**Test Assertions for VVSG 1.1, Volume 1, Section 7.2.3**

**September 23, 2016**

**VVSG 1.1, Vol 1, Requirement 7.2.3:** **Access Control Authentication**

Authentication establishes the validity of the identity of the user, application, or process interacting with the voting system. Authentication is based on the identification provided by the user, application, or process interacting with the voting system. User authentication is generally classified in one of the following three categories:

* Something the user knows – this is usually a password, pass phrase, or PIN
* Something the user has – this is usually a token that may be either hardware or software based, such as a smart card
* Something the user is – this is usually a fingerprint, retina pattern, voice pattern or other biometric data

Traditional password authentication is a single factor authentication method. A more secure method of authentication combines the various methods of authentication into two-factor authentication, or multi-factor authentication. For example, a user may use an authentication token and a passphrase for authentication. Using multi-factor provides stronger authentication than single factor. There are also cryptographic-based authentication methods such as digital signatures and challenge-response authentication, which are either software or hardware-based based tokens.

The following authentication requirements apply to all voting system equipment.

1. Voting system equipment shall authenticate users prior to granting them access to system functions or data.
2. When private or secret authentication data is stored in voting system equipment, the data shall be protected to ensure that the confidentiality and integrity of the data is not violated.
3. Voting system equipment shall allow the administrator group or role to set and change passwords, pass phrases, and keys.
4. Voting system equipment shall allow privilege groups or roles to be disabled and allow new individual privileged groups or roles to be created.
5. Voting system equipment shall lock out groups, roles, or individuals after a specified number of consecutive failed authentication attempts within a pre-defined time period.
6. Voting systems shall allow the administrator group or role to configure the account lock out policy, including the time period within which failed attempts must occur, the number of consecutive failed access attempts allowed before lock out, and the length of time the account is locked out.
7. If the voting system uses a user name and password authentication method, the voting system shall allow the administrator to enforce password strength, histories, and expiration.
8. The voting system shall allow the administrator group or role to specify password strength for all accounts, including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters.
9. The voting system shall enforce password histories, and allow the administrator to configure the history length.
10. Voting system equipment shall ensure that the username is not used in the password.
11. Voting systems shall provide a means to automatically expire passwords in accordance with the voting jurisdiction’s policies.

**Test Assertions**

**TA723a-1:** IF a user desires access to their permitted system functions THEN that the voting system SHALL authenticate that user before granting the user access to the system functions.

**TA723a-2:** IF a user desires access to their permitted system data THEN that the voting system SHALL authenticate that user before granting the user access to the system data.

**TA723b-1:** IF private authentication data is stored in voting system equipment, THEN the data SHALL be protected to ensure that the confidentiality and integrity of the data is not violated.

**TA723b-2:** IF secret authentication data is stored in voting system equipment, THEN the data SHALL be protected to ensure that the confidentiality and integrity of the data is not violated.

**TA723c-1:** Voting system equipment SHALL allow the administrator group/role to set passwords.

**TA723c-2:** Voting system equipment SHALL allow the administrator group/role to set pass phrases.

**TA723c-3:** Voting system equipment SHALL allow the administrator group/role to set keys.

**TA723c-4:** Voting system equipment SHALL allow the administrator group/role to change passwords.

**TA723c-5:** Voting system equipment SHALL allow the administrator group/role to change pass phrases.

**TA723c-6:** Voting system equipment SHALL allow the administrator group/role to change keys.

**TA723d-1:** Voting system equipment SHALL allow individual privilege groups/roles to be disabled.

**TA723d-2:** Voting system equipment SHALL allow some privilege groups/roles to be disabled.

**TA723d-3:** Voting system equipment SHALL allow all privilege groups/roles to be disabled.

**TA723d-4:** Voting system equipment SHALL allow individual groups/roles to be disabled.

**TA723d-5:** Voting system equipment SHALL allow some groups/roles to be disabled.

**TA723d-6:** Voting system equipment SHALL allow all groups/roles to be disabled.

**TA723d-7:** Voting system equipment SHALL allow new individual privileged groups/roles to be created.

**TA723d-8:** Voting system equipment SHALL allow new individual groups/roles to be created.

**TA723e-1:** Voting system equipment SHALL lock out groups/roles after a specified number of consecutive failed authentication attempts within a pre-defined time period.

**TA723e-2:** Voting system equipment SHALL lock out individuals after a specified number of consecutive failed authentication attempts within a pre-defined time period.

**TA723f-1:** Voting systems SHALL allow the administrator group/role to configure the account lock out policy.

**TA723f-1-1:** The account lock out policy allowed to be configured SHALL include the time period within which failed attempts must occur AND the number of consecutive failed access attempts allowed before lock out AND the length of time the account is locked out.

**TA723g-1:** IF the voting system uses a user name and password authentication method, THEN the voting system SHALL allow ONLY the administrator to enforce password strength.

**TA723g-2:** IF the voting system uses a user name and password authentication method, THEN the voting system SHALL allow ONLY the administrator to enforce password histories.

**TA723g-3:** IF the voting system uses a user name and password authentication method, THEN the voting system SHALL allow ONLY the administrator to enforce password expiration.

**TA723h-1:** The voting system SHALL allow ONLY the administrator group/role to specify password strength for all accounts.

**TA723h-1-1:** The password strength allowed to be specified SHALL include the POLICY governing the minimum password length AND use of capitalized letters AND use of numeric characters AND use of non-alphanumeric characters.

**TA723i-1:** The voting system SHALL enforce password histories.

**TA723i-2:** The voting system SHALL allow ONLY the administrator to configure the password history length.

**TA723j-1:** For all passwords used, the voting system equipment SHALL NOT allow the username to be used anywhere within in the password.

**TA723k-1:** Voting systems SHALL provide a mechanism to automatically expire passwords.

**TA723k-1-1:** This mechanism SHALL be configurable to include the voting jurisdiction’s policies.