VVSG 2007 Setup Inspection Requirements

This information is based on the requirements found at:
http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/2007-VVSG.pdf

5.2 Setup Inspection

This section provides requirements supporting the capability to verify properties of voting devices to help with the management and maintenance of voting devices during the election process. The requirements support the inspection of a voting device to determine that: (a) software installed on the voting device can be identified and verified; (b) the contents of the voting device's registers and variables can be determined; and (c) components of the voting device (such as touch screens, batteries, power supplies, etc.) are within proper tolerances, functioning properly, and ready for use. The requirements found in this section are derived from requirements found in commercial and federal standards such as Voluntary Voting System Guidelines 2005 [VVSG2005] and IEEE P1583 Draft Standard for the Evaluation of Voting Equipment [P1583].

5.2.1 Voting device software inspection

The requirements found in this section provide the ability to identify and verify voting system software installed on programmed devices of the voting system.

Programmed devices can be inspected to locate and identify the software stored on the device. Programmed devices that store software on devices with a file system can use directory paths and filenames to locate and identify software. When programmed devices store software on devices without file systems, a device's storage locations (such as memory addresses) can be used to locate the software. However, other information (such as byte strings) may be needed to identify software residing in the storage locations of the device.

The integrity of software installed on programmed devices can be inspected to determine if software has been modified. Software verification techniques use software reference information (such as digital signatures) to determine if the software has been modified. Although software validation techniques can detect modifications, they cannot determine the reason a modification to the software occurs – malicious intent or accidental error. Software reference information (such as digital signatures) from the test lab, National Software Reference Library (NSRL), or other notary repositories can be used to determine if software has been modified.

5.2.1.1 Software identification verification

5.2.1.1-A Voting device software identification

Requirement:	The voting device SHALL be able to identify all software installed on programmed devices of the voting device.

Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Software stored on programmed devices with file systems can use directory paths and filenames to locate and identify software. When software is stored on programmed devices without file systems, a device’s storage locations (such as memory addresses) can be used to locate the software. However, other information (such as byte strings) may be needed to identify software residing in the storage locations of the programmed device. This requirement generalizes [VVSG2005] I.7.4.6-c by not assuming that the software being identified is stored in a device with a file system.
Source:	[VVSG2005] I.7.4.6 (c)
Principle(s)/ Guideline(s):	*Security: Software Integrity* *Only software that is digitally signed by the appropriate authorities is installed on the voting system.* **Justification:** Although not intended for this requirement, a requirement for only executing signed software would meet this goal.

5.2.1.1-B Voting device, software identification verification log

Requirement:	Voting devices SHALL be capable of a software identification verification inspection that records, minimally, the following information to the device’s event log: a. Time and date of the inspection; b. Information that uniquely identifies the software (such as software name, version, build number, etc.); c. Information that identifies the location (such as full path name or memory address); and d. Information that uniquely identifies the programmed device that was inspected.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005] I.5.4.2
Principle(s)/ Guideline(s):	*Security: Detection/Monitoring* *Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.* **Justification:**

5.2.1.1-B.1 EMS, software identification verification log

Requirement:	EMSs and other programmed devices that identify and authenticate individuals also SHALL record identifying information of the individual and role that performed the inspection.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005] I.5.4.2

Principle(s)/ Guideline(s):	*Security: Access Control* *The voting system identifies users, roles and/or processes to which access is granted and the specific functions and data to which each entity holds authorized access.* Justification: This access control guideline mentions identification and authentication of individuals. A requirement can later be devised to specifically call out individuals performing inspection if needed.

5.2.1.2 Software integrity verification

5.2.1.2-A Software integrity verification

Requirement:	The voting device SHALL verify the integrity of software installed on programmed devices using cryptographic software reference information from the National Software Reference Library (NSRL), voting device owner, or designated notary repositories.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Cryptographic software reference information includes digital signatures and hash values. Notary repositories use software they receive to generate software integrity information (such as digital signatures or hash values) which can be used to verify the integrity of the piece of software. Notary repositories distribute software integrity information but they do not distribute the voting software or the software used to generate the software integrity information. This requirement updates [VVSG2005] I.7.4.6-b by creating a stand-alone requirement to verify that software installed on programmed devices of the voting device has not been modified.
Source:	[VVSG2005] I.7.4.6 (b)
Principle(s)/ Guideline(s):	

NIST Team Suggests Removal

5.2.1.2-B Voting device, software integrity verification log

Requirement:	Voting devices shall be capable of performing a software integrity verification inspection that records, minimally, the following information to the device’s event log: a. Time and date of the inspection; b. Information that uniquely identifies the software (such as software name, version, build number, etc.); c. Information that identifies the software integrity verification technique used; d. Results of the software verification, including the cryptographic software reference information used for the verification; and **e.** Information that uniquely identifies the voting device that contained the software that was verified.
Applies to:	Voting device

Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005] I.5.4.2
Principle(s)/ Guideline(s):	

NIST Team Suggests Removal

5.2.1.2-B.1 EMS, software integrity verification log

Requirement:	EMSs and other programmed devices that identify and authenticate individuals also shall record identifying information of the individual and role that performed the inspection.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005] I.5.4.2
Principle(s)/ Guideline(s):	

NIST Team Suggests Removal as this is a repeated requirement with 5.2.1.1-B.1

5.2.2 Voting device election information inspection

The requirements found in this section provide the ability to inspect contents of storage locations that hold election information for a voting device.

