Software Installation Requirements Gap Analysis

An overarching goal of the next VVSG is to have each requirement mapped to a principle and its associated guidelines. During the mapping activity for the Software Installation requirements, most requirements mapped to the current list of principles and guidelines. Others mapped directly to a principle and not any of the sub-guidelines.

The NIST team recommends no modifications to the principles and guidelines.

Other areas for future changes and development to the VVSG software installation requirements include:

- Remove all National Software Reference Library (NSRL) related content, which includes Part 1 5.3-E. This information resides within section 5.7 of the Election Assistance Commission's Testing & Certification Program Manual. The requirements were also removed from the 2015 VVSG 1.1.
- The Software Installation requirements are located in section 5.3 of the VVSG 2007. The numbering scheme within this section was inconsistent and seemed to refer to the previous section 5.2. These requirements can be seen below (5.2.1.2-G, 5.2.1.2-G.1, 5.2.1.2-J, and 5.2.1.2-J.1) This is likely a typographical error. When developing the new requirements, the number scheme should be consistent throughout the section.

The NIST team found that these other areas for future changes and development to the VVSG software installation requirements include downloading and installing voting system updates from a network-based repository.

Below is a list of software installation requirements that are discussed above for future changes and development. For more information about each requirement, please reference VVSG 2007 at: http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/2007-VVSG.pdf

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):	

5.2.1.2-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.

5.2.1.2-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.