May 17, 2017

2007 VVSG Security Requirements Mapping

The VVSG Cybersecurity Working Group is charged with identifying principles, guidelines, requirements, and test assertions for the next generation VVSG, known as VVSG 2.0. The requirements contained within the 2007 VVSG will be the foundation of the forthcoming VVSG 2.0. This document identifies the relevant sections of the relevant portions of the 2007 VVSG to undergo review, maps these sections to the principles and guidelines, and identifies open areas.

Relevant Requirements

Besides the introductory information, the 2007 VVSG contains 3 parts: voting equipment, documentation, and testing methods. The portions of the 2007 VVSG pertinent to the VVSG Cybersecurity Working Group are principally contained within the voting equipment volume, although relevant requirements do exist in the remaining 2 volumes. These are all listed below:

Part 1 - Voting Equipment

Heading Number	**Section Heading**
2.7	Software Independence
4	Security and Audit Architecture
4.1	Overview
4.2	Requirements for Supporting Auditing
4.3	Electronic Records
4.4	Independent Voter-Verifiable Records
5	General Security Requirements
5.1	Cryptography
5.2	Setup Inspection
5.3	Software Installation
5.4	Access Control
5.5	System Integrity Management
5.6	Communications Security
5.7	System Event Logging
5.8	Physical Security for Voting Devices

Part 2 – System Documentation

Heading Number	**Section Heading**
3.5	System Security Specification

Part 3 – Testing Methods

Heading Number	**Section Heading**
4.5.2	Security Control Code Review

5.4	Open Ended Vulnerability Testing

High-level Principles & Guidelines Mapping

The principles can generally be mapped to the following sections of 2007 VVSG requirements.

Principle	**Requirement**	**Section Heading**
Auditability	Part 1 - 2.7	Software Independence
Auditability	Part 1 - 4.1	Overview
Auditability	Part 1 - 4.2	Requirements for Supporting Auditing
Auditability	Part 1 - 4.3	Electronic Records
Auditability	Part 1 - 4.4	Independent Voter-Verifiable Records
Data Protection	Part 1 - 5.1	Cryptography
	Part 1 - 5.2	Setup Inspection
Software Integrity	Part 1 - 5.3	Software Installation
Access Control	Part 1 - 5.4	Access Control
Software Integrity	Part 1 - 5.5	System Integrity Management
Data Protection	Part 1 - 5.6	Communications Security
Detection & Monitoring	Part 1 - 5.7	System Event Logging
Physical Security	Part 1 - 5.8	Physical Security for Voting Devices
	Part 2 – 3.5	System Security Specification
	Part 3 – 4.5.2	Security Control Code Review
*	Part 3 – 5.4	Open Ended Vulnerability Testing

This mapping is not down to the guideline level, but generally shows that requirements at least exist for each principle identified by the Working Group. The *Setup Inspection*, *Security Control Code Review*, and *System Security Specification* 2007 VVSG sections do not have corresponding principles, potentially signaling superfluous requirements or an omission by the Cybersecurity Working Group. The *Security Control Code Review* could be viewed as out of scope, depending on how it's tested since it may be a software requirement. The *Open Ended Vulnerability Testing* section is a test method that should work to help validate that many, if not all, of the principles are built into the voting system.

Detailed Principles & Guidelines Mapping

The following maps the more specific guidelines to requirements. Each principle and guideline are introduced, mapped to requirements, and then a brief analysis is given as to the state of the 2007 VVSG requirements meeting the principles and guidelines.

Principle: Auditability
The voting system is auditable and enables evidence-based elections.

Guideline	Section Number	Section Heading
An undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results.	2.7	Software Independence
The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities.	4	Security & Audit Architecture
	4.2	Requirements for Supporting Auditing
	4.3	Electronic Records
	4.4	Independent Voter-Verifiable Records
	5.7	System Event Logging
Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.	4.3.1-C	Cryptographic protection of records from voting devices
	5.7.3	Protection logs from accidental or deliberate modification
	6.4.1.7-C	Prevent tampering with data
The voting system supports efficient audits.		

