From the Vendor Trace document or declaration, identify all documents that pertain to the **System Security Specification**. Each submitted (Vol. 1, Sect. 1.1) Technical Data Package document (Vol.2 Sect. 6.6) is reviewed (Vol. 1, Sect. 1.6.2.2).

Note about revisions: The first time a review form is completed, the form revision number is 01. As the review process continues, newer versions of vendor documents, or additional documents, will be submitted to close discrepancies. Each time new versions of documents are examined, the review form is saved with a new revision number. Save the form with the new revision (Save As) before you update the document names, versions and/or file names. Enter your name and date on the new revision.

Applicable TDP Documents table: List each applicable TDP document. Put the Title from inside the document in the first column, along with the version and date. Under "File name," copy the full document file name.

Trace Table: Verify whether the vendor correctly documented each applicable VVSG requirement listed in this template. Use the following notations to indicate results:

- **Traced** column: For each positive finding, enter the document number(s) corresponding to the **Applicable TDP Documents** Table below, with the section number(s) in each applicable document where the requirement is fulfilled. (Example: Doc. 2, Sec. 1.2)
- **Comments** column:
  - **"Y"** indicates that the document(s) fulfill the requirement.
  - **"N"** indicates that the document(s) do not fulfill the requirement.
  - **"P"** indicates that the document(s) partially fulfill the requirement
  - **"NT"** (not tested) indicates documents that are part of the system configuration but outside the scope of this certification review effort (only if not a full cert).
  - **"NS"** (not supported) indicates requirements that apply to features that are not supported in the configuration being tested (such as paper ballots).
  - Explain "**P**", "**N**", "**NT**" or "**NS**" findings here.
  - In addition, use the Comments column to enter any comments that would be helpful throughout the project.
  - **Discrepancies:**
    - List discrepancies in red.
    - A Documentation discrepancy is written when a VVSG requirement is not fulfilled or is partially fulfilled in the TDP.
    - An Informational discrepancy is written when the issue is outside the scope of the certification; Informational discrepancies are provided to the client but do not preclude certification.
    - Enter the discrepancy number of any discrepancies written (from the separate discrepancy report), with a short description in the Comments column.

Vendor :	Hart InterCivic	**Reviewer(s):**	L. Hoppert, Georgia Fortun
Voting System:	AES	**Review Date:**	11/30/15, 02/08/2016

Applicable TDP Documents

Document Title (from cover pg), version, date	Doc #	File name
Verity System Description Technical Document, v B.00, 8/14/2015 - PUBLIC	#1	Verity System Description 4005466 B00
Verity Security Requirements Document, v A.07, 10/28/2015 - **Proprietary**	#2	Verity Security Requirements 4005464 A07
Verity Risk Assessment, v A.01, 6/1/2015 - **Proprietary**	#3	Verity Risk and Threat Assessment 4005513 A01

Document Title (from cover pg), version, date	Doc #	File name
Verity Key Design Technical Document, v A.00, 1/3/2014 - **Proprietary**	#4	Verity Key Design 4005514 A00
Verity Service and Maintenance Verity Voting Maintenance Information Operations Technical Reference Manual, v B01, no date - PUBLIC	#5	Verity Service and Maintenance Operations Technical Reference Manual 6610001 B01
Verity Build Election Definition and Device Settings Technical Reference Manual (DRAFT), v B01, no date - PUBLIC	#6	Verity Build Technical Reference Manual 6600002 B01
Verity Central Ballot Scanning and Review Software Technical Reference Manual (DRAFT), v B01, no date - PUBLIC	#7	Verity Central Technical Reference Manual 6600003 B01
Verity Count Vote Tabulation Software Technical Reference Manual (DRAFT), v B01, no date - PUBLIC	#8	Verity Count Technical Reference Manual 6620004 B01
Verity 1.3.0 Technical Data Package Overview, v B.00, 10/10/2015 - PUBLIC	#9	Verity 2.0 TDP Overview 4005511 B00
Verity Voting Verity Operational Environment, v B.01, 10/23/2015 - **Proprietary**	#10	Verity Operational Environment 4005515 B01
Verity Operational Guide, v B.00, no date - PUBLIC	#11	Verity Operational Guide 6640001 B00
Verity Data Ballot Design Software Technical Reference Manual, v A01, no date PUBLIC	#12	Verity Data Technical Reference Manual 6600009 A01
Verity Print Ballot on Demand Printing Technical Reference Manual, v A01 PUBLIC	#13	Verity Print Technical Reference Manual 6600007 A01
Verity Operational Guide, 6640001 Ver B01, no date	#14	Verity Operational Guide 6640001 B01.pdf
Verity Voting Verity Operational Environment, Rev. B.02, 02/03/2016	#15	Verity Operational Environment 4005515 B02.pdf

