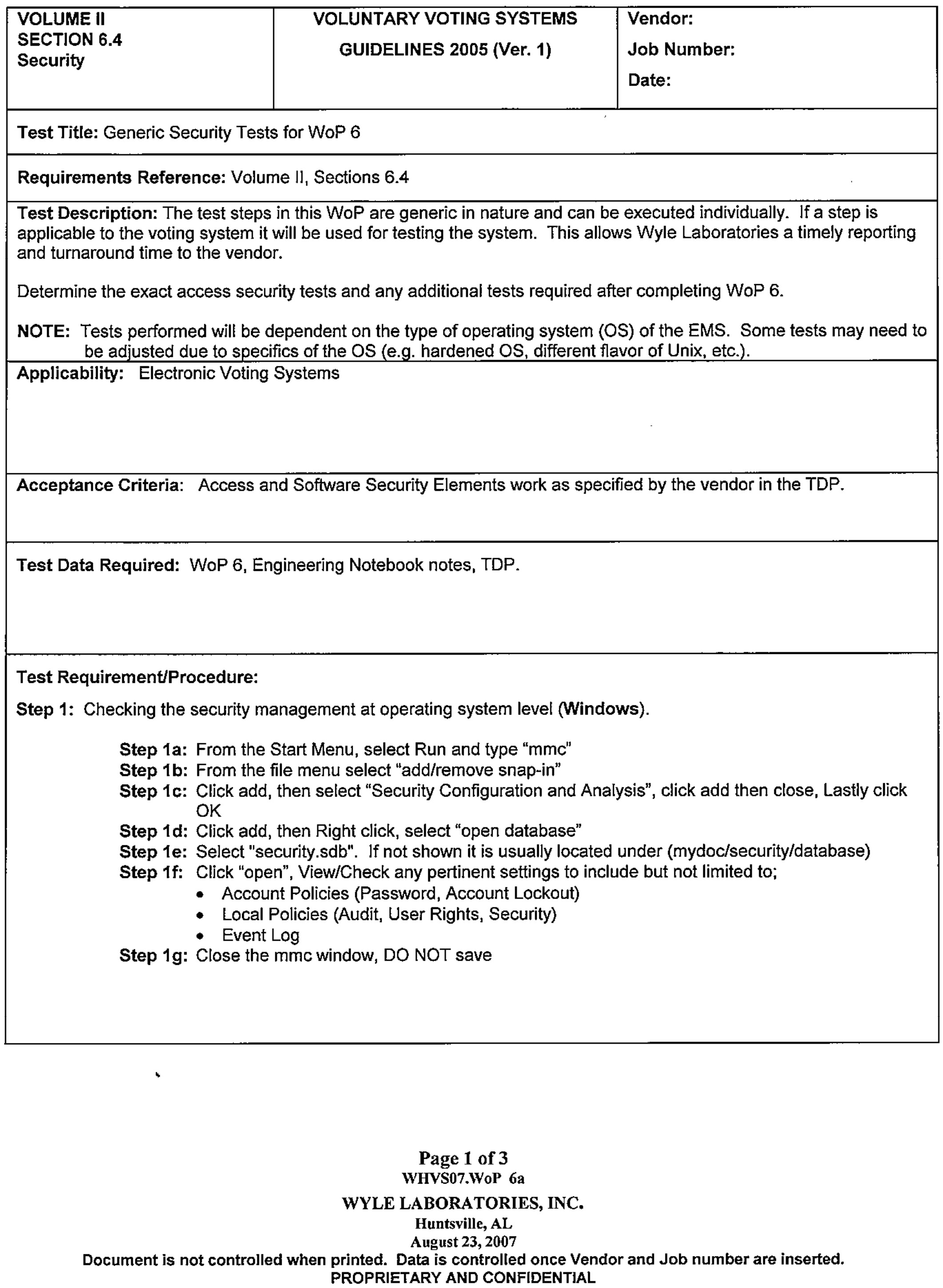
2	Protection against Malicious Software Review the vendor's TDP *(esp. Protection against malicious software)* From this review verify that the vendor has documents:		Reference the TDP section addressing this test step. ____________ ____________
	a) How the system deploys protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs.	a. P□ F□ NA□ U□	*a.* ____________
	b) The procedures to be followed to ensure that such protection is maintained in a current status.	b. P□ F□ NA□ U□	*b.* ____________
	(Indicate TDP ref. in comments column)		
3	Actual test and Verification		List any specific findings from WoP 6c.
	Conduct WoP 6c to help verify that the previous steps are indeed implemented within the voting system.	P□ F□ NA□ U□	____________ ____________

