VVSG 2007 System Integrity Management Requirements

This information is based on the requirements found at:
http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/2007-VVSG.pdf

5.5 System Integrity Management

This chapter is a guideline for securely deploying and maintaining voting system electronic devices across all system modes of voting. It is inclusive of platform security configuration including network interfaces. In many ways, security of the electronic devices is subject to the current voting system state. Perhaps more importantly, the voting system state is an indicator of who requires access to any given device. This factor significantly influences security measures.

There are some similarities between voting machines and gaming machines. As a method of assuring completeness of requirements, the Nevada Gaming Commission's [NGC06] technical standards on gaming machines were consulted for applicability.

5.5.1 Electronic devices

Electronic device requirements are minimum safeguards for voting platforms once the platform is deployed.

5.5.1-A Protecting the integrity of the boot process

Requirement:	Before boot up or initialization, electronic devices SHALL verify the integrity of the components used to boot up or initialize the electronic device using a tamper-resistant hardware module.
Applies to:	Electronic device
Test Reference:	Part 3:4.5 "Source Code Review", 5.2 "Functional Testing"
Discussion:	A tamper-resistant hardware module, such as a trusted platform module (TPM), can be used to store the cryptographic software reference information of the components that are required to boot the electronic device. The specific types of components required for booting vary by device type, but examples of these components are boot loader files and kernel modules on a PC. The device will not boot if the files have been modified or the boot storage has been removed from the voting system. This requirement augments [VVSG2005] I.7.4.6 by explicitly requiring integrity checking of components used to boot up or initialize an electronic device.
Source:	[VVSG2005] I.7.4.6-a, I.7.4.6-b, I.7.4.6-e
Principle(s)/ Guideline(s):	*Security: System Integrity* *The voting system maintains and verifies the integrity of software, firmware, and other critical components.* **Justification:** The requirement discusses verifying the integrity of voting system components.

5.5.1-B Integrity verification of binaries before execution or memory load

Requirement:	Electronic devices SHALL verify the integrity of binaries (e.g., device drivers, library

	files, applications, and utilities) using a tamper-resistant hardware module and confirm that the binaries have been specified by the manufacturer as being required for the current voting system state before they are executed or loaded into memory.
Applies to:	Electronic device
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	Verifying the integrity of binaries prevents modified binaries, such as those infected with malware or inadvertently corrupted by a software or hardware failure, from being executed or loaded. A tamper-resistant hardware module, such as a trusted platform module (TPM), can be used to store the cryptographic software reference information to be used to verify integrity and voting system state specifications. Binaries that are not required for a particular state should not be executed while a device is in that state. The potential impact of permitting the binaries’ execution varies depending on the state and the nature of the binaries – examples include altering or disrupting the functionality of the system. This requirement augments [VVSG2005] 7.4.6-b by mandating cryptographic software reference information as a mechanism for verifying the integrity of binaries, by specifying that binary integrity checking must be performed before binaries are executed or loaded into memory, and by requiring that only binaries specified as required for a particular voting system mode may be executed or loaded into memory during that mode.
Source:	[VVSG2005] I.7.4.6-b
Principle(s)/ Guideline(s):	*Security: System Integrity* *The voting system maintains and verifies the integrity of software, firmware, and other critical components.* **Justification:** The requirement discusses verifying the integrity of software components.

5.5.1-C Sandboxing applications

Requirement:	Electronic devices that support multi-processing architectures SHALL logically separate each application such that applications can only access resources necessary for normal functionality.
Applies to:	Electronic device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Logically separating applications such that only required resources can be accessed is often referred to as “sandboxing” an application. It is meant to ensure that subversion of an application’s native security will not result in access beyond normal resources.
Source:	[NIST05] Security Control AC-6, SC-2
Principle(s)/ Guideline(s):	*Security: System Integrity* *The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports and by using other technical controls.* *sys* *The voting system maintains and verifies the integrity of software, firmware, and other critical components.*

	Justification: By limiting access to resources this limits the attack surface by reducing data paths.

