**Test Assertions for VVSG 1.1, Volume 1, Section 7.4.6**

**September 23, 2016**

**VVSG 1.1, Vol 1, Requirement 7.4.6:** **Software Setup Validation**

The following requirements support the security of voting systems by providing methods to verify that only certified software is present on voting systems. It includes requirements for two software verification techniques. One method verifies digital signatures on software prior to installation on pieces of voting system equipment. This is a useful mechanism that helps prevent accidental or malicious software from being installed and could be employed by any voting system to protect against unauthorized software. The second method provides an external interface to voting system software. A separate piece of equipment could use this interface to verify the software on the voting system. However, this method merely provides a mechanism for detecting unauthorized software and, by itself, does not help prevent the installation of accidental or malicious software.

1. Setup validation methods **shall** verify that only certified software is present on the voting equipment. Certified software is COTS software components needed to run the voting system and voting software components identified by the manufacturer as authorized.
2. The manufacturer **shall** provide a method to comprehensively list all software files that are installed on voting systems.
3. This method **shall** list version names and numbers for all application software on the voting system.
4. This method should list of the date of installation for all application software on the voting system.
5. Setup validation methods **shall** include a software verification method that ensures that the voting system software has not been modified illegitimately.
6. The voting systems **shall** include any supporting software and hardware necessary to conduct the software verification method.
7. The manufacturer **shall** document the process used to conduct the software verification method.
8. The software verification method **shall** not modify the voting system software on the voting system.
9. Voting systems **shall** include a software verification method that either verifies software prior to installation or a method that verifies software using an external interface. Voting systems may include both software verification methods. Voting systems may provide ancillary setup validation methods, including methods for verifying or identifying installed software, other than those described in this section. There are no specific requirements for ancillary setup validation methods. However, any method intended to serve as the voting system software verification method must meet the requirements outlined in this section.
10. Voting systems which implement a software verification method that verifies software prior to installation **shall** meet the following requirements.
11. The voting system **shall** contain no more than one method for installing, updating, or removing software on a system.
	* Voting system equipment **shall** prevent processes from installing software except for the one specific software installation process identified by the manufacturer.
	* The voting system manufacturer **shall** document the procedures for installing, updating, and removing voting system software, configuration files, and data files.
	* Voting system equipment **shall** prevent processes from installing, updating or removing software while the polls are open.
	* Voting system equipment **shall** prevent the execution of software not installed using the specified software installation process.
12. The voting system **shall** only allow authenticated administrators to install software on voting equipment. The voting system **shall** present the administrator with a description of the software change being performed, including:
	* A list of all applications and/or file names being updated.
	* The type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file)
13. Voting system equipment **shall** store the current version identification of all software installed on the voting system equipment.
	* The current version identification **shall** be included as part of reports created by the voting system equipment.
	* The current version identification **shall** be displayed as part of the voting system equipment start up process.
14. The process for installing, updating and removing software **shall** make software changes based on information contained in software update packages. Software update packages **shall** minimally contain the following information:
	* A unique identifier for the software update package.
	* Names of the applications or files modified during the update process.
	* Version numbers of the applications or files modified during the update process.
	* Any software prerequisites or dependencies for the software involved in the update.
	* A description of the type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file).
	* The binary data of any new or updated files involved in the update process.
15. Software update packages **shall** be digitally signed by using a NIST approved algorithm with a security strength of at least 112 bits.
16. The software installation process **shall** verify digital signatures, software version identification, software prerequisites and dependencies, and manufacturer specific authorization information associated with the software before the software is installed. The software installation process **shall** not install software with invalid digital signatures, version numbers, or manufacturer specific authorization information, and **shall** not install software on systems that do not meet the update requisites.
17. The voting system **shall** have the capability to prevent the installation of previous versions of applications or files.
18. The software installation process **shall** result in information being stored in the voting system equipment’s log such that altering or deleting log entries or the log will be detected.
19. The minimum information to be included in the voting system audit log **shall** be:
	* Success or failure of the software installation process;
	* Cause of a failed software installation (such as invalid version identification, digital signature, etc.);
	* Application or file name(s), and version number(s);
	* A description of the type of action performed on each application and/or file (e.g., new application/file, deletion or overwriting of existing file);
	* A cryptographic hash of the software update package using FIPS 140-2 level 1 or higher validated cryptographic module.
20. If software is verified after being installed on the voting system equipment, the voting system equipment **shall** provide an external interface to the location of the voting system software for software verification purposes.
21. The external interface:
	* **Shall** be protected using tamper evident techniques,
	* **Shall** have a physical or logical indicator showing when the interface is enabled and disabled
	* **Shall** be disabled or protected during voting
	* Should provide a direct read-only access to the location of the voting system software without the use of installed software
22. The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system manufacturer.
	* 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.
	* 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.
23. Setup validation methods **shall** verify the contents of all system storage locations (e.g., system registers, variables, files, etc.) containing election specific information (e.g., ballot style, candidate registers, measure registers, etc.).
24. The manufacturer should provide a method to query the voting system to determine the value contained in all system storage locations containing election specific information.
25. The manufacturer **shall** document the default values of all system storage locations that hold election specific information.