Model: S/N:	SPECIAL/MAJOR TEST SUPPORT EQUIPMENT:

ASSESSMENT/RESULTS/OBSERVATIONS/REMARKS:

PASS ____ FAIL ____ NOTICE OF ANOMALY NO. _______

Signed ______________________________ Approved ____________________________



VOLUME II SECTION 6.4 Security	VOLUNTARY VOTING SYSTEMS GUIDELINES 2005 (Ver. 1)	Vendor: Job Number: Date:

Test Title: Generic Security Tests for WoP 6

Requirements Reference: Volume II, Sections 6.4

Test Description: The test steps in this WoP are generic in nature and can be executed individually. If a step is applicable to the voting system it will be used for testing the system. This allows Wyle Laboratories a timely reporting and turnaround time to the vendor.

Determine the exact access security tests and any additional tests required after completing WoP 6.

NOTE: Tests performed will be dependent on the type of operating system (OS) of the EMS. Some tests may need to be adjusted due to specifics of the OS (e.g. hardened OS, different flavor of Unix, etc.).

Applicability: Electronic Voting Systems

Acceptance Criteria: Access and Software Security Elements work as specified by the vendor in the TDP.

Test Data Required: WoP 6, Engineering Notebook notes, TDP.

Test Requirement/Procedure:

Step 1: Checking the security management at operating system level (**Windows**).

Step 1a: From the Start Menu, select Run and type "mmc"
Step 1b: From the file menu select "add/remove snap-in"
Step 1c: Click add, then select "Security Configuration and Analysis", click add then close, Lastly click OK
Step 1d: Click add, then Right click, select "open database"
Step 1e: Select "security.sdb". If not shown it is usually located under (mydoc/security/database)
Step 1f: Click "open", View/Check any pertinent settings to include but not limited to;

- Account Policies (Password, Account Lockout)
- Local Policies (Audit, User Rights, Security)
- Event Log

Step 1g: Close the mmc window, DO NOT save

Page 1 of 3
WHVS07.WoP 6a
WYLE LABORATORIES, INC.
Huntsville, AL
August 23, 2007
Document is not controlled when printed. Data is controlled once Vendor and Job number are inserted.
PROPRIETARY AND CONFIDENTIAL

Step 2: Checking file permissions of key file and data objects (**Windows**).

NOTE: The steps listed here can be performed manually using the "cacls" command from the DOS prompt if the system does not permit the loading or running of batch files.

Step 2a: Review TDP and make list of vital files and data objects to the voting system where Integrity is a must (e.g. database, audit logs, etc.)
Step 2b: Create a text document "permchk.txt". In the document list the <u>complete</u> directory path (to include the file name) of all the objects to be checked, one per line.
Step 2c: In notepad copy the following lines:

```
@echo off
echo "test of file permissions" > permissions.txt
for /f "usebackq delims=" %%a in (permchk.txt) do (

cacls %%a >> permissions.txt

)
```

Step 2d: Save using quotes "perm.bat"
Step 2e: Load both these files onto the system (in the same directory).
Step 2f: Open the command prompt to the directory where the files are located. TYPE "perm.bat"
Step 2g: When the batch file has finished running open "permissions.txt" and check the permissions on the objects. Note any discrepancies (e.g. audit logs being editable by any user, program being executable by unprivileged user, etc.).
Step 2h: When finished permanently delete all three files from the system (perm.bat, permchk.txt, permissions.txt) using SHIFT/DELETE.

Step 3: Checking file permissions of key file and data objects (**Unix**).

