**DRAFT Test Assertions for VVSG 1.0 Section 7.6.1**

**August 24, 2015**

**Requirement 7.6.1**

**VVSG 1.0 Requirement 7.6.1:**

All systems that transmit data over public telecommunications networks shall:

1. Preserve the secrecy of voter ballot selections and prevent anyone from violating ballot privacy
2. Employ digital signatures for all communications between the vote server and other devices that communicate with the server over the network
3. Require that at least two authorized election officials activate any critical operation regarding the processing of ballots transmitted over a public communications network, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of votes

**Test Assertions**

**TA761a-1:** IF a voting system transmits data over at least one public transportation network THEN the voting system SHALL preserve the secrecy of voter ballot selections.

**TA761a-2:** IF a voting system transmits data over at least one public transportation network THEN the voting system SHALL prevent anyone from violating ballot privacy, including, but not limited to, the identity of the ballot caster.

**TA761b-1:** IF a voting system transmits data over at least one public telecommunications network THEN the voting system SHALL employ cryptographic digital signatures for all communications between the vote server and other devices that communicate with the server over that network.

**TA761c-1:** A voting system that transmits data over at least one public transportation network SHALL NOT allow any critical operation regarding the processing of ballots transmitted over a public communications network without the authorization of at least two election officials.

**TA761c-1:** The allowance MAY be satisfied by means of voting system documentation.

**TA761c-2:** The allowance MAY be satisfied by means of voting system work flow implementation.

**TA761c-3:** Such critical operations SHALL include, but not be limited to, the aggregation and sending of votes and vote tabulations.

**TA761c-2:** Cryptography used to provide protection of data transmitted over public telecommunications networks SHALL use NIST approved algorithms with security strength of at least 112 bits.

**TA761c-3:** Message Authentication Code (MAC) keys SHALL have a security strength of at least 112 bits.