**DRAFT Test Assertions for VVSG 1.0 Section 7.4.6**

**August 24, 2015**

**Requirement 7.4.6a**

**VVSG 1.0 Requirement 7.4.6a:**

1. Setup validation methods shall verify that no unauthorized software is present on the voting equipment.

**Test Assertions**

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

**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.

**VVSG 1.0 Requirement 7.4.6b:**

**VVSG 1.0 Requirement 7.4.6b:**

1. 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.
2. The process used to verify software should be possible to perform without using software installed on the voting system.
3. The vendor shall document the process used to verify software on voting equipment.
4. The process shall not modify the voting system software on the voting system during the verification process.

**Test Assertions**

**TA746b-1:** The manufacturer SHALL have a process to verify that the correct software is loaded on the voting system, using the reference information from the NSRL or using the reference information from a State designated repository.

**TA746b-2:** The manufacturer SHALL have a process to verify that there is no unauthorized software on the voting system, using the reference information from the NSRL or using the reference information from a State designated repository.

**TA746b-3:** The manufacturer SHALL have a process to verify that voting system software on the voting system has not been modified, using the reference information from the NSRL or using the reference information from a State designated repository.

**TA746bi:** The manufacturer’s process used to verify software SHOULD not require the use of software installed on the voting system.

**TA746bii:** The manufacturer SHALL document, in the TDP, the process used to verify software on the voting system.

**TA746biii:** IF the verification process has been started THEN the manufacturer’s software verification process SHALL NOT modify the voting system software on the voting system.

**VVSG 1.0 Requirement 7.4.6c:**

**VVSG 1.0 Requirement 7.4.6c:**

1. The vendor shall provide a method to comprehensively list all software files that are installed on voting systems.

**Test Assertions**

**TA746c-1:** The manufacturer SHALL provide a method to comprehensively list all software files that are installed on voting systems.

**TA746c-1-1:** This method SHOULD list version names for all application software on the voting system.

**TA746c-1-2:** This method SHOULD list numbers for all application software on the voting system.

**TA746c-1-3:** This method SHOULD list the date of installation for all application software on the voting system.

**VVSG 1.0 Requirement 7.4.6d:**

**VVSG 1.0 Requirement 7.4.6d:**

1. The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system vendor.
2. 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.
3. 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.

**Test Assertions**

**TA746d-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.

**TA746d-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.

**TA746d-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.

**VVSG 1.0 Requirement 7.4.6e:**

**VVSG 1.0 Requirement 7.4.6e:**

1. 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.
	* + - 1. The external interface shall be protected using tamper evident techniques
				2. The external interface shall have a physical indicator showing when the interface is enabled and disabled
				3. The external interface shall be disabled during voting
				4. The external interface should provide a direct read-only access to the location of the voting system software without the use of installed software

**Test Assertions**

**TA746e-1:** Voting system equipment SHALL provide a trusted external interface to ensure that the system software is able to be verified.

**TA746ei-1:** The trusted external interface SHALL be protected using tamper evident techniques.

**TA746eii-1:** The trusted external interface SHALL have a physical indicator showing when the interface is enabled.

**TA746eii-2:** The trusted external interface SHALL have a physical indicator showing when the interface is disabled.

**TA746eiii-1:** IF voting is in process THEN the trusted external interface SHALL be disabled.

**TA746eiv-1:** The external interface SHOULD provide a direct read-only access to the location of the voting system software without using installed software.

**VVSG 1.0 Requirement 7.4.6f:**

**VVSG 1.0 Requirement 7.4.6f:**

1. Setup validation methods shall verify that registers and variables of the voting system equipment contain the proper static and initial values.
	* + - 1. 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.
				2. 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.

**Test Assertions**

**TA746fi-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.

**TA746fi-1-1:** All system storage locations SHALL include, but not be limited to, system registers, variables, and files.

**TA746fi-1-2:** Election specific information SHALL include, but not be limited to, ballot style, candidate registers, and measure registers.

**TA746fii-1:** The manufacturer SHALL document the default values of all system storage locations that hold election specific information.

**TA746fii-1-1:** All system storage locations SHALL include, but not be limited to, system registers, variables, and files.

**TA746fii-1-2:** Election specific information SHALL include, but not be limited to, ballot style, candidate registers, and measure registers.

**TA746f-1:** Setup validation methods SHALL verify the contents of all system storage locations that contain election specific information.

**TA746f-1-1:** All system storage locations SHALL include, but not be limited to, system registers, variables, and files.

**TA746f-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**)