**Test Assertions for VVSG 1.1, Volume 1, Section 7.5.4**

**September 23, 2016**

**VVSG 1.1, Vol 1, Requirement 7.5.4:** **Shared Operating Environment**

Ballot recording and vote counting can be performed in either a dedicated or non-dedicated environment. If ballot recording and vote counting operations are performed in an environment that is shared with other data processing functions, both hardware and software features shall be present to protect the integrity of vote counting and of vote data.

Systems that use a shared operating environment shall:

1. Use security procedures and logging records to control access to system functions
2. Partition or compartmentalize voting system functions from other concurrent functions at least logically, and preferably physically as well
3. Control system access by means of passwords, and restrict account access to necessary functions only
4. Have capabilities in place to control the flow of information, precluding data leakage through shared system resources

**Test Assertions**

**TA754-1:** The test assertions in this section SHALL apply even if the system does not implement communications.

**TA754-2:** IF ballot recording and vote counting operations are both performed in an environment that is shared with other data processing functions THEN hardware features SHALL be present to protect the integrity of vote counting and of vote data.

**TA754-2-1:** Implementing HW-enforced process isolation features to preserve integrity SHALL be sufficient to satisfy this requirement.

**TA754-3:** IF ballot recording and vote counting operations are both performed in an environment that is shared with other data processing functions THEN software features SHALL be present to protect the integrity of vote counting and of vote data.

**TA754-3-1:** Designing software to use the HW-enforced process isolation features SHALL be sufficient to satisfy this requirement.

**TA754a-1:** IF voting systems use a shared operating environment THEN those systems SHALL use security procedures to control access to system functions.

**TA754a-1-1:** IF voting systems use a shared operating environment THEN those systems SHALL use security procedures to control physical and/or logical access to system functions.

**TA754a-2:** IF voting systems use a shared operating environment THEN those systems SHALL use logging records to record access to system functions.

**TA754b-1:** IF voting systems use a shared operating environment THEN those systems SHALL partition voting system functions logically from other concurrent functions.

**TA754b-2:** IF voting systems use a shared operating environment THEN those systems SHOULD also compartmentalize voting system functions physically from other concurrent functions.

**TA754c-1:** IF voting systems use a shared operating environment THEN those systems SHALL restrict election-administration functions to accounts for election officials.

**TA754c-2:** IF voting systems use a shared operating environment THEN those systems SHOULD ensure that election-specific accounts only have privileges necessary to perform election-administration functions.

**TA754c-3:** IF voting systems use a shared operating environment and use password authentication THEN those systems SHALL ensure that election-specific accounts only have privileges necessary to perform election-administration functions.

**TA754c-4:** IF voting systems use a shared operating environment THEN those systems SHALL restrict account access to necessary functions only.

**TA754d-1:** IF voting systems use a shared operating environment THEN those systems SHALL have capabilities in place to control the flow of information to and from shared system resources.

**TA754d-1-1:** Non-voting-related processes and services SHALL NOT have access to memory or storage location used by voting-related processes and services.