Trace Table

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
2	**Technical Data Package**		
2.1	**Scope**		
2.1.1	**Content and Format**		
2.1.1.1	**Required Content for Initial Certification** *(Indicate "*" if this document does not fall into the identified category of documentation.)*		
f.	At minimum, the TDP shall contain the following documentation: System security specifications;	Doc #1: Entire Doc Doc #2: Entire Doc	Y
2.1.1.3	**Format**		
	The requirements for formatting the TDP are general in nature; specific format details are of the vendor's	Doc #9: Entire Doc	Y

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	choosing. The TDP shall include a detailed table of contents for the required documents, an abstract of each document and a listing of each of the informational sections and appendices presented. A cross-index shall be provided indicating the portions of the documents that are responsive to documentation requirements for any item presented.		
2.1.3	**Protection of Proprietary Information**		
	The vendor shall identify all documents, or portions of documents, containing proprietary information not approved for public release. Any person or test agency receiving proprietary information shall agree to use it solely for the purpose of analyzing and testing the system, and shall agree to refrain from otherwise using the proprietary information or disclosing it to any other person or agency without the prior written consent of the vendor, unless disclosure is legally compelled.	Doc #1, 2, 3 and 4 can be clearly identified as to whether they are proprietary. Doc #9 - Entire doc	Y
2.6	**System Security Specification**		
	Vendors shall submit a system security specification that addresses the security requirements of Volume I, Section 7. This specification shall describe the level of security provided by the system in terms of the specific security risks addressed by the system, the means by which each risk is addressed, the process used to test and verify the effective operation of security capabilities and, for systems that use public telecommunications networks as defined in Volume I, Section 6, the means used to keep the security capabilities of the system current to respond to the evolving threats against these systems. Information provided by the vendor in this section of the TDP may be duplicative of information required by other sections. Vendors may cross reference to information provided in other sections provided that the means used provides a clear mapping to the requirements of this section.	See below	Y

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	Information submitted by the vendor shall be used to assist in developing and executing the system certification test plan. The Security Specification shall contain the sections identified below.		
2.6.1	**Access Control Policy**		
	The vendor shall specify the features and capabilities of the access control policy **recommended to purchasing jurisdictions** to provide effective voting system security. The access control policy shall address the general features and capabilities and individual access privileges indicated in Volume I, Subsection 7.2.	Doc #1: 2.3 User Access Management, 4.2 Security Description Doc #5: Appendix A Security Best Practices	Y
2.6.2	**Access Control Measures**		
	The vendor shall provide a detailed description of all system access control measures and mandatory procedures designed to permit access to system states in accordance with the access policy, and to prevent all other types of access to meet the specific requirements of Volume I, Subsection 7.2.	Doc #1: 2.3, 4.2 Doc #2: 3.3.3 Authentication, 3.3.4 Authorization Doc #3: entire document Doc #4: 2.1 System Introduction (Verity Key) Doc #5: Appendix A Security Best Practices	Y
	The vendor also shall define and provide a detailed description of the methods used to preclude unauthorized access to the access control capabilities of the system itself.	Doc #1: 4.2 Security Description Doc #3: entire document Doc #4: 2.1 System Introduction (Verity Key)	Y
Vol 1, 7.2.1	**General Access Control Policy**		
a.	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: Software access controls	Doc #1: 2.3, 4.2 Doc #5: Appendix A Security Best Practices Doc #6: 1, subsection Verity Build Security, 4 User Management Doc #7: 1, subsection Verity Central Security, 4 User Management Doc #8: 1, subsection Verity Count Security, 4 User Management Doc #12: 1, subsection Verity Data Security, 4	Y ~~Info DISC 13: The document "Verity Operational Guide 6640001 B00" Section 7 VOTING - VERITY POLLING PLACE EQUIPMENT, subsection Security states: "The Verity Security Requirements document provides a detailed set of requirements for Verity security." However, the referenced document is listed as Proprietary in the TDP~~