Voting devices can be inspected to determine the content for storage locations that hold election information. Storage locations can hold election information that changes, such as accumulation registers, or information that does not change during an election. The proper initial and constant values of storage locations use to hold election information can be determined from documentation provided by manufacturers and jurisdictions before a voting device is used during an election.

5.2.2-A Election information value determination

Requirement:	The voting device SHALL be able to determine the values contained in storage locations used to hold election information that changes during the election such as the number of ballots cast or total for a given contest.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement restates [VVSG2005] I.7.4.6-f with some word changes.
Source:	[VVSG2005] I.7.4.6 (f), I.2.2.5 (e), I.2.2.6 (b)
Principle(s)/ Guideline(s):	Security: Data Protection *The voting system protects sensitive data from unauthorized access, modification, or deletion.* **Justification:** The data protection guideline ensures that the election storage protections are only altered when properly accessed.

5.2.3 Voting equipment properties inspection

In addition to the inspection of the software, registers, and variables, other properties can be inspected to determine if a voting device is ready. These other properties that can be inspected include: (a) the connections of the cables (network, power, etc.); (b) the calibration and function of input and output interfaces such as touch screens; (c) the current level of consumables (paper, ink, battery, etc.); and (d) the state of physical mechanisms (such as locks, tamper evident tape, enclosure panels, etc.) used to protect input and output interfaces. In addition, a voting device can perform tests to exercise the functionality of voting equipment components to determine if the components are malfunctioning or misconfigured.

5.2.3-A Backup power source charge indicator

Requirement:	The voting device SHALL indicate the remaining charge of backup power sources in quarterly increments (i.e. full, three-quarters full, half-full, quarter full, empty) at a minimum without the use of software.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Backup power sources for voting equipment include but are not limited to batteries.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	General: High-Quality Construction *Handle errors actively and appropriately, recovering from failure gracefully – processing or avoiding well-known errors and/or software bugs; and avoiding single points of failure that could cause complete loss of voting capabilities* **Justification:** Ensuring that election officials know the battery status of a unit prevents failures from occurring.

5.2.3-B Cabling connectivity indicator

Requirement:	The voting device SHALL indicate the connectivity of cabling attached to the voting device without the use of software.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	For example, LEDs can be used to indicate when power cables are connected and conducting electricity. LEDs can also be used to indicate when network cables are connected and can transmit information.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	General: High-Quality Construction *Use trustworthy materials, methods, standards, and best practices – including accepted and appropriate tools/standards for constructing hardware and software, protocols for constructing and performing telecommunications, as well as best practices for quality assurance and configuration management* **Justification:** Best practices and configuration management helps to ensure this requirement is met.

5.2.3-C Communications operational status indicator

Requirement:	The voting device SHALL indicate the operational status of the communications capability of the voting device.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	VVSG 2007
Principle(s)/ Guideline(s):	General: High-Quality Construction *Use trustworthy materials, methods, standards, and best practices – including accepted and appropriate tools/standards for constructing hardware and software, protocols for constructing and performing telecommunications, as well as best practices for quality assurance and configuration management* *Security: Detection/Monitoring* *Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.* **Justification:** The operational status of the communications capability is the important activity recorded in this requirement.

5.2.3-D Communications on/off indicator

Requirement:	The voting device SHALL indicate when the communications capability of the voting device is on/off without the use of software.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	For example, LEDs can be used to indicate when a given device is on or off. Physical switches can be used to physically turn on or off devices.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	General: High-Quality Construction *Use trustworthy materials, methods, standards, and best practices – including accepted and appropriate tools/standards for constructing hardware and software, protocols for constructing and performing telecommunications, as well as best practices for quality assurance and configuration management* *Security: Detection/Monitoring* *Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.* **Justification:** The operational status of the communications capability is the important activity recorded in this requirement.

5.2.3-E Consumables remaining indicator

Requirement:	The voting device SHALL indicate the remaining amount of voting device consumables (i.e. ink, paper, etc.) in quarterly increments (i.e. full, three-quarters full, half-full, quarter full, empty) at a minimum.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	

Source:	VVSG 2007
Principle(s)/ Guideline(s):	

5.2.3-F Calibration determination of voting device components

Requirement:	The voting device SHALL be able to determine the calibration of voting device components that require calibration.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Examples of voting device components that may require calibration are touch screens and optical scan sensors.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	

5.2.3-G Calibration of voting device components adjustment

Requirement:	The voting device SHALL be able adjust the calibration of voting device components that require calibration.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	VVSG 2007
Principle(s)/ Guideline(s):	

Note: These requirements do not follow the numbering scheme.

5.2.1.2-H Voting device, property inspection log

Requirement:	Voting devices shall be capable of performing a device properties inspection that records, minimally, the following information to the device’s event log: a. Time and date of the inspection; b. A description of the inspections performed; c. Results of each inspection; and d. Information that uniquely identifies the voting device that was inspected.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005] I.5.4.2
Principle(s)/ Guideline(s):	*Security: Detection/Monitoring* *Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.* **Justification:** The requirement directly aligns with this guideline.

5.2.1.2-H.1 EMS, property inspection log

Requirement:	EMSs and other programmed devices that identify and authenticate individuals also shall record identifying information of the individual and role that performed the inspection.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005] I.5.4.2
Principle(s)/ Guideline(s):	*Security: Detection/Monitoring* *Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.* **Justification:** The requirement directly aligns with this guideline.

NIST Team Suggests Removal as this is a repeated requirement with 5.2.1.1-B.1