NOTES: The steps listed here can be run from within a script if the system allows loading and running of shell scripts. The type of shell script used will be dependent on the build and flavor of the Unix system.
Remember if using a script; after loading it to use "chmod" command to make it executable and delete all files when finished.

Step 3a: Review TDP and make list of vital files, directories and data objects to the voting system where Integrity is a must (e.g. shadow file, database, audit logs, etc.)
Step 3b: Find all files on the system that are world writable using (without brackets);
`[ find / -perm -0002 -exec ls -l {} \; > /tmp/0002prem.txt ]`
Step 3c: Find files in /etc owned by root with read and execute permissions to the group and other users;
`[ find /etc -user root -perm 655 -exec ls -l {} \; > /tmp/655prem.txt]`
Step 3d: Find files in /etc that are owned by root and that have read and write permission set for both the group and everybody;
`[ find /etc -user root -perm 644 -exec ls -l {} \; > /tmp/644prem.txt ]`
Step 3e: Run any other find statements pertinent to the list from step 3a.
Step 3f: Change to the tmp directory and use vi or cat to view the text files and check permissions from the list in step 3a. Note any discrepancies (e.g. a protected file being world writable).

NOTE: Check to make sure sticky bit is being used properly (t-bit, s-bit). Permissions key below;

777 is rwx rwx rwx
655 is rw - r - xr - x
644 is rw - r - - r - -
400 is r - - - - - - - -

Model: S/N:	SPECIAL/MAJOR TEST SUPPORT EQUIPMENT:
ASSESSMENT/RESULTS/OBSERVATIONS/REMARKS: PASS ____ FAIL ____ NOTICE OF ANOMALY NO. ______	

Signed ______________________________ Approved ___________________________

VOLUME II **SECTION 6.4.1** **Security** **Physical**	**VOLUNTARY VOTING SYSTEMS** **GUIDELINES 2005 (VER 1)**	**Vendor:** **Job Number:** **Date:**

Test Title: Security Access Control Requirements (Physical Security)

Requirements Ref: VVSG Volume II Section 6.4.

Test Description: Wyle Laboratories will conduct tests of system capabilities and review the access control policies and procedures submitted by the vendor 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 Wyle Laboratories will design tests to confirm that these security elements work as specified.

Determine if any additional physical security tests are required after completing WoP 6.

Applicability: Electronic voting systems

Acceptance Criteria: Physical Security Elements work as specified by the vendor in the TDP. No access is allowed to internal components of the voting system and election integrity cannot be comprised.

Test Data Required: WoP 6, Engineering Notebook notes, TDP.

Test Requirement/Procedure:

Step 1: Review WoP 6 and the TDP. List all access control procedures and capabilities.
Step 2: Configure voting system as per TDP.
Step 3: Perform Operation Status Check (WoP 1). The general election will be loaded and utilized for this procedure WoP 30a Test Case GEN-01).
Step 4: Ensure the voting system operates as specified in the TDP.

Step 5: Check all access areas and ensure that seals or locks provide adequate security from gaining access to the systems internal components. P□ F□ NA□ U□

Step 6: Personnel will try and open the panels without removing the seals or locks and determine the amount of access that can be gained. (Seals and locks will be checked to ensure they are of rigid construction and not easily compromised.) P□ F□ NA□ U□

Step 7: Verify that ballot storage devices (if utilized) are secure. Personnel will try to retrieve and insert ballots without removing any seals. P□ F□ NA□ U□

Step 8: Verify that supplies that must be accessed by the poll worker (ex, paper, ink) can be changed without providing access to the ballots or internal voting system components. Personnel will open access areas for changing supplies and try and enter the ballot path area or other internal areas of the voting system. P□ F□ NA□ U□

Step 9: Verify that the ballot counter cannot be reset by any other person other than authorized persons at authorized points. Verify in the TDP where these points are. With the polls open, and prior to casting a ballot personnel will try and reset the ballot counter. P□ F□ NA□ U□

Step 10: Audio Security

- Enable audio voting and have one technician wear headphones to vote:
- Ensure that audio levels are within required range (The machine shall provide an adjustable volume control from 20 to 100 dB SPL).
- Use external microphone and audio meter or sound system as an audio listing device to determine if any sounds can be heard that are discernable outside the voting area.