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
		User Management	~~Overview. Readers looking for security information may not have access to the referenced document~~. Discrepancy Resolved by Doc #14: Section 7 VOTING - VERITY POLLING PLACE EQUIPMENT, subsection Security, pg. 22.
b.	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: Hardware access controls	Doc #1: 2.3, 4.2 Doc #5: Appendix A Security Best Practices Doc #13: APPENDIX A Security [Print]	Y
c.	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: Communications	Doc #1: 2.3, 4.2 Doc #5: Appendix A Security Best Practices	Y
d.	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: Effective password management	Doc #1: 2.3, 4.2	Y
e.	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: Protection abilities of a particular operating system	Doc #6, 7, 8, 12 - 1, subsection Secure Environment and Operating System Doc #10: entire doc* Doc #11: 12, subsection "Generating File Listings on Verity Applications on Workstations"	Y *Doc #10 is labeled Proprietary, but it covers the security requirements of the OSs used by the system
f.	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:	Doc #1: 2.3, 4.2 Doc #5: Appendix A Security Best Practices Doc #6: 1, subsection Verity Build Security, 4 User Management	Y

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	General characteristics of supervisory access privileges	Doc #7: 1, subsection Verity Central Security, 4 User Management Doc #8: 1, subsection Verity Count Security, 4 User Management Doc #12: 1, subsection Verity Data Security, 4 User Management	
g.	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: Segregation of duties	Doc #1: 2.3, 4.2 Doc #5: Appendix A Security Best Practices	Y
h.	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: Any additional relevant characteristics	Doc #1: 2.3, 4.2 Doc #5: Appendix A Security Best Practices	Y
Vol 1, 7.2.1.1	**Individual Access Privileges**		
a.	Voting system vendors shall: Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access	Doc #1: 2.3 User Access Management, 4.2 Security Description Doc #2: 3.3.3 Authentication, 3.3.4 Authorization Doc #3: entire document Doc #4: 2.1 System Introduction (Verity Key) Doc #5: Appendix A Security Best Practices	Y
b.	Voting system vendors shall: Specify whether an individual's authorization is limited to a specific time, time interval or phase of the voting or counting operations	Doc #1: 2.3, 4.2 Doc #2: 3.3.3, 3.3.4 Doc #3: entire document Doc #4: 2.1 (Verity Key) Doc #5: Appendix A Security Best Practices	Y
c.	Voting system vendors shall:	Doc #1: 2.2 Security Overview, 2.3, 4.2 Doc #2: 3.3.3, 3.3.4	Y

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	Permit the voter to cast a ballot expeditiously, but preclude voter access to all aspects of the vote counting processes	Doc #3: entire document Doc #4: 2.1 (Verity Key) Doc #5: Appendix A Security Best Practices	
Vol 1, 7.2.1.2	**Access Control Measures**		
a.	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: Use of data and user authorization	Doc #1: 2.3 User Access Management, 4.2 Security Description Doc #2: 3.3.3 Authentication, 3.3.4 Authorization Doc #3: entire document Doc #4: 2.1 System Introduction (Verity Key) Doc #5: Appendix A Security Best Practices	Y
b.	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: Program unit ownership and other regional boundaries	Doc #1: 2.3, 4.2 Doc #2: 3.3.3, 3.3.4 Doc #3: entire document Doc #4: 2.1 (Verity Key) Doc #5: Appendix A Security Best Practices	Y
c.	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: One-end or two-end port protection devices	Doc #1: 2.3, 4.2 Doc #2: 3.3.3, 3.3.4 Doc #3: entire document Doc #4: 2.1 (Verity Key) Doc #5: Appendix A Security Best Practices	Y
d.	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: Security kernels	Doc #1: 2.3, 4.2 Doc #2: 3.3.3, 3.3.4 Doc #3: entire document Doc #4: 2.1 (Verity Key) Doc #5: Appendix A Security Best Practices	Y
e.	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:	Doc #1: 2.3, 4.2 Doc #2: 3.3.3, 3.3.4 Doc #3: entire document Doc #4: 2.1 (Verity Key)	Y