**Test Assertions**

**TA746a-1:** The manufacturer SHALL identify, in the TDP, all voting system components designated as authorized.

**TA746a-2:** The manufacturer SHALL identify, in the TDP, all COTS software components that are needed to run the voting system.

**TA746a-3:** Election officials SHALL verify that the software present on the voting equipment is limited to authorized voting system components and/or COTS software components needed to run the voting system.

**TA746b-1:** The manufacturer SHALL provide a method to comprehensively list all software files that are installed on voting systems.

**TA746bi-1:** This method SHALL list version names for all application software on the voting system.

**TA746bi-2:** This method SHALL list version numbers for all application software on the voting system.

**TA746bii-1:** This method SHOULD list the date of installation for all application software on the voting system.

**TA746c-1:** Setup validation methods SHALL include a software verification method that ensures that voting system software on the voting system has not been modified without authorization.

**TA746ci-1:** The voting systems SHALL include any supporting software necessary to conduct the software verification method.

**TA746ci-2:** The voting systems SHALL include any supporting hardware necessary to conduct the software verification method.

**TA746cii-1:** The manufacturer SHALL document, in the TDP, the process used to conduct the software verification method.

**TA746ciii-1:** The software verification method SHALL NOT modify the voting system software on the voting system.

**TA746d-1:** Voting systems SHALL include a software verification method that 1) either verifies software prior to installation OR 2) verifies software using an external interface.

**TA746d-2:** Voting systems MAY include both a software verification method that verifies software prior to installation and a method that verifies software using an external interface.

**TA746d-3:** Voting systems MAY provide ancillary setup validation methods, including, but not limited to, methods for verifying or identifying installed software, other than those described in this section (Section 7.4.6a of the VVSG 1.1.)

**TA 746d-3-1:** All methods intended to serve as a voting system software verification method SHALL meet all the requirements outlined in this section (Section 7.4.6a of the VVSG 1.1.)

**TA746ei-1:** IF a voting system implements a software verification method that verifies software prior to installation THEN that voting system SHALL contain AT MOST one method for installing software on a system.

**TA746ei-1-1:** Voting system equipment SHALL NOT allow processes to install software except for the one specific software installation process identified by the manufacturer.

**TA746ei-1-2:** Voting system equipment SHALL NOT allow the execution of software that was not installed using the specified software installation process.

**TA746ei-1-3:** The voting system manufacturer SHALL document the procedures for installing voting system software.

**TA746ei-1-4:** The voting system manufacturer SHALL document the procedures for installing voting system configuration files.