P□ F□ NA□ U□

Step 11: Personnel will try and bypass or otherwise defeat the resulting security environment. These tests will include simulation of attempts to physically destroy components of the voting system in order to validate the correct operation of system redundancy and backup capabilities.

- Personnel will disable printer and ensure election results are still retrievable via electronic means.
- Personnel will disable Voter Access port and ensure that the voting systems results can still be obtained.
- Personnel will remove power from the machine and determine the effect on the voting system.

P□ F□ NA□ U□

Step 12: If there are any external I/O connections (USB, firewire, etc.) or port jacks (phone, Ethernet) uncovered during normal operation time personnel will check to see if connection is disabled. If live personnel should try and penetrate the system through that point.

P□ F□ NA□ U□

Model: **S/N:**	**SPECIAL/MAJOR TEST SUPPORT EQUIPMENT:** See Instrumentation Equipment Sheet

ASSESSMENT/RESULTS/OBSERVATIONS/REMARKS:

PASS ____ FAIL ____ NOTICE OF ANOMALY NO. _______

Signed ________________________________ Approved ____________________________

VOLUME II **SECTION 6.4** **Security** **Software**	**VOLUNTARY VOTING SYSTEMS** **GUIDELINES 2005 (VER 1)**	**Vendor:** **Job Number:** **Date:**

Test Title: Software Security Requirements

Requirements Ref: VVSG Volume II Section 6.4.

Test Description: Wyle Laboratories will conduct tests of system capabilities and review the access control policies and procedures submitted by the vendor 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 Wyle Laboratories will design tests to confirm that these security elements work as specified.

Determine if any additional physical security tests are required after completing WoP 6.

NOTE: Software security testing is incorporated in to the System Integration Testing and Source Code review. Wyle Laboratories may meet these testing requirements by confirming proper implementation of proven commercial security software. In this case, the vendor 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.

Applicability: Electronic voting systems

Acceptance Criteria: Software Security Elements work as specified by the vendor in the TDP.

Test Data Required: Engineering Notebook notes, TDP.

Test Requirement/Procedure:

Step 1: Review WoP 6 and the TDP. List all access control procedures and capabilities.
Step 2: Configure voting system as per TDP.
Step 3: Perform Operation Status Check (WoP 1). The general election will be loaded and utilized for this procedure (WoP 30a Test Case GEN-02).
Step 4: Ensure the voting system operates as specified in the TDP.