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	Computer-generated password keys	Doc #5: Appendix A Security Best Practices	
f.	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: Special protocols	Doc #1: 2.3, 4.2 Doc #2: 3.3.3, 3.3.4 Doc #3: entire document Doc #4: 2.1 (Verity Key) Doc #5: Appendix A Security Best Practices	Y
g.	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: Message encryption	Doc #1: 2.3, 4.2 Doc #2: 3.3.3, 3.3.4 Doc #3: entire document Doc #4: 2.1 (Verity Key) Doc #5: Appendix A Security Best Practices	Y
h.	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: Controlled access security	Doc #1: 2.3, 4.2 Doc #2: 3.3.3, 3.3.4 Doc #3: entire document Doc #4: 2.1 (Verity Key) Doc #5: Appendix A Security Best Practices	Y
END	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.	Doc #1: 4.2 Doc #3: entire document Doc #4: 2.1 (Verity Key)	Y
2.6.3	**Equipment and Data Security**		
	The vendor shall provide a detailed description of system capabilities and mandatory procedures for purchasing jurisdictions to prevent disruption of the voting process and corruption of voting data to meet the specific requirements of Volume I, Subsection 7.3. This information shall address measures for polling place security and central count location security.	Doc #1: 4.2 Security Description Doc #5: Appendix A Security Best Practices	Y
Vol 1, 7.3	**Physical Security Measures**		
	A voting system's sensitivity to disruption or corruption of data depends, in part, on the physical location of	Doc #1: 2.2, 2.3, 4.2.2 Doc #2: 3.1	Y

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	equipment and data media, and on the establishment of secure telecommunications among various locations. Most often, the disruption of voting and vote counting results from a physical violation of one or more areas of the system thought to be protected. Therefore, security procedures shall address physical threats and the corresponding means to defeat them.	Doc #3: entire document Doc #5: Appendix A Security Best Practices	
Vol 1, 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.	Doc #1: 2.2, 2.3, 4.1.8.2, 4.2.2 Doc #2: 3.1 Doc #3: entire document Doc #5: Appendix A Security Best Practices	Y
	The measures shall allow the immediate detection of tampering with vote casting devices and precinct ballot counters.	Doc #1: 1.3.2, 2.2.2, 4.2.2 Doc #2: 3.1	Y
	They also shall control physical access to a telecommunications link if such a link is used	NA	NA - no actual telecom, only restricted LANs
Vol 1, 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:	Doc #5: Appendix A Security Best Practices Doc #8: 1, subsection Verity Count Security	Y
	handling of ballot boxes,		
	preparing of ballots for counting,		
	counting operations and		
	reporting data.		
2.6.4	**Software Installation**		
	The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure software (including firmware) installation to meet the specific requirements of Volume I, Subsection 7.4. This	See below	Y

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	information shall address software installation for all system components.		
Vol 1, 7.4	**Software Security**		
	Voting systems shall meet specific security requirements for the installation of software and for protection against malicious software.	See below	Y
Vol 1, 7.4.1	**Software and Firmware Installation**		
a.	The system shall meet the following requirements for installation of software, including hardware with embedded firmware. 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.	Doc #2: 3.3.5 Doc #5: 3.1 Overview, Verify firmware validation under 3.4 (Touch Writer), 3.7 (Controller, Touch, Touch w/ Access), 3.10 (Scan), 3.13 (Print), 4.2 Paper-Based Elections, 4.3 Direct-Recording Elections Doc #11: 7, subsection Verify firmware validation	Y
b.	The system shall meet the following requirements for installation of software, including hardware with embedded firmware. 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.	Doc #11: 13 Security	Y
c.	The system shall meet the following requirements for installation of software, including hardware with embedded firmware. 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	Doc #1: 4.2.10 Component Security	Y