**TA746ei-1-5:** The voting system manufacturer SHALL document the procedures for installing voting system data files.

**TA746ei-1-6:** Voting system equipment SHALL NOT allow processes to install software while the polls are open.

**TA746ei-2:** IF a voting system implements a software verification method that verifies software prior to installation THEN that voting system SHALL contain AT MOST one method for updating software on a system.

**TA746ei-2-1:** The voting system manufacturer SHALL document the procedures for updating voting system software.

**TA746ei-2-2:** The voting system manufacturer SHALL document the procedures for updating voting system configuration files.

**TA746ei-2-3:** The voting system manufacturer SHALL document the procedures for updating voting system data files.

**TA746ei-2-4:** Voting system equipment SHALL NOT allow processes to update software while the polls are open.

**TA746ei-3:** IF a voting system implements a software verification method that verifies software prior to installation THEN that voting system SHALL contain AT MOST than one method for removing software on a system.

**TA746ei-3-1:** The voting system manufacturer SHALL document the procedures for removing voting system software.

**TA746ei-3-2:** The voting system manufacturer SHALL document the procedures for removing voting system configuration files.

**TA746ei-3-3:** The voting system manufacturer SHALL document the procedures for removing voting system data files.

**TA746ei-3-4:** Voting system equipment SHALL NOT allow processes to remove software while the polls are open.

**TA746eii-1:** The voting system SHALL ONLY allow authenticated administrators to install software on voting equipment.

**TA746eii-2:** The voting system SHALL present the administrator with a description of the software change being performed, including, but not limited to:

o A list of all applications being updated.

o A list of all file names being updated.

o The type of action performed on each application.

o The type of action performed on each file.

**TA746eii-2-1:** The types of actions MAY include installing a new application.

**TA746eii-2-2:** The types of actions MAY include installing a new file.

**TA746eii-2-3:** The types of actions MAY include deleting an existing file.

**TA746eii-2-4:** The types of actions MAY include overwriting of an existing file.

**TA746eiii-1:** Voting system equipment SHALL store the current version identification of all software installed on the voting system equipment.

**TA746eiii-1-1:** The current version identification SHALL be included as part of reports created by the voting system equipment.

**TA746eiii-1-2:** The current version identification SHALL be displayed as part of the voting system equipment start up process.

**TA746eiv-1:** The process for installing software SHALL make software changes based on information contained in software update packages.

**TA746eiv-2:** The process for updating software SHALL make software changes based on information contained in software update packages.

**TA746eiv-3:** The process for removing software SHALL make software changes based on information contained in software update packages.

**TA746eiv-4:** Software update packages SHALL contain AT LEAST the following information:

o A unique identifier for the software update package.

o Names of the applications modified during the update process.

o Names of the files modified during the update process.

o Version numbers of the applications modified during the update process.

o Version numbers of the files modified during the update process.

o Any software prerequisites for the software involved in the update.

o Any software dependencies for the software involved in the update.

o A description of the type of action performed on each application (e.g., new application).

o A description of the type of action performed on each file (e.g., new file, deletion or overwriting of existing file).

o The binary data of any new files involved in the update process.

o The binary data of any updated files involved in the update process.

**TA746ev-1:** Software update packages SHALL be digitally signed by using a NIST approved algorithm.

**TA746ev-1-1:** The NIST approved algorithm SHALL have a security strength of at least 112 bits.

**TA746evi-1:** The software installation process SHALL verify digital signatures associated with the software before the software is installed.

**TA746evi-2:** The software installation process SHALL verify software version identification associated with the software before the software is installed.

**TA746evi-3:** The software installation process SHALL verify software prerequisites associated with the software before the software is installed.

**TA746evi-4:** The software installation process SHALL verify software dependencies associated with the software before the software is installed.

**TA746evi-5:** The software installation process SHALL verify manufacturer specific authorization information associated with the software before the software is installed.

**TA746evi-6:** The software installation process SHALL NOT install software with invalid digital signatures.

**TA746evi-7:** The software installation process SHALL NOT install software with invalid version numbers.

**TA746evi-8:** The software installation process SHALL NOT install software with invalid manufacturer specific authorization information.

