**DRAFT Test Assertions for VVSG 1.0 Section 7.7.1**

**August 24, 2015**

**Requirement 7.7.1**

**VVSG 1.0 Requirement 7.7.1:**

1. If wireless communications are used in a voting system, then the vendor shall supply documentation describing how to use all aspects of wireless communications in a secure manner. This documentation shall include:
   1. A complete description of the uses of wireless in the voting system including descriptions of the data elements and signals that are to be carried by the wireless mechanism
   2. A complete description of the vulnerabilities associated with this proposed use of wireless, including vulnerabilities deriving from the insertion, deletion, modification, capture or suppression of wireless messages
   3. A complete description of the techniques used to mitigate the risks associated with the described vulnerabilities including techniques used by the manufacturer to ensure that wireless cannot send or receive messages other than those situations specified in the documentation. Cryptographic techniques shall be carefully and fully described, including a description of cryptographic key generation, management, use, certification, and destruction
   4. A rationale for the inclusion of wireless in the proposed voting system, based on a careful and complete description of the perceived advantages and disadvantages of using wireless for the documented uses compared to using non-wireless approaches

**Discussion:** In general, convenience is not a sufficiently compelling reason, on its own, to justify the inclusion of wireless communications in a voting system. Convenience must be balanced against the difficulty of working with cryptographic keys.

1. The details of all cryptographic protocols used for wireless communications, including the specific features and data, shall be documented.
2. The wireless documentation shall be closely reviewed for accuracy, completeness, and correctness.
3. There shall be no undocumented use of the wireless capability, nor any use of the wireless capability that is not entirely controlled by an election official.

**Discussion:** This can be tested by reviewing all of the software, hardware, and documentation, and by testing the status of wireless activity during all phases of testing.

1. If a voting system includes wireless capabilities, then the voting system shall be able to accomplish the same function if wireless capabilities are not available due to an error or no service.
   1. The manufacturer shall provide documentation how to accomplish these functions when wireless is not available.
2. The system shall be designed and configured so it is not vulnerable to a single point of failure using wireless communications that causes a total loss of any voting capabilities.
3. If a voting system includes wireless capabilities, then the system shall have the ability to turn on the wireless capability when it is to be used and to turn off the wireless capability when the wireless capability is not in use.
4. If a voting system includes wireless capabilities, then the system shall not activate the wireless capabilities without confirmation from an elections official.

**Test Assertions**

**TA771a-1:** IF a voting system uses wireless communications THEN then the manufacturer SHALL supply documentation, in the TDP, describing how to use all aspects of wireless communications in a secure manner. This documentation SHALL include, but not be limited to:

**TA771ai-1:** A complete description of the uses of wireless in the voting system.

**TA771ai-1-1:** The uses of wireless in the voting system SHALL include descriptions of the data elements that are to be carried by the wireless mechanism.

**TA771ai-1-2:** The uses of wireless in the voting system SHALL include descriptions of the control signals and/or commands that are to be carried by the wireless mechanism.

**TA771aii-1:** A complete description of the vulnerabilities associated with this proposed use of wireless.

**TA771aii-1-1:** These vulnerabilities SHALL include, but not be limited to, vulnerabilities deriving from the insertion of wireless messages.

**TA771aii-1-2:** These vulnerabilities SHALL include, but not be limited to, vulnerabilities deriving from the deletion of wireless messages.

**TA771aii-1-3:** These vulnerabilities SHALL include, but not be limited to, vulnerabilities deriving from the modification of wireless messages.

**TA771aii-1-4:** These vulnerabilities SHALL include, but not be limited to, vulnerabilities deriving from the capture of wireless messages.

**TA771aii-1-5:** These vulnerabilities SHALL include, but not be limited to, vulnerabilities deriving from the suppression of wireless messages.

**TA771aiii-1:** A complete description of the techniques used to mitigate the risks associated with the described vulnerabilities.

**TA771aiii-1-1:** These techniques SHALL include, but not be limited to, techniques used by the manufacturer to ensure that wireless cannot send messages other than IN those situations specified in the documentation.

**TA771aiii-1-2:** These techniques SHALL include, but not be limited to, techniques used by the manufacturer to ensure that wireless cannot receive messages other than IN those situations specified in the documentation.

**TA771aiii-2:** ALL cryptographic techniques SHALL be comprehensively described in the TDP.

**TA771aiii-3:** This cryptographic documentation SHALL include descriptions of the basis of the technique with respect to:

1. algorithms used
2. standards used
3. its purpose

**TA771aiii-3-1:** Cryptographic techniques SHALL include, but not be limited to, a description of cryptographic key generation.

**TA771aiii-3-2:** Cryptographic techniques SHALL include, but not be limited to, a description of cryptographic key management.

**TA771aiii-3-3:** Cryptographic techniques SHALL include, but not be limited to, a description of cryptographic key use.

**TA771aiii-3-4:** Cryptographic techniques SHALL include, but not be limited to, a description of cryptographic key certification.

**TA771aiii-3-5:** Cryptographic techniques SHALL include, but not be limited to, a description of cryptographic key destruction.

**TA771aiii-4:** ALL rationale for the inclusion of wireless in the proposed voting system SHALL be comprehensively described in the TDP.

**TA771aiii-5:** This documentation SHALL include descriptions of the basis of the rationale with respect to:

1. algorithms used
2. standards used
3. its purpose

**TA771aiv-5-1:** This rationale SHALL be based on a careful description of the perceived advantages and disadvantages of using wireless for the documented uses compared to using non-wireless approaches.

**TA771aiv-5-2:** This rationale SHALL be based on a complete description of the perceived advantages and disadvantages of using wireless for the documented uses compared to using non-wireless approaches.

**TA771b-1:** IF a cryptographic protocol is used for wireless communications THEN its details SHALL be documented.

**TA771b-1-1:** These details SHALL include, but not be limited to what the protocol is (cite or provide the relevant standard or specification that describes this protocol).

**TA771b-1-2:** These details SHALL include, but not be limited to how the protocol is used.

**TA771b-1-3:** These details SHALL include, but not be limited to any optional features or “protocol extensions” implemented by the voting system’s use of the protocol.

**TA771d-1:** All usage of the wireless capability SHALL be documented.

**TA771d-2:** Voting systems SHALL allow election officials to control wireless communications.

**TA771e-1:** IF a voting system includes wireless capabilities AND wireless capabilities are not available due to an error or wireless capabilities are not available due to not having service THEN the voting system SHALL be able to accomplish the same function that was being accomplished by wireless capabilities.

**TA771ei-1:** For all functions that are carried out by wireless capabilities, the manufacturer SHALL provide documentation, in the TDP, that explains how to accomplish these functions when wireless is not available.

**TA771f-1:** The voting system SHALL be designed so that when using wireless communications it is not vulnerable to a single point of failure that causes a total loss of any voting capabilities.

**TA771f-2:** The voting system SHALL be configured so that when using wireless communications it is not vulnerable to a single point of failure that causes a total loss of any voting capabilities.

**TA771g-1:** IF a voting system includes wireless capabilities THEN that system SHALL have the ability to turn on the wireless capability when the wireless capability is to be used.

**TA771g-2:** IF a voting system includes wireless capabilities THEN that system SHALL have the ability to turn off the wireless capability when the wireless capability is not in use.

**TA771h-1:** IF a voting system includes wireless capabilities THEN that system SHALL ONLY activate the wireless capabilities by obtaining confirmation from an elections official.