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	other than by the authorized initiation and execution of the vote counting program, and its associated exception handlers.		
d.	The system shall meet the following requirements for installation of software, including hardware with embedded firmware. 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.	Doc #10: 2.2.2.1 Secure BIOS, 2.2.2.2 CFAST storage	Y (Separate memory partitions) ~~Info DISC 14: The document "Verity Operational Environment 4005515 B01" page 14 mentions "-Verity 1.0.x applications." This should be updated to reflect Verity 2.0.x applications.~~ Discrepancy resolved by: Doc #15: pg. 14.
e.	The system shall meet the following requirements for installation of software, including hardware with embedded firmware. After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.	Workstations: Doc #10: 2.3.1 Verity Workstations (pg. 15) Voting devices: Doc #10: 2.3.12 Verity Devices (pg. 70) General: Doc #10 file manifests	Y
Vol 1, 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.	Doc #10: Entire Document	Y
Vol 1, 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.	See below	Y
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	Documentation: Doc #9, entire doc Software vendor name, product names: Doc #1, entire doc	Y (Cert app. info is public information and is tied to the voting system name/version)

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	number of the voting system, file names and paths or other location information (such as storage addresses) of the software.	File names/paths: see a.ii	
a.ii.	The documentation shall designate all software files as static, semi-static or dynamic.	Doc #10: Sections 2.3.3, 2.3.5, 2.3.7, 2.3.9, 3.1.1, 3.1.5	Y
d.ii.	The vendor shall document 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.	Doc # 6, 7, 8, 12, Chapter 2 Exporting File Hashes	Y Note: Verity Applications are installed by Hart but can be verified by customers after installation
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.	Doc #5: 3.1 Overview, Verify firmware validation under 3.4 (Touch Writer), 3.7 (Controller, Touch, Touch w/ Access), 3.10 (Scan), 3.13 (Print), 4.2 Paper-Based Elections, 4.3 Direct-Recording Elections Doc #11: 7, subsection Verify firmware validation	Y
f.	The vendors and testing labs shall document to whom they provide voting system software.	This is mentioned in the Configuration Management doc section 3.3 Design Control	Y
Vol 1, 7.4.6	**Software Setup Validation**		
a.	Setup validation methods shall verify that no unauthorized software is present on the voting equipment.	See below	Y
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.	Polling Place devices: Doc #11: 7, subsection Verify firmware validation Software: Doc #6, 7, 8, 12, Chapter 2 Exporting File Hashes	Y
b.i.	The process used to verify software should be possible to perform without using software installed on the voting system.	Doc #6, 7, 8, 12, Chapter 2 Exporting File Hashes; Doc #11: 7, subsection Verify firmware validation	Y
b.ii.	The vendor shall document the process used to verify	Doc #11: 7, subsection Verify firmware	Y

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	software on voting equipment.	validation	
b.iii.	The process shall not modify the voting system software on the voting system during the verification process.	Doc #6, 7, 8, 12, Chapter 2 Exporting File Hashes; Doc #11: 7, subsection Verify firmware validation	Y
c.	The vendor shall provide a method to comprehensively list all software files that are installed on voting systems.	Doc #6, 7, 8, 12, Chapter 2 Exporting File Hashes; Doc #11: 7, subsection Verify firmware validation	Y
d.	The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system vendor.	Doc #11: 7, subsection Verify firmware validation; 12, subsection Generating File Listings on Verity Applications on Workstations	Y
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.	Doc #6, 7, 8, 12, Chapter 1, Security section, Digital Signature	Y
d.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.	Doc #11: 7, subsection Verify firmware validation; 12, subsection Generating File Listings on Verity Applications on Workstations	Y
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.	Doc #6, 7, 8, 12, Chapter 2 Exporting File Hashes; Doc #11: 7, subsection Verify firmware validation; 12, subsection Generating File Listings on Verity Applications on Workstations	Y
e.i.	The external interface shall be protected using tamper evident techniques	Doc #11: 7, subsection Verify firmware validation; 12, subsection Generating File Listings on Verity Applications on Workstations	Y
e.ii.	The external interface shall have a physical indicator showing when the interface is enabled and disabled	Doc #11: 7, subsection Verify firmware validation; 12, subsection Generating File Listings on Verity Applications on Workstations	Y
e.iii.	The external interface shall be disabled during voting	Doc #11: 7, subsection Verify firmware	Y