**TA746evi-9:** The software installation process SHALL NOT install software on systems that do not meet the update requisites.

**TA746evii-1:** The voting system SHALL have the capability to prevent the installation of previous versions of applications.

**TA746evii-2:** The voting system SHALL have the capability to prevent the installation of previous versions of files.

**TA746eviii-1:** The software installation process SHALL result in information being stored in the voting system equipment’s log such that altering or deleting log entries or the log will be detected.

**TA746eix-1:** The information in the voting system audit log SHALL include, but not be limited to:

o Success or failure of the software installation process;

o Cause of a failed software installation;

o Application or file name;

o Application or file version number(s);

o A description of the type of action performed on each application and/or file;

o A cryptographic hash of the software update package using FIPS 140-2 level 1 or higher validated cryptographic module.

**TA746eix-1-1:** The type of action performed on each application and/or file MAY include a new application/file;

**TA746eix-1-2:** The type of action performed on each application and/or file MAY include deletion of existing file;

**TA746eix-1-3:** The type of action performed on each application and/or file MAY include overwriting of existing file;

**TA746eix-2:** IF the software installation process failed THEN the log SHALL include the cause of the failure;

**TA746eix-2-1:** The cause of the failure MAY be invalid version identification.

**TA746eix-2-2:** The cause of the failure MAY be invalid digital signature.

**TA746f-1:** IF software is verified after being installed on the voting system equipment, THEN the voting system equipment SHALL provide an external interface to the location of the voting system software for software verification purposes.

**TA746fi-1:** The external interface SHALL be protected using tamper evident techniques.

**TA746fi-2:** The external interface SHALL have a physical or logical indicator showing when the interface is enabled.

**TA746fi-3:** The external interface SHALL have a physical or logical indicator showing when the interface is disabled.

**TA746fi-4:** The external interface SHALL be disabled or SHALL be protected during voting.

**TA746fi-5:** The external interface SHOULD provide a direct read-only access to the location of the voting system software without the use of installed software.

**TA746fii-1:** The verification process SHOULD be capable of being performed using COTS software and/or COTS hardware that are not acquired from the voting system manufacturer.

**TA746fii-2:** IF the verification process uses hashes OR IF the verification process uses digital signatures THEN the software used in the verification process SHALL use a FIPS 140-2 level 1 validated cryptographic module OR the software used in the verification process SHALL use a validated cryptographic module higher than FIPS 140-2 level 1.

**TA746fii-3:** The verification process SHALL do one or more of the following two things:

1. The verification process SHALL use reference information on unalterable storage media received from the repository.
2. The verification process SHALL verify the digital signature of the reference information on any other media.

**TA746g-1:** Setup validation methods SHALL verify the contents of all system storage locations containing election specific information (e.g., ballot style, candidate registers, measure registers, etc.).

**TA746g-1-1:** All system storage locations SHALL include, but not be limited to, system registers, variables, and files.

**TA746g-1-2:** Election specific information SHALL include, but not be limited to, ballot style, candidate registers, and measure registers.

**TA746gi-1:** The manufacturer SHOULD provide a method to query the voting system to determine the value contained in all system storage locations that contain election specific information.

**TA746gi-1-1:** All system storage locations SHALL include, but not be limited to, system registers, variables, and files.

**TA746gi-1-2:** Election specific information SHALL include, but not be limited to, ballot style, candidate registers, and measure registers.

**TA746gii-1:** The manufacturer SHALL document the default values of all system storage locations that hold election specific information.

**TA746gii-1-1:** All system storage locations SHALL include, but not be limited to, system registers, variables, and files.

**TA746gii-1-2:** Election specific information SHALL include, but not be limited to, ballot style, candidate registers, and measure registers.

**Operational Definitions**

**Verification** – The process of querying and comparing baseline election-specific values. (ref TA746f-1)