**DRAFT Test Assertions for VVSG 1.0 Section 7.5.1**

**August 24, 2015**

**Requirement 7.5.1**

**VVSG 1.0 Requirement 7.5.1:**

Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function.

1. Voting systems that use electrical or optical transmission of data shall ensure the receipt of valid vote records is verified at the receiving station. This should include standard transmission error detection and correction methods such as checksums or message digest hashes. Verification of correct transmission shall occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.
2. Voting systems that use telecommunications to communicate between system components and locations before the polling place is officially closed shall:
3. Implement an encryption standard currently documented and validated for use by an agency of the U.S. government
4. Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System

**Test Assertions**

**TA751a-1:** IF a voting system uses electrical transmission of data (including but not limited Ethernet transmission) THEN the voting system SHALL ensure that the receipt of valid vote records is verified at the receiving station.

**TA751a-2:** IF a voting system uses optical transmission of data (including but not limited to infrared or fiber optic transmission) THEN the voting system SHALL ensure that the receipt of valid vote records is verified at the receiving station.

**TA751a-3:** Verification at the receiving station SHOULD include standard transmission error detection.

**TA751a-4:** Verification at the receiving station SHOULD include correction methods.

**TA751a-4-1:** The correction methods MAY include checksums.

**TA751a-4-2:** The correction methods MAY include message digest hashes.

**TA751a-5:** Verification of correct transmission SHALL occur at the voting system application level.

**TA751a-5-1:** Verification of correct transmission MAY occur through receipt of assurances or evidence from another level.

**TA751a-6:** Verification of correct transmission SHALL ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.

**TA751a-7:** Cryptography used to verify the receipt of vote records SHALL use NIST approved algorithms with security strength of at least 112 bits.

**TA751a-8:** Message Authentication Code (MAC) keys SHALL have a security strength of at least 112 bits.

**TA751bi-1:** IF a voting system uses telecommunications to communicate between system components and locations before the polling place is officially closed THEN that voting system SHALL implement an encryption standard currently documented by an agency of the U.S. government.

**TA751bi-2:** IF a voting system uses telecommunications to communicate between system components and locations before the polling place is officially closed THEN that voting system SHALL implement an encryption standard validated for use by an agency of the U.S. government.

**TA751bi-3:** IF a voting system uses telecommunications to communicate between system components and locations THEN that voting system SHALL implement encryption using NIST approved algorithms with a security strength of at least 112 bits within a FIPS 140-2 level 1 or higher validated cryptographic module operating in FIPS mode.

**TA751bii-1:** IF a voting system uses telecommunications to communicate between system components and locations before the polling place is officially closed THEN that voting system SHALL provide a means to detect the presence of an intrusive process.

**TA751bii-1-1:** The means to detect the presence of an intrusive process MAY be an Intrusion Detection System.

**Operational Definitions**

**Telecommunications** – Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means. (SOURCE: CNSSI-4009)

**Public telecommunications** – Is a form of telecommunications which includes electrical, optical, and wireless transmission using public telecommunications lines.