5.5.2 Removable media

While removable media is used in a number of precincts as a part of the voting process, removable media is sometimes a mechanism to propagate malicious code or exfiltrate data from electronic devices. For this reason, removable media requirements focus on enabling use of removable media, while protecting the electronic device.

5.5.2-A Restricting the use of removable media

Requirement:	Electronic devices SHALL disable all removable media interfaces that are not needed for each voting system state.
Applies to:	Electronic device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Disabling a removable media interface prevents access to removable media connected to that interface. An interface may be disabled through physical or logical means. Physically securing the removable media interface prevents the insertion and removal of removable media. Logically securing the removable media interface prevents the use of removable media inserted into the electronic device, and also prevents the removal of removable media from the electronic device (e.g., ejecting a CD or dismounting a USB flash drive). See Chapter 14: Physical Security for requirements related to physical security.
Source:	[NIST05] Security Control AC-3, AC-6, MP-2
Principle(s)/ Guideline(s):	*Security: System Integrity* *The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports and by using other technical controls.* **Justification:** By limiting access to resources this limits the attack surface by reducing data paths.

5.5.3 Backup and recovery

Backup and recovery requirements describe minimum authorization, auditing, and protective measures, without regard to specific media.

5.5.3-A Restricting backup and restore capabilities

Requirement:	Electronic devices other than EMSs SHALL NOT provide backup or restore capabilities.
Applies to:	Electronic device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Backup and restore capabilities introduce security holes into systems because backup operations could disrupt system functionality (e.g., locking files that the system needs to access) or give an attacker access to the system's data, and restore operations could alter system functionality or data (e.g., replacing

	existing files with previous versions). Therefore, use of backup and restore capabilities should be minimized. EMSs are permitted, but are not required, to have backup and restore capabilities because of the types of information they store.
Source:	[NIST05] Security Control SC-2
Principle(s)/ Guideline(s):	*Security: Data Protection* *The voting system protects sensitive data from unauthorized access, modification, or deletion.* **Justification:** By disallowing electronic devices (other than EMSs) from providing backup/restore, this prevents unauthorized access as mentioned in this guideline. *Security: System Integrity* *The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports and by using other technical controls.* **Justification:** Limiting capabilities within the EMS can limit the attack surface.

5.5.3-B Restricting the performance of backups and restores

Requirement:	EMSs that provide backup or restore capabilities SHALL only permit backup and restore operations while not in the Activated state.
Applies to:	EMS
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Backup and restore operations should not be performed while EMSs are in the Activated state because backup operations could disrupt system functionality (e.g., locking files that the system needs to access) and restore operations could alter system functionality, vote data, etc.
Source:	[NIST05] Security Control SC-2
Principle(s)/ Guideline(s):	*Security: Data Protection* *The voting system protects sensitive data from unauthorized access, modification, or deletion.* **Justification:** Ensuring the EMSs do not perform backups while in an Activated State may keep the data safe from disruption.

5.5.3-C Authenticity and integrity of backup information

Requirement:	EMSs that perform backups SHALL create digital signatures, message authentication codes, or hashes for their backups so that their authenticity and integrity can be verified in the future.
Applies to:	EMS
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement allows EMSs to verify the authenticity and integrity of backups before restoring them.
Source:	[NIST05] Security Control CP-9
Principle(s)/ Guideline(s):	*Security: System Integrity* *The voting system maintains and verifies the integrity of software, firmware, and other critical components.* **Justification:** The digital signatures, message authentication codes, or hashes are

	used to maintain integrity and allow for integrity checking of the EMS backups.

5.5.3-D Verifying backup authenticity and integrity

Requirement:	EMSs that perform restores SHALL verify the authenticity and integrity of backups before restoring them.
Applies to:	EMS
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[NIST05] Security Control CP-10
Principle(s)/ Guideline(s):	*Security: System Integrity* *The voting system maintains and verifies the integrity of software, firmware, and other critical components.* **Justification:** The EMS verifies the integrity before restoring. This aligns with this guideline.