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
		validation; 12, subsection Generating File Listings on Verity Applications on Workstations	
e.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	Doc #11: 7, subsection Verify firmware validation; 12, subsection Generating File Listings on Verity Applications on Workstations	Y
f.	Setup validation methods shall verify that registers and variables of the voting system equipment contain the proper static and initial values.	Doc #10: 3 Verity Datastore Environments	Y
f.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.	Doc #10: 3 Verity Datastore Environments	Y
f.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.	Doc #10: 3 Verity Datastore Environments	Y
2.6.5	**Telecommunications & Data Transmission Security**		
	The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure data transmission to meet the specific requirements of Volume I, Subsection 7.5:		NS
a.	For all systems, this information shall address access control, and prevention of data interception;		NS
b.	For systems that use public communications networks as defined in Volume I Section 6, this information shall also include: i. Capabilities used to provide protection against threats to third party products and services; ii. Policies and processes used by the vendor to ensure that such protection is updated to remain		NS

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	effective over time; iii. Policies and procedures used by the vendor to ensure that current versions of such capabilities are distributed to user jurisdictions and are installed effectively by the jurisdiction; iv. A detailed description of the system capabilities and procedures to be employed by the jurisdiction to diagnose the occurrence of a denial of service attack, to use an alternate method of voting, to determine when it is appropriate to resume voting over the network, and to consolidate votes cast using the alternate method; v. A detailed description of all activities to be performed in setting up the system for operation that are mandatory to ensure effective system security, including testing of security before an election; and vi. A detailed description of all activities that should be prohibited during system setup and during the timeframe for voting operations, including both the hours when polls are open and when polls are closed.		
Vol 1, 7.5	**Telecommunications and Data Transmission**		
	There are four areas that must be addressed by telecommunications and data transmission security capabilities: access control, data integrity, detection and prevention of data interception, and protection against external threats.		NS
Vol 1, 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		NS

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	function.		
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.		NS
	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.		NS
b.	Voting systems that use telecommunications to communicate between system components and locations before the polling place is officially closed shall:		NS
b.i.	Implement an encryption standard currently documented and validated for use by an agency of the U.S. government		NS
b.ii.	Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System		NS
Vol 1, 7.5.2	**Protection Against External Threats**		
a.	Voting systems that use public telecommunications networks shall implement protections against external threats to which commercial products used in the system may be susceptible.		NS
b.	Voting systems that use public telecommunications networks shall provide system documentation that clearly identifies all COTS hardware and software products and communications services used in the development and/or operation of the voting system, including operating systems, communications routers, modem drivers and dial-up networking software.		NS
b.i.	Such documentation shall identify the name, vendor, and version used for each such component.		NS
c.	Voting systems that use public telecommunications networks shall use protective software at the receiving-		NS

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	end of all communications paths to:		
c.i.	Detect the presence of a threat in a transmission		NS
c.ii.	Remove the threat from infected files/data		NS
c.iii.	Prevent against storage of the threat anywhere on the receiving device		NS
c.iv.	Provide the capability to confirm that no threats are stored in system memory and in connected storage media		NS
c.v.	Provide data to the system audit log indicating the detection of a threat and the processing performed		NS
d.	Vendors shall use multiple forms of protective software as needed to provide capabilities for the full range of products used by the voting system.		NS
Vol 1, 7.5.3	**Monitoring and Responding to External Threats**		
a.	Voting systems that use public telecommunications networks may become vulnerable, by virtue of their system components, to external threats to the accuracy and integrity of vote recording, vote counting, and vote consolidation and reporting processes. Therefore, vendors of such systems shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to: Monitor threats, such as through the review of assessments, advisories, and alerts for COTS components issued by the Computer Emergency Response Team (CERT), for which a current listing can be found at http://www.cert.org, the National Infrastructure Protection Center (NIPC), and the Federal Computer Incident Response Capability (FedCIRC), for which additional information can be found at www.uscert.gov		NS

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
b.	Voting systems that use public telecommunications networks may become vulnerable, by virtue of their system components, to external threats to the accuracy and integrity of vote recording, vote counting, and vote consolidation and reporting processes. Therefore, vendors of such systems shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to: Evaluate the threats and, if any, proposed responses		NS
c.	Voting systems that use public telecommunications networks may become vulnerable, by virtue of their system components, to external threats to the accuracy and integrity of vote recording, vote counting, and vote consolidation and reporting processes. Therefore, vendors of such systems shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to: Develop responsive updates to the system and/or corrective procedures		NS
d.	Voting systems that use public telecommunications networks may become vulnerable, by virtue of their system components, to external threats to the accuracy and integrity of vote recording, vote counting, and vote consolidation and reporting processes. Therefore, vendors of such systems shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to:		NS

