VVSG 2007 Software Installation Requirements

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

5.3 Software Installation

The following requirements support the installation of voting system software on programmed devices of the voting system. The requirements support the authentication and integrity of voting system software using digital signatures provided by test labs, National Software Reference Library (NSRL), and notary repositories. Notary repositories distribute software integrity information (such as digital signatures and hash values) they generate. However, notary repositories do not distribute the voting software they receive or the software used to generate the software integrity information.

5.3-A Software installation state restriction

Requirement:	Vote-capture devices SHALL only allow software to be installed while in the pre-voting state.
Applies to:	Vote-capture device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	See Part 1:8.2 “Vote-Capture Device State Model (informative)” for modes specified for vote-capture devices.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Software Integrity* *Voting systems prevent the unauthorized installation or modification of firmware, software, and critical configuration files.* **Justification:** This requirement mapped best to the Software Integrity principle itself.

5.3-B Authentication to install software

Requirement:	Programmed devices SHALL allow only authenticated administrators to install software on voting equipment.
Applies to:	Programmed device
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	This requirement mandates that, for all programmed devices, authentication of an administrator must be performed for allowing software to be installed.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Access Control* *The voting system authenticates administrators, users, devices and services before granting access to sensitive functions.* **Justification:** This requirement best mapped to the Access control principle.

5.3-B.1 Authentication to install software on EMS

Requirement:	The EMS shall uniquely authenticate individuals associated with the administrator role before allowing software to be installed on the voting equipment.
Applies to:	EMS
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”

Discussion:	The EMS must authenticate the individual administrator, e.g., the administrator's user account name.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Access Control* *The voting system authenticates administrators, users, devices and services before granting access to sensitive functions.* **Justification:** This requirement best mapped to the Access control principle.

5.3-C Authentication to install software election-specific software

Requirement:	Programmed devices SHALL only allow authenticated central election officials to install election-specific software and data files on voting equipment.
Applies to:	Programmed device
Test Reference:	Part 3:4.5 "Source Code Review", 5.2 "Functional Testing"
Discussion:	This requirement strengthens the base authentication required for software installation by requiring additional authentication to perform updates to election-specific software by the central election official role.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Access Control* *The voting system authenticates administrators, users, devices and services before granting access to sensitive functions.* **Justification:** This requirement mapped well to the Access control principle.

5.3-C.1 Authentication to install software election-specific software on EMS

Requirement:	The EMS shall uniquely authenticate individuals associated with the central election official role before allowing election-specific software and data files to be installed on the voting equipment.
Applies to:	EMS
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This requirement strengthens the base authentication required for software installation by requiring additional individual authentication for election-specific software installation by the central election official role.
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Access Control* *The voting system authenticates administrators, users, devices and services before granting access to sensitive functions.* **Justification:** This requirement best mapped to the Access control principle.

5.3-D Software installation procedures usage documentation

Requirement:	Software on programmed devices of the voting system SHALL only be able to be installed using the procedures in the user documentation.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Requirement part2:4.3.3-F requires manufacturers to document the procedures used to install software on programmed devices of the voting system.
Source:	VVSG 2007

Principle(s)/ Guideline(s):	*Security: Software Integrity* *Voting systems prevent the unauthorized installation or modification of firmware, software, and critical configuration files.* **Justification:** This requirement mapped best to the Software Integrity principle itself. We may need a guideline to map better.

5.3-E Software digital signature verification

Requirement:	A test lab, National Software Reference Library (NSRL), or notary repository digital signature associated with the software SHALL be successfully validated before placing the software on programmed devices of voting systems.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This requirement checks that software is an unaltered version of the software traceable back to a test lab, National Software Reference Library (NSRL), or notary repository. Notary repositories such as the NSRL 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 modifies [VVSG2005] 7.4.6-b, which requires manufacturers to have a process to verify software using reference information from the NSRL or from a state designated repository. This requirement instead requires that software must be validated using information from the NSRL prior to installation on the voting device.
Source:	[VVSG2005] I.7.4.6-b
Principle(s)/ Guideline(s):	

5.3-E.2 Software digital signature verification record

Requirement:	The results of digital signature verifications including who generated the signature SHALL be part of the software installation record.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing" as part of Requirement Part 1:5.3-G
Discussion:	
Source:	VVSG 2007
Principle(s)/ Guideline(s):	Security: Auditability Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. **Justification:** The record provided by this requirement provides verification of the digital signature.