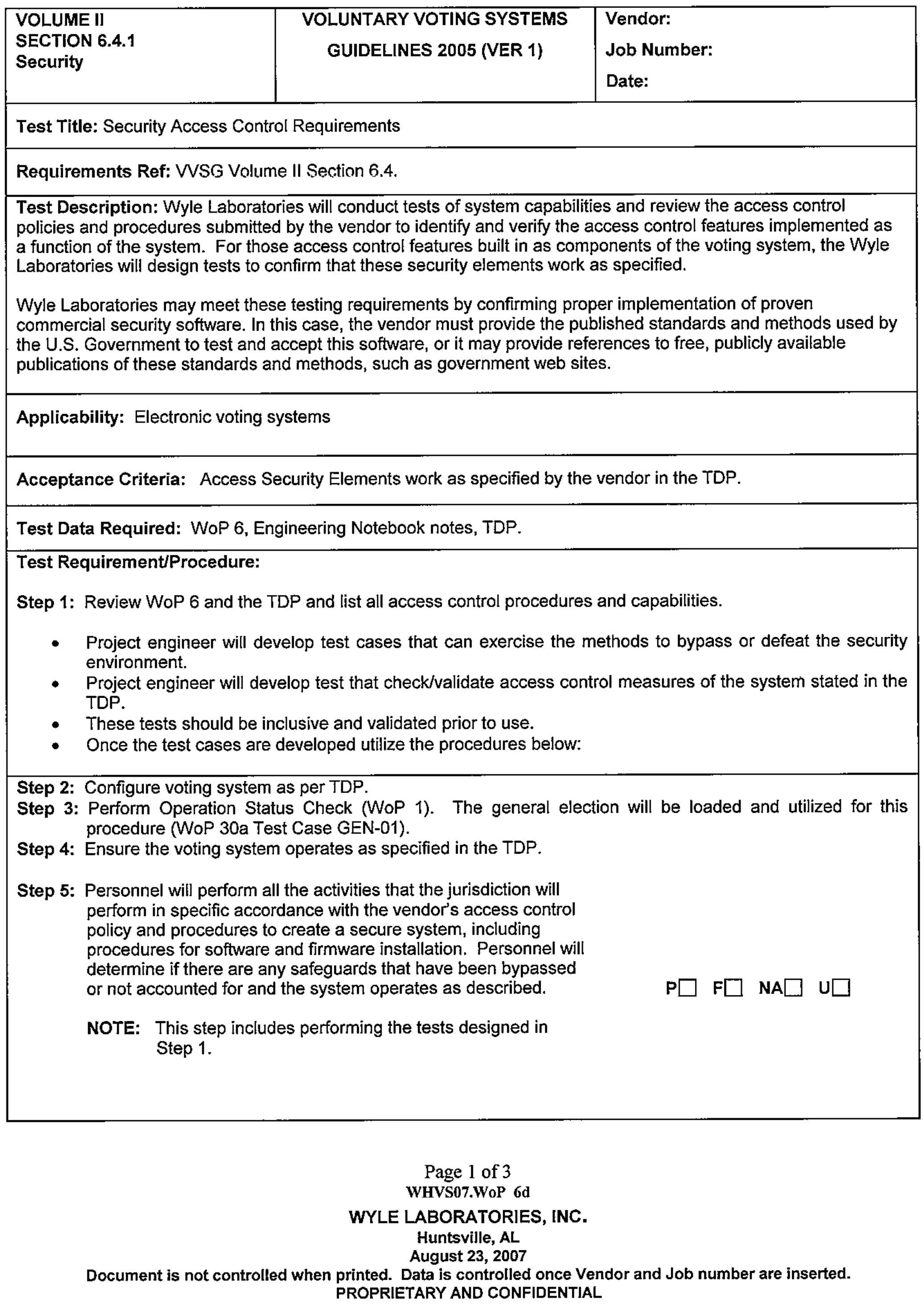
Step 4: Verify that all software and firmware installed on the EMS or hardware device is as stated in the vendor's documentation. For a PC-based system this can be accomplished by using the Windows Explorer to document what files are installed. For hardware devices this can be accomplished with the use of an eprom reader, pc card reader or other such device to check the files installed on the various types of chips installed in the hardware component. **P□ F□ NA□ U□**

Step 5: Verify that the vendor has provided a way to prevent malicious software from threatening the system. On a PC-based system this can be accomplished by the installation of a virus protection and spyware protection program. On a hardware device there can be physical limiting access devices in place to prevent an attack by locking the case. **P□ F□ NA□ U□**

Step 6: During software installation verify that the intended software has been installed. If on a PC-based system this can be accomplished by using Windows Explorer or through the DOS prompt to check that the files were installed. On a hardware device you can obtain the list of files on the hardware media through similar programs using the PC. Be sure to verify the vendor has provided a way to verify all installed software. **P□ F□ NA□ U□**

Step 7: Verify that the vendor prevents malicious software and data corruption from threatening the system. Ensure that disabling of interface and unused I/O connections are done during different modes of operation (i.e. when in voting mode no USB connection is enabled). If on a PC-based system or Kiosk also check to ensure voter cannot corrupt system (e.g. sql injection when in "write in" section of balloting).	**P**□ **F**□ **NA**□ **U**□
Model: **S/N:**	**SPECIAL/MAJOR TEST SUPPORT EQUIPMENT:** See Instrumentation Equipment Sheet
ASSESSMENT/RESULTS/OBSERVATIONS/REMARKS: **PASS** ____ **FAIL** ____ **NOTICE OF ANOMALY NO.** ______	

Signed ______________________ Approved ______________________



VOLUME II **SECTION 6.4.1** **Security**	**VOLUNTARY VOTING SYSTEMS** **GUIDELINES 2005 (VER 1)**	**Vendor:** **Job Number:** **Date:**

Test Title: Security Access Control Requirements

Requirements Ref: VVSG Volume II Section 6.4.

