**DRAFT Test Assertions for VVSG 1.0 Section 7.7.3**

**August 24, 2015**

**Requirement 7.7.3**

**VVSG 1.0 Requirement 7.7.3:**

The transmitted data, especially via wireless communications, needs to be protected to ensure confidentiality and integrity. Examples of election information that needs to be protected include: ballot definitions, voting device counts, precinct counts, opening of poll signal, and closing of poll signal. Examples of other information that needs to be protected include: protocol messages, address or device identification information, and passwords. Since radio frequency wireless signals radiate in all directions and pass through most construction material, anyone may easily receive the wireless signals. In contrast, infrared signals are line of sight and do not pass through most construction material. However, infrared signals can still be received by other devices that are in the line of sight. Similarly, wireless signals can be transmitted by others to create unwanted signals. Thus, encryption is required to protect the privacy and confidentiality of the voting information.

* + 1. All information transmitted via wireless communications shall be encrypted and authenticated--with the exception of wireless T-coil coupling--to protect against eavesdropping and data manipulation including modification, insertion, and deletion.
			1. The encryption shall be as defined in Federal Information Processing Standards (FIPS) 197, “Advanced Encryption Standard (AES).”
			2. The cryptographic modules used shall comply with FIPS 140-2, Security Requirements for Cryptographic Modules.
		2. The capability to transmit non-encrypted and non-authenticated information via wireless communications shall not exist.
		3. If audible wireless communication is used, and the receiver of the wireless transmission is the human ear, then the information shall not be encrypted.

**Discussion:** This specifically covers wireless T-Coil coupling for assistive devices used by people who are hard of hearing.

**Test Assertions**

**TA773a-1:** IF information is transmitted via wireless communications THEN all that information, except wireless T-coil coupling, SHALL be encrypted in order to protect against eavesdropping.

**TA773a-2:** IF information is transmitted via wireless communications THEN all that information, except wireless T-coil coupling, SHALL be encrypted in order to protect against data manipulation including modification, insertion, and deletion.

**TA773a-3:** IF information is transmitted via wireless communications THEN all that information, except wireless T-coil coupling, SHALL be authenticated in order to protect against eavesdropping.

**TA773a-4:** IF information is transmitted via wireless communications THEN all that information, except wireless T-coil coupling, SHALL be authenticated in order to protect against data manipulation including modification, insertion, and deletion.

**TA773a-5:** Cryptography used SHALL use NIST approved algorithms with security strength of at least 112 bits.

**TA773ai-1:** The encryption SHALL be as defined in Federal Information Processing Standards (FIPS) 197, “Advanced Encryption Standard (AES).”

**TA773ai-2:** Message Authentication Code (MAC) keys SHALL have a security strength of at least 112 bits.

**TA773aii-1:** The cryptographic modules used SHALL comply with FIPS 140-2, Security Requirements for Cryptographic Modules.

**TA773b-1:** Voting Systems SHALL ONLY have the capability to transmit encrypted and authenticated information via wireless communications.

**TA773b-2:** Voting Systems SHALL ONLY have the capability to transmit non-authenticated information via wireless communications.

**TA773c-1:** IF audible wireless communication is used AND IF the receiver of the wireless transmission is the human ear THEN the information SHALL NOT be encrypted.