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	Submit the proposed response to the test labs and appropriate states for approval, identifying the exact changes and whether or not they are temporary or permanent		
e.	Voting systems that use public telecommunications networks may become vulnerable, by virtue of their system components, to external threats to the accuracy and integrity of vote recording, vote counting, and vote consolidation and reporting processes. Therefore, vendors of such systems shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to: After implementation of the proposed response is approved by the state, assist clients, either directly or through detailed written procedures, how to update their systems and/or to implement the corrective procedures within the timeframe established by the state		NS
f.	Voting systems that use public telecommunications networks may become vulnerable, by virtue of their system components, to external threats to the accuracy and integrity of vote recording, vote counting, and vote consolidation and reporting processes. Therefore, vendors of such systems shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to: Address threats emerging too late to correct the system by:		NS
f.i.	Providing prompt, emergency notification to the accredited test labs and the affected states and user jurisdictions		NS

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
f.ii.	Assisting client jurisdictions directly or advising them through detailed written procedures to disable the public telecommunications mode of the system		NS
f.iii.	Modifying the system after the election to address the threat, submitting the modified system to an accredited test lab and the EAC or state certification authority for approval, and assisting client jurisdictions directly or advising them through detailed written procedures, to update their systems and/or to implement the corrective procedures after approval		NS
Vol 1, 7.5.4	**Shared Operating Environment**		
	Ballot recording and vote counting can be performed in either a dedicated or non-dedicated environment. If ballot recording and vote counting operations are performed in an environment that is shared with other data processing functions, both hardware and software features shall be present to protect the integrity of vote counting and of vote data.		NS
a.	Systems that use a shared operating environment shall: Use security procedures and logging records to control access to system functions		NS
b.	Systems that use a shared operating environment shall: Partition or compartmentalize voting system functions from other concurrent functions at least logically, and preferably physically as well		NS
c.	Systems that use a shared operating environment shall: Control system access by means of passwords, and restrict account access to necessary functions only		NS
d.	Systems that use a shared operating environment shall: Have capabilities in place to control the flow of information, precluding data leakage through shared		NS

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	system resources		
Vol 1, 7.5.5	**Incomplete Election Returns**		
a.	If the voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, the system shall: 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		NS
b.	If the voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, the system shall: 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:		NS
b.i.	The output file or database has no provision for write access back to the system		NS
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		NS
2.6.6	**Other Elements of an Effective Security Program**		
	The vendor shall provide a detailed description of additional procedures required for use by the purchasing jurisdiction; including:	See below	Y
a.	Administrative and management controls for the voting system and election management, including access	Doc #1: 2.3 User Access Management, 4.2	Y

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	controls;	Security Description Doc #5: Appendix A Security Best Practices Doc #11: 13. Security	
b.	Internal security procedures, including operating procedures for maintaining the security of the software for each system function and operating mode;	Doc #1: 2.3, 4.2 Doc #5: Appendix A Security Best Practices Doc #11: 13. Security	Y
c.	Adherence to, and enforcement of, operational procedures (e.g., effective password management);	Doc #1: 2.3, 4.2 Doc #5: Appendix A Security Best Practices Doc #11: 13. Security	Y
d.	Physical facilities and arrangements;	Doc #5: Appendix A Security Best Practices Doc #11: 13. Security	Y
e.	Organizational responsibilities and personnel screening.	Doc #11: Entire doc	Y
END	This documentation shall be prepared such that these requirements can be integrated by the jurisdiction into local administrative and operating procedures.	Doc #1: 2.3, 4.2 Doc #5: Appendix A Security Best Practices Doc #11: Entire doc	Y
Vol 1, 7.6.2.1	**Documentation of Mandatory Security Activities**		
a.	Vendors of voting systems that cast individual ballots over a public telecommunications network shall provide detailed descriptions of: All activities mandatory to ensuring effective voting system security to be performed in setting up the system for operation, including testing of security before an election		NS
b.	Vendors of voting systems that cast individual ballots over a public telecommunications network shall provide detailed descriptions of: All activities that should be prohibited during voting equipment setup and during the timeframe for voting operations, including both the hours when polls are open and when polls are closed		NS
Vol 1,	**Wireless Communications**		

