**Test Assertions for VVSG 1.1, Volume 1, Section 7.4.2**

**September 23, 2016**

**VVSG 1.1, Vol 1, Requirement 7.4.2:** **Protection Against Malicious Software**

1. Voting systems **shall** deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs.
2. Manufacturers **shall** develop and document the procedures to be followed to ensure that such protection is maintained in a current status.

**Test Assertions**

**TA742a-1:** The voting system manufacturer SHALL develop a threat model that documents all possible attacks against the voting system.

**TA742a-1-1:** The threat model SHALL include file viruses.

**TA742a-1-2:** The threat model SHALL include macro viruses.

**TA742a-1-3:** The threat model SHALL include worms.

**TA742a-1-4:** The threat model SHALL include Trojan Horses.

**TA742a-1-5:** The threat model SHALL include logic bombs.

**TA742a-1-6:** The threat model SHALL include Rootkits.

**TA742a-2:** Voting systems SHALL deploy protection against each and every threat identified in the threat matrix.

**TA742b-1:** Voting System manufacturers SHALL develop procedures, and include them in the TDP, that must be followed to ensure that the protection for each threat is maintained and kept up-to-date.

**TA742b-2:** Voting System manufacturers SHALL document procedures, and include them in the TDP, that must be followed to ensure that the protection for each threat is maintained and kept up-to-date.

**TA742b-3:** The protection for each threat SHALL be maintained in an up-to-date status.

**Operational Definitions**

**Logic Bomb –** A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

**Macro Virus –** A macro virus is a computer virus that is written in a macro language, which enables a program to work and instigates a designated group of actions and commands. When these actions and commands are replaced by a virus, this can cause significant harm to a computer.

**Rootkit –** Stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.

**Threat Model –** a formal description for a set of possible attacks and their remedies

**Trojan Horse –** A Trojan horse, or Trojan, in computing is a generally a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm.

**Virus –** A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".

**Worm –** A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program.