**DRAFT Test Assertions for VVSG 1.0 Section 7.2.1**

**August 24, 2015**

**Requirement 7.2.1**

**VVSG 1.0 Requirement 7.2.1:** The vendor shall specify the general features and capabilities of the access control policy recommended to provide effective voting system security.

Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for:

1. Software access controls
2. Hardware access controls
3. Communications
4. Effective password management
5. Protection abilities of a particular operating system
6. General characteristics of supervisory access privileges
7. Segregation of duties
8. Any additional relevant characteristics

**Test Assertions**

**TA721-1:** The TDP SHALL contain a detailed list of general features of the recommended access control policy that are needed to provide effective voting system security.

**TA721-2:** The TDP SHALL contain a detailed list of capabilities of the recommended access control policy that are needed to provide effective voting system security.

**TA721-3:** The list of features and capabilities, described in the TDP, SHALL be designed to permit authorized access to the voting system.

**TA721-4:** The list of features and capabilities, described in the TDP, SHALL be designed to prevent unauthorized access to the voting system.

**TA721a-1:**  The TDP SHALL contain a description of recommended policies for software access controls.

**TA721b-1:** The TDP SHALL contain a description of recommended policies for hardware access controls including, but not limited to, seals, locks, and keys.

**TA721c-1:** The TDP SHALL contain a description of recommended policies for how access control is performed among network-connected devices.

**TA721c-1-1:** Network-connected devices SHALL include those connected local (or private) networks and those connected to public networks.

**TA721c-1-2:** Point to point communication with I/O devices or peripherals MAY NOT be considered to be network-connected devices.

**TA721d-1:** The TDP SHALL contain a description of recommended policies for effective password management, including but not limited to, password generation (i.e., manual vs. automated), strength, length, use, default, expiration, and distribution.

**TA72d-1-1:** This shall include the policy for password creation, change, activation, or deactivation.

**TA72d-1-2:** This shall also document who is authorized to carry out the above activities.

**TA721e-1:** The TDP SHALL contain a description of recommended policies for access control enforced by the voting system’s operating systems.

**TA721e-1-1:** This description MAY reference a checklist.

**TA721f-1:**  The TDP SHALL contain a description of recommended policies for general characteristics of supervisory access privileges, including but not limited to, listing supervisory and administrative accounts, the permissions or capabilities of those accounts, and a description of how to configure those accounts.

**TA721g-1:** The TDP SHALL contain a description of recommended policies for segregation of duties.

**TA721h-1:** The TDP SHALL contain a description of recommended policies for any other characteristics of access control used by the voting system that are needed to provide effective voting system security, including but not limited to, biometrics, tokens, smart cards, digital pins, and digital signatures.

**TA721-5:** The TDP SHALL contain a description of recommended policies for providing controls that permit or deny access to the device’s software and files.

**TA721-6:** The TDP SHALL contain a description of recommended policies for preventing modification to software or firmware through any means other than the documented procedure for software upgrades.

**TA721-7:** The TDP SHALL contain a description of recommended policies for prevention of tampering with software or firmware through any means other than the documented procedure for software upgrades.

**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)*