Analysis of the Auditability Principle & Guidelines
The Cybersecurity Working Group has already identified that new types of audits that need to be defined and included - risk limiting audits and image interpretation audits. These will likely need to be added to Part 1, Section 4. New requirements are needed to address the "efficient audits" guideline. An external issue exists, as many of the auditing requirements necessitate the addition of specific information being placed into a voting system's Cast Vote Record (CVR). The CVR is being developed by another Working Group who may choose not to add this Group's information to the data structure.

Principle: Ballot Secrecy
The voting system protects the secrecy of voters' ballot selections.

Guideline	Section Number	Section Heading
Ballot secrecy is maintained throughout the voting process.	3.2.3.1-A	System support of privacy
	3.2.3.1-A.2	Auditory privacy
	3.2.3.1-A.4	No receipts
	7.5.1.2	Secrecy of the ballot
Records produced by the voting system do not reveal how a voter voted.	4.4.2.6-B	VVPAT, paper-roll, privacy during printer errors
	5.7.1-A	Event logging mechanisms requirement
	5.7.1-C	Voter privacy and ballot secrecy requirement

Analysis of the Ballot Secrecy Principle & Guidelines
Ballot secrecy requirements are spread throughout the 2007 VVSG with no central section focused on ballot secrecy. The most applicable section is Part 1 Section 3.2.3 under the General Usability Requirements. Breaking this out ballot secrecy into its own section may be beneficial, although it may be a rather short section. Finally, there may be a need to separate tying a cast ballot to a specific voter (ballot secrecy) from voting process oriented personal attributes (privacy of personal information).

Principle: Access Control
The voting system authenticates administrators, users, devices and services before granting access to sensitive functions.

Guideline	Section Number	Section Heading
The voting system identifies users, roles and/or processes to which access is granted and the specific functions and data to which each entity holds authorized access.	5.4.1	General access control
	5.4.2	Access control identification

The voting system supports authentication mechanisms and allows administrators to configure them.	5.4.2-E	Access control configuration
	5.4.3	Access control authentication
Default access control policies enforce the principles of least privilege.	5.4.1-E	Minimum permissions default
	5.8.2	Physical port and access least functionality

Analysis of the Access Control Principle & Guidelines

The 2007 VVSG contains a fairly robust section on the topic of Access Control, going as far as to mandate access control states (requirement 5.4.1-C) and compliance with the Role Based Access Control standard if RBAC is being used. The primary least privilege requirement (5.4.1-E) needs a better specific requirement, or needs to be more clearly stated. The access control section is quite detailed in some areas and may be able to be rewritten to be less implementation specific.

Principle: Physical Security

The voting system prevents or detects attempts to tamper with voting system hardware.

Guideline	Section Number	Section Heading
Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence.	5.8.6-A	Secure ballot box requirement
	5.8.4-B	Physical port tamper evidence requirement
	5.8.6-A	Secure ballot box requirement
Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing.	5.8.2	Physical port and access least functionality
	5.8.5	Door cover and panel security

Analysis of the Physical Security Principle & Guidelines
The Physical Security section contains the necessary requirements to fulfill the guidelines, with the exception of tamper detection requirements for paper ballots. If one exists it was overlooked and should be made more clear.

Principle: Data Protection
The voting system protects sensitive data from unauthorized access, modification, or deletion.

Guideline	Section Number	Section Heading
Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.	4.3.1-C	Cryptographic protection of records from voting devices
The source and integrity of electronic tabulation reports are verifiable.	4.3.1-C	Cryptographic protection of records from voting devices
	4.3.4	Digital signature verification
	4.3.5	Digital signature verification
	5.5.1-C	Sandboxing applications
All cryptographic algorithms are public, well-vetted, and standardized.	5.1.1	Cryptographic module validation
Voting systems protect the integrity, authenticity and confidentiality of sensitive data transmitted over all networks.	5.6.2-C	Implementing integrity of data in transit

Analysis of the Data Protection Principle & Guidelines
Although the 2007 VVSG requirements are a significant improvement over the 2005 VVSG, many requirements may need to be redrafted to specifically address items in many of the Data Protection guidelines, specifically the first two. Protecting information stored on the voting system needs to be revisited and stated in a more clear and concise manner.

