**Test Assertions for VVSG 1.1, Volume 1, Section 7.3**

**September 23, 2016**

**VVSG 1.1, Vol 1, Requirement 7.3:** **Physical Security Measures**

A voting system’s sensitivity to disruption or corruption of data depends, in part, on the physical location of equipment and data media. Most often, the disruption of voting and vote counting results from a physical violation of one or more areas of the system thought to be protected. Therefore, security procedures shall address physical threats and the corresponding means to defeat them.

1. Any unauthorized physical access shall leave physical evidence that an unauthorized event has taken place.
2. Voting systems shall only have physical ports and access points that are essential to voting operations and/or to voting system testing and/or auditing.
3. An event log entry that identifies the name of the affected device shall be generated if a component connected to a piece of voting system equipment is disconnected while polls are open.
4. Ports disabled while polls are open shall only be re-enabled by authorized administrators.
5. Access points, such as covers and panels, shall be secured by locks or tamper-evident seals or tamper resistant countermeasures shall be implemented so that the authorized election official can monitor access to voting system components through these points.
6. Ballot boxes shall be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.

**Test Assertions**

**TA73-1:** A voting system SHALL contain a risk assessment of physical threats.

**TA73-1-1:** The risk assessment SHALL identify all potential vulnerabilities.

**TA73-1-2:** The risk assessment SHALL identify all potential threats.

**TA73-1-3:** The risk assessment SHALL identify all potential risks that each identified vulnerability is exercised by all corresponding threats.

**TA73-1-4:** The risk assessment SHALL identify the impact of each identified risk.

**TA73-1-5:** The risk assessment SHALL contain likelihood of threat events as well as the basis used to determine those likelihoods.

**TA73-1-6:** The risk assessment SHALL contain impact of threat events as well as the basis used to determine those impacts.

**TA73-1-7:** The risk assessment SHALL identify all potential vulnerabilities and threats capable of exploiting those vulnerabilities.

**TA73-1-8:** Voting systems MAY use SP-800-30 (Guide for Conducting Risk Assessments) in developing this risk assessment.

**TA73a-1:** IF an unauthorized event has occurred THEN physical evidence SHALL be present that allows an election official to identify that the unauthorized event has occurred.

**TA73b-1:** IF a voting system contains one or more physical ports THEN the voting system manufacturer SHALL document, in the TDP, what operations would fail if that port did not exist.

**TA73b-2:** IF a voting system contains one or more physical ports THEN each and every physical port SHALL be essential to voting system testing.

**TA73b-3:** IF a voting system contains one or more physical ports THEN each and every physical port SHALL be essential to voting system auditing.

**TA73b-4:** IF a voting system contains one or more access points THEN the voting system manufacturer SHALL document, in the TDP, what operations would fail if that access point did not exist.

**TA73b-5:** IF a voting system contains one or more access points THEN each and every access point SHALL be essential to voting system testing.

**TA73b-6:** IF a voting system contains one or more access points THEN each and every access point SHALL be essential to voting system auditing.

**TA73b-7:** IF a voting system contains one or more physical ports THEN each and every physical port SHALL be essential to one or more of the following: voting operations, voting system testing, or voting system auditing.

**TA73b-8:** IF a voting system contains one or more access points THEN each and every access point SHALL be essential to one or more of the following: voting operations, voting system testing, or voting system auditing.

**TA73c-1:** IF a voting system component is disconnected while the polls are open THEN an event log entry SHOULD be generated.

**TA73c-1-1**: The event log entry SHALL identify the name of the affected device.

**TA73d-1:** The voting system SHALL allow ONLY authorized administrators to reenable disabled ports while polls are open.

**TA73e-1:** All voting system access points, including but not limited to, covers and panels, SHOULD implement at least one of the following three requirements:

**TA73e-1-1:** The access points SHOULD be secured by locks.

**TA73e-1-2:** The access points SHOULD be secured by tamper-evident seals.

**TA73e-1-3:** Tamper resistant counter measures SHOULD be implemented.

**TA73e-1-3-1:** IF tamper resistant counter measures are implemented THEN system owners SHALL be able monitor access to voting system components thorough these points.

**TA73f-1:** IF unauthorized physical access occurs to a ballot box THEN physical evidence, which makes the unauthorized physical access apparent, SHALL be available.

**Operational Definitions**

**Ballot box –** a sealed box into which voters put completed ballots (ref 73f-1)

**Threat model –** a formal description for a set of possible attacks and their remedies (ref 73-1)