Test Description: Wyle Laboratories will conduct tests of system capabilities and review the access control policies and procedures submitted by the vendor 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 Wyle Laboratories will design tests to confirm that these security elements work as specified.

Wyle Laboratories may meet these testing requirements by confirming proper implementation of proven commercial security software. In this case, the vendor 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.

Applicability: Electronic voting systems

Acceptance Criteria: Access Security Elements work as specified by the vendor in the TDP.

Test Data Required: WoP 6, Engineering Notebook notes, TDP.

Test Requirement/Procedure:

Step 1: Review WoP 6 and the TDP and list all access control procedures and capabilities.

- Project engineer will develop test cases that can exercise the methods to bypass or defeat the security environment.
- Project engineer will develop test that check/validate access control measures of the system stated in the TDP.
- These tests should be inclusive and validated prior to use.
- Once the test cases are developed utilize the procedures below:

Step 2: Configure voting system as per TDP.
Step 3: Perform Operation Status Check (WoP 1). The general election will be loaded and utilized for this procedure (WoP 30a Test Case GEN-01).
Step 4: Ensure the voting system operates as specified in the TDP.

Step 5: Personnel will perform all the activities that the jurisdiction will perform in specific accordance with the vendor's access control policy and procedures to create a secure system, including procedures for software and firmware installation. Personnel will determine if there are any safeguards that have been bypassed or not accounted for and the system operates as described. **P□ F□ NA□ U□**

NOTE: This step includes performing the tests designed in Step 1.

Step 6: The assigned personnel will exercise verification of password security management at the **operating system level** for the EMS. (i.e. user permission level, administration account, guest account, password aging, password limitation, lock out on login attempts, attempt to gain access by by-passing the login requirement).

P☐ F☐ NA☐ U☐

NOTE: Perform Step 1 in WoP 6d or an appropriate test for the specific Operating System.

Step 7: The assigned personnel will exercise verification of password security management at the **application level** for EMS (i.e. password aging, password limitations, verify no hard coded passwords, lock out on login attempts, attempt to gain access by by-passing the login requirement).

P☐ F☐ NA☐ U☐

NOTES:

- Perform Step 2 or 3 in WoP 6d or an appropriate test to check the file permissions.
- Verification that no hard coded passwords should be done in WoP 5 Source Code Review.

Step 8: The assigned personnel will exercise verification of password security management at the **component level** for each precinct component (i.e. verify roles assigned to card access, verify roles assigned to user accounts, attempt to by login, attempt to locate any back door access).

P☐ F☐ NA☐ U☐

NOTE: This step includes performing the tests designed in Step 1 and checks performed in WoP 6d.

Step 9: The assigned personnel will exercise verification of **database security management** (i.e. password aging, user roles, user permissions: insert, delete, and update, database administration account, ability to access tables, views, stored procedures, indexes, and triggers outside of front end application).

P☐ F☐ NA☐ U☐

NOTE: Perform Step 2 or 3 in WoP 6d or an appropriate test to check the file permissions.

Step 10: The assigned personnel will exercise verification of **audit log management** (i.e. deletions of audit logs, modification of audit log, access to audit logs, direct altering of audit logs files or records, modification of audit file or record).

NOTE:

- Perform Step 1 in WoP 6d (if Windows OS) or an appropriate test for the specific Operating System.
- Perform Step 2 or 3 in WoP 6d or an appropriate test to check the file permissions.

P☐ F☐ NA☐ U☐

Model: S/N:	SPECIAL/MAJOR TEST SUPPORT EQUIPMENT: See Instrumentation Equipment Sheet
ASSESSMENT/RESULTS/OBSERVATIONS/REMARKS: PASS ____ FAIL ____ NOTICE OF ANOMALY NO. _______	

Signed ______________________________ Approved ____________________________