The Cybersecurity Working Group may wish to discuss how to accommodate other domain-specific cryptographic algorithms that do not fit under the FIPS 140-2 umbrella. Currently, wireless is banned and the group may want to revisit that. Transmission of data makes the distinction between official and unofficial results, but the EAC decided to treat all transmitted

results as official per **RFI 2012-02 -- EAC Decision on Transmission of Results (Official and Unofficial Results)**. Interestingly, there seems to be a need for a solid requirement for confidentiality of transmitted information. If one exists it was overlooked and should be made more clear.

Principle: Software Integrity
Voting systems prevent the unauthorized installation or modification of firmware, software, and critical configuration files.

Guideline	Section Number	Section Heading
Only software that is digitally signed by the appropriate authorities is installed on the voting system.	5.5.1-A	Protecting the integrity of the boot process
	5.5.1-B	Integrity verification of binaries before execution or memory load
	5.2.1.2-A	Software integrity verification
	5.2.1.1-A	Voting device software identification
The authenticity and integrity of software updates are verified by the voting system prior to installation and authorized by an administrator.	5.3-C	Authentication to install software election-specific software
	5.5.4-B	Malware detection software signature updates

Analysis of the Software Integrity Principle & Guidelines
The first guideline could simply be made into a requirement to make the digital signature requirement for installed software more robust. There is no requirement to write protect storage areas, such as SSD or HDD, after an installed program has its signature verified. Although two requirements are cited for the second guideline, they are only tangentially related and a stronger requirement for verifying system updates is needed.

Principle: Detection & Monitoring
The voting system provides mechanisms to detect and remediate anomalous or malicious behavior.

Guideline	Section Number	Section Heading
Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.	5.7.2-C	Log format requirement
	5.7.1-E.1	Minimum logging disabling requirement
The voting system generates, stores, and reports to the user	3.2.2.1-F	Notification of ballot casting failure (DRE)

or election official, all error messages as they occur.		
	3.2.2.2-F	Notification of ballot casting failure (PCOS)
Voting systems employ mechanisms to protect against malware.	5.5.4	Malicious software protection
If the voting system contains networking capabilities, it employs appropriate modern defenses against network-based attacks.	5.5.4	Activation device, connects to router/firewall

Analysis of the Detection & Monitoring Principle & Guidelines
While many of the guidelines within this principle are addressed, more explicit requirements could be generated to meet the spirit of these guidelines. Specifically, requirements need to be drafted about notifying all error messages to the user as they occur and deploying modern network defenses. Voting systems are embedded systems, and generally deploying malware detection mechanisms on embedded systems is a little odd. It may be more reasonable to specify malware detection mechanisms on ancillary laptops or PCs managing and configuring voting systems, such as election management systems.

Open Items

Both vulnerability scanning and network scanning could be added as test methods in Part 3. It is possible that they could be incorporated within a new principle labeled Reduced Attack Surface, or modify the Software Integrity guideline to be titled System Integrity. This would include scanning the system for known vulnerabilities and misconfigured ports and services. It seems reasonable that voting systems should not be certified with known vulnerabilities. Additionally, since OEVT was a controversial topic back in 2007, the Cybersecurity Working Group may need to revisit it again, and update its title to be called the generally accepted term of Penetration Testing.

The important topics of risk management and timely software / security updates are not included within the VVSG, but they may be more appropriately addressed by either the EAC's Certification Program Manual or their Election Management Guidelines. Finally, remote Electronic Ballot Marking and Ballot Return requirements are not included, and likely should not be treated as DREs with other public telecommunications capabilities.