5.5.4 Malicious software protection

As described in the National Institute of Standards and Technology Special Publication 800-83 [NIST05a], malicious software, also known as malicious code and malware, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim. For a number of reasons, electronic devices associated with voting systems may be targeted by malware. Malware is inclusive of viruses, worms, Trojan horses, and malicious mobile code, as well as combinations of these, known as blended attacks. Malware also includes attacker tools such as backdoors, rootkits, and keystroke loggers. Given this understanding of malware, requirements focus on preventing occurrences of malware on electronic devices.

5.5.4-A Installing malware detection software

Requirement:	EMSs SHALL use malware detection software to protect themselves from common known malware that targets their operating systems, services, and applications.
Applies to:	EMS
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Off-the-shelf malware detection software, such as antivirus software, anti-spyware software, and rootkit detection, can identify common known malware that attempts to infect an electronic device, as well as identify infections on the device. The scope of this requirement is limited to EMSs because they should have the required resources to use off-the-shelf malware detection software and also because there should be off-the-shelf malware detection software available for their platforms. For many other electronic devices, neither of these conditions is true; also, some platforms do not have common known malware threats, so malware detection software would not be useful. This requirement augments [VVSG2005] I.7.4.2 by specifying installation of malware detection/scanning software.

Source:	[VVSG2005] I.7.4.2
Principle(s)/ Guideline(s):	*Security: Detection/Monitoring* *The voting system employs mechanisms to protect against malware.* **Justification:** The EMS protects against malware by employing malware detection software.

5.5.4-B Malware detection software signature updates

Requirement:	EMSs SHALL provide a mechanism for updating the malware detection software with newer malware signatures.
Applies to:	EMS
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	As new malware threats are discovered, particularly threats specific to voting systems, the election management's malware detection software may need to be updated so that it can recognize and stop these threats. Many malware detection software products use the Internet by default to retrieve updates; since the use of the Internet by electronic devices is prohibited, another mechanism is needed to distribute updates, such as using a device on the local network to distribute updates, or manually distributing updates through read-only removable media. This requirement augments [VVSG2005] 7.4.2 by specifying the capability to update malware detection software with current malware signatures.
Source:	[VVSG2005] I.7.4.2
Principle(s)/ Guideline(s):	*Security: Detection/Monitoring* *The voting system employs mechanisms to protect against malware.* **Justification:** To continue to protect against malware the EMS must have a mechanism to update the malware detection software with new malware signatures.

5.5.4-C Scanning removable media for malware

Requirement:	EMSs SHALL run malware detection software against removable media to verify no common known malware is present before accepting any data from the removable media.
Applies to:	EMS
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This prevents the introduction of common known malware onto an electronic device from removable media. This requirement augments [VVSG2005] I.7.4.2 by specifying scanning of removable media for common known malware.
Source:	[VVSG2005] I.7.4.2
Principle(s)/ Guideline(s):	*Security: Detection/Monitoring* *The voting system employs mechanisms to protect against malware.* **Justification:** The EMS protects against malware by using malware detection software on removable media.

5.5.4-D Periodic malware scanning

Requirement:	EMSs SHALL be scanned for common known malware at least once every 24 hours during operation, including malware specifically targeted at voting

	systems.
Applies to:	EMS
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This identifies any current infections on the electronic device caused by common known malware. This requirement augments [VVSG2005] I.7.4.2 by specifying scanning of removable media for common known malware.
Source:	[VVSG2005] I.7.4.2
Principle(s)/ Guideline(s):	*Security: Detection/Monitoring* *The voting system employs mechanisms to protect against malware.* **Justification:** This requirement regulates how often the EMS is scanned for malware. The time intervals play a role in protecting against malware.

5.5.4-E Real-time malware scanning

Requirement:	EMSs SHALL perform real-time scanning for common known malware.
Applies to:	EMS
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This prevents files infected with common known malware from being executed or otherwise loaded within the electronic device. This requirement augments [VVSG2005] I.7.4.2 by specifying real-time scanning for common known malware.
Source:	[VVSG2005] I.7.4.2
Principle(s)/ Guideline(s):	*Security: Detection/Monitoring* *The voting system employs mechanisms to protect against malware.* **Justification:** This requirement discusses the type of scanning performed on the EMS. This scanning is used to protect against malware in real-time.