5.3-F Software installation error alert media

Requirement:	When installation of software fails, software installation programs SHALL provide an externally visible error message identifying the software that has failed to be installed on programmed devices of the voting system.

Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	VVSG 2007
Principle(s)/ Guideline(s):	Security: Detection/Monitoring The voting system generates, stores, and reports to the user or election official, all error messages as they occur. **Justification:** This requirement aligns with this guideline.

Note: (Strange Numbering Scheme) Requirements in this section seem to be from outside of this section: 5.2.1.2-G & 5.2.1.2-G.1.

5.2.1.2-G Programmed device, software installation logging

Requirement:	Programmed devices shall be able to log, minimally, the following information associated with each piece of software installed to the device’s event log: a. The date and time of the installation; b. The software’s filename and version; c. The location where the software is installed (such as directory path or memory addresses); d. If the software was installed successfully or not; and **e.** The digital signature validation results including who generated the signature.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	VVSG 2007
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 minimal information recorded in this requirement may be considered “important activities” recorded through event logging.

5.2.1.2-G.1 EMS, vote equipment property inspection log

Requirement:	EMSs and other programmed devices that identify and authenticate individuals also shall record identifying information of the individual and role performing the software installation.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	VVSG 2007
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 requirement aligns with this guideline.

5.3-H Authentication to access configuration file

Requirement:	Programmed devices SHALL allow only authenticated administrators to access and modify voting device configuration file(s).
Applies to:	Programmed device
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Access Control* *The voting system authenticates administrators, users, devices and services before granting access to sensitive functions.* **Justification:** This requirement aligns with the Access control principle itself.

5.3-H.1 Authentication to access configuration file on EMS

Requirement:	The EMS shall uniquely authenticate individuals associated with the administrator role before allowing them to access and modify voting device configuration files.
Applies to:	EMS
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Access Control* *The voting system authenticates administrators, users, devices and services before granting access to sensitive functions.* **Justification:** This requirement aligns with the Access control principle itself.

5.3-I Authentication to access election–specific configuration file

Requirement:	Programmed device SHALL allow authenticated only central election officials to access and modify election specific configuration files.
Applies to:	Programmed device
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	
Source:	VVSG 2007
Principle(s)/ Guideline(s):	*Security: Access Control* *The voting system authenticates administrators, users, devices and services before granting access to sensitive functions.* **Justification:** This requirement aligns with the Access control principle itself.

5.3-I.1 Authentication to access election–specific configuration file on EMS

Requirement:	The EMS SHALL uniquely authenticate individuals associated with the central election official role before allowing them to access and modify voting device configuration files.
Applies to:	EMS
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	
Source:	VVSG 2007

Principle(s)/ Guideline(s):	*Security: Access Control* *The voting system authenticates administrators, users, devices and services before granting access to sensitive functions.* **Justification:** This requirement aligns with the Access control principle itself.

Note: (Strange Numbering Scheme) Requirements in this section seem to be from outside of this section: 5.2.1.2-J & 5.2.1.2-J.1.

5.2.1.2-J Programmed device, configuration file access logging

Requirement:	Programmed devices shall be able to log, minimally, the following information associated with configuration file accesses: a. The date and time of the access; b. The configuration file's filename; c. An indication of the configuration file was modified; and **d.** The location of the configuration file (such as directory path or memory addresses).
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	
Source:	VVSG 2007
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 minimal information recorded in this requirement may be considered "important activities" recorded through event logging.

5.2.1.2-J.1 EMS, configuration file access logging

Requirement:	EMSs and other programmed devices that identify and authenticate individuals also shall record identifying information of the individual and role accessing the configuration file.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	
Source:	VVSG 2007
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 requirement aligns with this guideline.