**Test Assertions for VVSG 1.1, Volume 1, Section 7.5.2**

**September 23, 2016**

**VVSG 1.1, Vol 1, Requirement 7.5.2:** **Protection Against External Threats**

1. Voting systems that use public telecommunications networks **shall** implement protections against external threats to which commercial products used in the system may be susceptible.
2. Voting systems that use public telecommunications networks **shall** provide system documentation that clearly identifies all COTS hardware and software products and communications services used in the development and/or operation of the voting system, including operating systems, communications routers, modem drivers and dial-up networking software.
	1. Such documentation **shall** identify the name, manufacturer, and version used for each such component.
3. Voting systems that use public telecommunications networks **shall** use protective software at the receiving-end of all communications paths to:
	1. Detect the presence of a threat in a transmission
	2. Remove the threat from infected files/data
	3. Prevent against storage of the threat anywhere on the receiving device
	4. Provide the capability to confirm that no threats are stored in system memory and in connected storage media
	5. Provide data to the system audit log indicating the detection of a threat and the processing performed
4. Manufacturers **shall** use multiple forms of protective software as needed to provide capabilities for the full range of products used by the voting system.

**Test Assertions**

**TA752a-1:** IF a voting system uses a public telecommunications network THEN that voting system SHALL implement protections against external threats.

**TA752a-1-1:** IF a voting system uses a public telecommunications network THEN that voting system SHALL account for known vulnerabilities to which commercial products used in the voting system may be susceptible.

**TA752b-1:** IF a voting system uses a public telecommunications network THEN that voting system SHALL provide documentation that clearly identifies all COTS hardware products used in the development of the voting system.

**TA752b-2:** IF a voting system uses a public telecommunications network THEN that voting system SHALL provide documentation that clearly identifies all COTS hardware products used in the operation / deployment of the voting system.

**TA752b-3:** IF a voting system uses a public telecommunications network THEN that voting system SHALL provide documentation that clearly identifies all COTS software products used in the development of the voting system.

**TA752b-4:** IF a voting system uses a public telecommunications network THEN that voting system SHALL provide documentation that clearly identifies all COTS software products used in the operation / deployment of the voting system.

**TA752b-5:** IF a voting system uses a public telecommunications network THEN that voting system SHALL provide documentation that clearly identifies all communications services products used in the development of the voting system.

**TA752b-6:** IF a voting system uses a public telecommunications network THEN that voting system SHALL provide documentation that clearly identifies all communications services products used in the operation / deployment of the voting system.

**TA752b-7:** IF a voting system uses a public telecommunications network THEN that voting system SHOULD document the above information in Common Configuration Enumeration (CCE) format (https://nvd.nist.gov/CCE/Index.aspx).

**TA752b-8:** This documentation, provided by the voting system, SHALL include, but not be limited to, the following items:

* Operating systems
* Communications routers
* Modem drivers
* Dial-up networking software

**TA752bi-1:** This documentation, provided by the voting system, SHALL identify the name used for each such component.

**TA752bi-2:** This documentation, provided by the voting system, SHALL identify the vendor used for each such component.

**TA752bi-3:** This documentation, provided by the voting system, SHALL identify the version used for each such component.

**TA752ci-1:** IF a voting system uses a public telecommunications network THEN that voting system SHALL use protective software at the receiving-end of all communications paths to detect the presence of a threat in a transmission.

**TA752cii-1:** IF a voting system uses a public telecommunications network THEN that voting system SHALL use protective software at the receiving-end of all communications paths to remove the threat from infected files.

**TA752cii-2:** IF a voting system uses a public telecommunications network THEN that voting system SHALL use protective software at the receiving-end of all communications paths to remove the threat from infected data.

**TA752ciii-1:** IF a voting system uses a public telecommunications network THEN that voting system SHALL use protective software at the receiving-end of all communications paths to prevent against storage of the threat anywhere on the receiving device.

**TA752civ-1:** IF a voting system uses a public telecommunications network THEN that voting system SHALL use protective software at the receiving-end of all communications paths to provide the capability to confirm that no threats are stored in system memory.

**TA752civ-2:** IF a voting system uses a public telecommunications network THEN that voting system SHALL use protective software at the receiving-end of all communications paths to provide the capability to confirm that no threats are stored in connected storage media.

**TA752cv-1:** IF a voting system uses a public telecommunications network THEN that voting system SHALL use protective software at the receiving-end of all communications paths to provide data to the system audit log indicating the detection of a threat.

**TA752cv-2:** IF a voting system uses a public telecommunications network THEN that voting system SHALL use protective software at the receiving-end of all communications paths to provide data to the system audit log indicating the processing performed.

**TA752d-1:** Manufacturers SHALL use multiple forms of protective software as needed in order to provide capabilities for the full range of products used by the voting system.

**TA752d-1-1:** In order to provide security protections for the full range of products, industry standard security technology MAY include:

1. firewalls,
2. network and/or host-based intrusion detection and prevention systems,
3. log management applications,
4. cryptographic suites.

**Operational Definitions**

**Telecommunications** – Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means. (SOURCE: CNSSI-4009)

**Public telecommunications** – Is a form of telecommunications which includes electrical, optical, and wireless transmission using public telecommunications lines.