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
7.7			
Vol 1, 7.7.1	**Controlling Usage**		
a.	If wireless communications are used in a voting system, then the vendor shall supply documentation describing how to use all aspects of wireless communications in a secure manner. This documentation shall include:		NS
a.i.	A complete description of the uses of wireless in the voting system including descriptions of the data elements and signals that are to be carried by the wireless mechanism		NS
a.ii.	A complete description of the vulnerabilities associated with this proposed use of wireless, including vulnerabilities deriving from the insertion, deletion, modification, capture or suppression of wireless messages		NS
a.iii.	A complete description of the techniques used to mitigate the risks associated with the described vulnerabilities including techniques used by the vendor to ensure that wireless cannot send or receive messages other than those situations specified in the documentation. Cryptographic techniques shall be carefully and fully described, including a description of cryptographic key generation, management, use, certification, and destruction		NS
a.iv.	A rationale for the inclusion of wireless in the proposed voting system, based on a careful and complete description of the perceived advantages and disadvantages of using wireless for the documented uses compared to using non-wireless approaches		NS
b.	The details of all cryptographic protocols used for wireless communications, including the specific features and data, shall be documented.		NS
c.	The wireless documentation shall be closely reviewed for accuracy, completeness, and correctness.		NS
d.	There shall be no undocumented use of the wireless		NS

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	capability, nor any use of the wireless capability that is not entirely controlled by an election official.		
e.	If a voting system includes wireless capabilities, then the voting system shall be able to accomplish the same function if wireless capabilities are not available due to an error or no service. i. The vendor shall provide documentation how to accomplish these functions when wireless is not available.		NS
f.	The system shall be designed and configured so it is not vulnerable to a single point of failure using wireless communications that causes a total loss of any voting capabilities.		NS
g.	If a voting system includes wireless capabilities, then the system shall have the ability to turn on the wireless capability when it is to be used and to turn off the wireless capability when the wireless capability is not in use.		NS
h.	If a voting system includes wireless capabilities, then the system shall not activate the wireless capabilities without confirmation from an elections official.		NS
Vol 1, 7.7.2	**Identifying Usage**		
a.	If a voting system provides wireless communications capabilities, then there shall be a method for determining the existence of the wireless communications capabilities.		NS
b.	If a voting system provides wireless communications capabilities, then there shall be an indication that allows one to determine when the wireless communications (such as radio frequencies) capability is active.		NS
c.	The indication shall be visual.		NS
d.	If a voting system provides wireless communications capabilities, then the type of wireless communications used (such as radio frequencies) shall be identified either via a label or via the voting system documentation.		NS

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
Vol 1, 7.7.3	**Protecting Transmitted Data**		
	The transmitted data, especially via wireless communications, needs to be protected to ensure confidentiality and integrity. Examples of election information that needs to be protected include: ballot definitions, voting device counts, precinct counts, opening of poll signal, and closing of poll signal. Examples of other information that needs to be protected include: protocol messages, address or device identification information, and passwords. Since radio frequency wireless signals radiate in all directions and pass through most construction material, anyone may easily receive the wireless signals. In contrast, infrared signals are line of sight and do not pass through most construction material. However, infrared signals can still be received by other devices that are in the line of sight. Similarly, wireless signals can be transmitted by others to create unwanted signals. Thus, encryption is required to protect the privacy and confidentiality of the voting information.		NS
a.	All information transmitted via wireless communications shall be encrypted and authenticated--with the exception of wireless T-coil coupling--to protect against eavesdropping and data manipulation including modification, insertion, and deletion.		NS
a.i.	The encryption shall be as defined in Federal Information Processing Standards (FIPS) 197, “Advanced Encryption Standard (AES).”		NS
a.ii.	The cryptographic modules used shall comply with FIPS 140-2, Security Requirements for Cryptographic Modules.		NS
b.	The capability to transmit non-encrypted and non-authenticated information via wireless communications shall not exist.		NS
c.	If audible wireless communication is used, and the		NS

Req #	VVSG 2005 Testing Standards - Vol.2 unless otherwise specified	Traced	Comments
	receiver of the wireless transmission is the human ear, then the information shall not be encrypted.		

End of Document