**Test Assertions for VVSG 1.1, Volume 1, Section 7.2.1**

**September 23, 2016**

**VVSG 1.1, Vol 1, Requirement 7.2.1:** **General Access Control**

General requirements address the high-level functionality of a voting system. These are the fundamental access control requirements upon which other requirements in this section are based.

1. Voting system equipment shall provide access control mechanisms designed to permit authorized access to the voting system and to prevent unauthorized access to the voting system.
2. Access control mechanisms on the EMS shall be capable of identifying and authenticating individuals permitted to perform operations on the EMS.
3. Voting system equipment shall provide controls that permit or deny access to the device’s software and files.
4. The default access control permissions shall implement the minimum permissions needed for each role or group identified by a device.
5. The voting system equipment shall prevent a lower-privileged process from modifying a higher-privileged process.
6. An administrator of voting system equipment shall authorize privileged operations.
7. Voting system equipment shall prevent modification to or tampering with software or firmware through any means other than the documented procedure for software upgrades.

**Test Assertions**

**TA721a-1:** Voting system equipment SHALL provide access control mechanisms.

**TA721a-1-1:** These access control mechanisms SHALL permit authorized access to the voting system.

**TA721a-1-2:** These access control mechanisms SHALL prevent unauthorized access to the voting system.

**TA721ai-1:** Access control mechanisms on the EMS SHALL be capable of identifying individuals permitted to perform operations on the EMS.

**TA721ai-2:** Access control mechanisms on the EMS SHALL be capable of authenticating individuals permitted to perform operations on the EMS.

**TA721b-1-1:** Voting system equipment SHALL provide controls that permit authorized access to the device’s software.

**TA721b-1-2:** Voting system equipment SHALL provide controls that deny unauthorized access to the device’s software.

**TA721b-2-1:** Voting system equipment SHALL provide controls that permit authorized access to the device’s files.

**TA721b-2-2:** Voting system equipment SHALL provide controls that deny unauthorized access to the device’s files.

**TA721c-1:** The default access control permissions SHALL implement ONLY the minimum permissions needed for each role/group identified by a device.

**TA721d-1:** The voting system equipment SHALL NOT allow a lower-privileged process to modify a higher-privileged process.

**TA721e-1:** ONLY an administrator of voting system equipment SHALL authorize privileged operations.

**TA721f-1:** IF the documented procedure for software upgrades is not followed THEN the voting system equipment SHALL NOT allow modification to software or firmware.

**TA721f-2:** IF the documented procedure for software upgrades is not followed THEN the voting system equipment SHALL NOT allow tampering with software or firmware.

**Operational Definitions**

**Access control:** The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).

(source: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf)

**Election management system (EMS):** Set of processing functions and databases within a voting system that defines, develops and maintains election databases, performs election definitions and setup functions, format ballots, count votes, consolidates and report results, and maintains audit trails.

(source: https://eac926.ae-admin.com/assets/1/Documents/VVSG.1.1.VOL.1.FINAL.pdf)