VVSG 2.0 Security Requirements

Gema Howell
September 2019

How did we get here?

Baseline requirements:	• VVSG 1.1 • 2007 VVSG Recommendations
New Security Innovations:	• General Industry Practices • Voting System Specific Practices
VVSG Cybersecurity Public Working Groups	• Feedback and input from public working group calls

Where to find the Security Requirements?

- The majority of the security requirements fall under Principles 9 through 15
- A few requirements that cover software security are under Principle 2
- Some areas of overlap with other principles

	Principle
9	Auditable
10	Ballot Secrecy
11	Access Control
12	Physical Security
13	Data Protection
14	System Integrity
15	Detection and Monitoring

	Principle
2	High Quality Implementation

Principle 9 – Auditable Overview

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

- 4 Guidelines
- 40 Requirements
- Focuses on machine support for post-election audits

Guideline 9.1 –Overview

An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

- Requirements for software independence
  - **9.1.1-A – Software independent**
  - **9.1.1-B – Paper-based or cryptographic E2E system**
  - 9.1.1-C –Mechanism documentation
  - 9.1.2-A – Tamper evident records
  - 9.1.2-B – Tamper-evident record creation
  - **9.1.3-A – Records for voter verification**
  - 9.1.3-B – Identification of errors
  - 9.1.3-C – Ballot error correction
  - 9.1.3-D – Voter reported errors
  - **9.1.4-A – Auditor verification**
  - 9.1.4-B – Auditable with compromised software, firmware, or hardware
  - 9.1.5-A – Paper record production
  - 9.1.5-B – Paper record retention
  - 9.1.5-D – Matching selections
  - 9.1.6-A – Cryptographic E2E transparency
  - **9.1.6-B – Cryptographic verification**
  - 9.1.6-C – Ballot receipt
  - 9.1.6-A – Number of ballots to check
  - 9.1.6-B – No fixed margin of error
  - 9.1.6-C – Random number generation

Guideline 9.2 –Overview

The voting system produces readily available 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.

- Requirements to provide all the necessary documents and artifacts to perform an audit
  - 9.2-A – Compliance audit procedures
  - **9.2-B – General post-election audit procedures**
  - **9.2-C – Generating CVRs**
  - 9.2-D – Reporting intermediate results
  - 9.2-E – Reporting unusual audit events
  - 9.2-F – Reporting format
  - **9.2-G – Ballot count**

Guideline 9.3 –Overview

Voting system records are resilient in the presence of intentional forms of tampering and accidental errors

- Requirements to protect the audit records
  - 9.3-A – Data protection requirements for audit records

Data Protection Guidelines

- 13.1 - The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.
- 13.2 - The source and integrity of electronic tabulation reports are verifiable.

Guideline 9.4 –Overview

The voting system supports efficient audits.

- Requirements to include support for audit efficiency
  - 9.4-A – Efficient compliance audit
  - **9.4-B – Efficient risk-limiting audit**
  - **9.4-C – Unique ballot identifiers**
  - **9.4-D – Multipage ballots**

Principle 10 – Ballot Secrecy Overview

The voting system protects the secrecy of voters' ballot selections.

- 2 Guidelines
- 20 Requirements
- New section that distinguishes ballot secrecy from voter privacy

Guideline 10.1 –Overview

Ballot secrecy is maintained throughout the voting process

- Requirement to cover the prevention of "*accepting, processing, storing, and reporting*" voter identity throughout the voting system and voting process
  - **10.1-A – System use of voter information**

Guideline 10.2 –Overview

The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.

- Requirements to prevent the association of a voter's identity to their ballot selections
  - 10.2.1-A – Direct voter associations
  - **10.2.1-B – Indirect voter associations**
  - 10.2.1-C – Use of indirect voter associations
  - 10.2.1-D – Election worker selection of indirect associations
  - 10.2.1-E – Isolated storage location
  - 10.2.1-F – Confidentiality for indirect association
  - **10.2.2-A – Identifiers used for audits**
  - 10.2.2-B – No voter record order information
  - 10.2.2-C – Identifying information in voter record file names
  - 10.2.2-D – Non-memorable identifiers and associations
  - **10.2.2-E – Aggregating and ordering**
  - 10.2.3-A – Least privilege access to store
  - 10.2.3-B – Limited access
  - 10.2.3-C – Authorized access
  - 10.2.3-D – Digital voter record access log
  - **10.2.4-A – Voting information in receipts**
  - **10.2.4-B – Ballot secrecy for receipts**
  - 10.2.4-C – Logging of ballot selections
  - 10.2.4-D – Activation device records

Principle 11 – Access Control Overview

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

- 5 Guidelines
- 26 Requirements
- Significant updates made to strengthen monitoring of access and ensure critical operations are performed by authorized users

Guideline 11.1 – Overview

Access privileges, accounts, activities, and authorizations are logged, monitored, and reviewed periodically and modified as needed.

- Requirements for logging access within the voting system.
  - **11.1-A – Logging activities and resource access**
  - 11.1-B – Voter information in log files
  - **11.1-C – No disabling logging**
  - 11.1-D – On-demand access to logs

Guideline 11.2 – Overview

The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

- Requirements for managing access based on users, functions, and voting stage.
  - 11.2.1-A – Ensuring authorized access
  - 11.2.1-B – Modifying authorized user lists
  - **11.2.1-C – Access control by voting stage**
  - 11.2.1-D – Access control configuration
  - **11.2.1-E – Administrator modified permissions**
  - 11.2.1-F – Authorized assigning groups or roles
  - **11.2.2-A – Role-based access control standard**
  - **11.**2.2-B – Minimum groups or roles
  - **11.2.2-C – Minimum group or role permissions**
  - 11.2.2-D – Applying permissions

Guideline 11.3 – Overview

The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

- Requirements for authentication mechanisms:
  - 1.3.1-A – Access control mechanism application
  - **11.3.1-B – Multi-factor authentication for critical operations**
  - **11.3.1-C – Multi-factor authentication for administrators**
  - 11.3.2-A – Username and password management
  - **11.3.2-B – Password complexity**
  - 11.3.2-C – Minimum password complexity
  - 11.3.2-D – Usernames within passwords

Guideline 11.4 – Overview

Default access control policies enforce the principles of least privilege and separation of duties.

- Requirements align directly with the guideline
  - **11.4-A – Least privilege for access policies**
  - **11.4-B – Separation of duties**

Guideline 11.5 – Overview

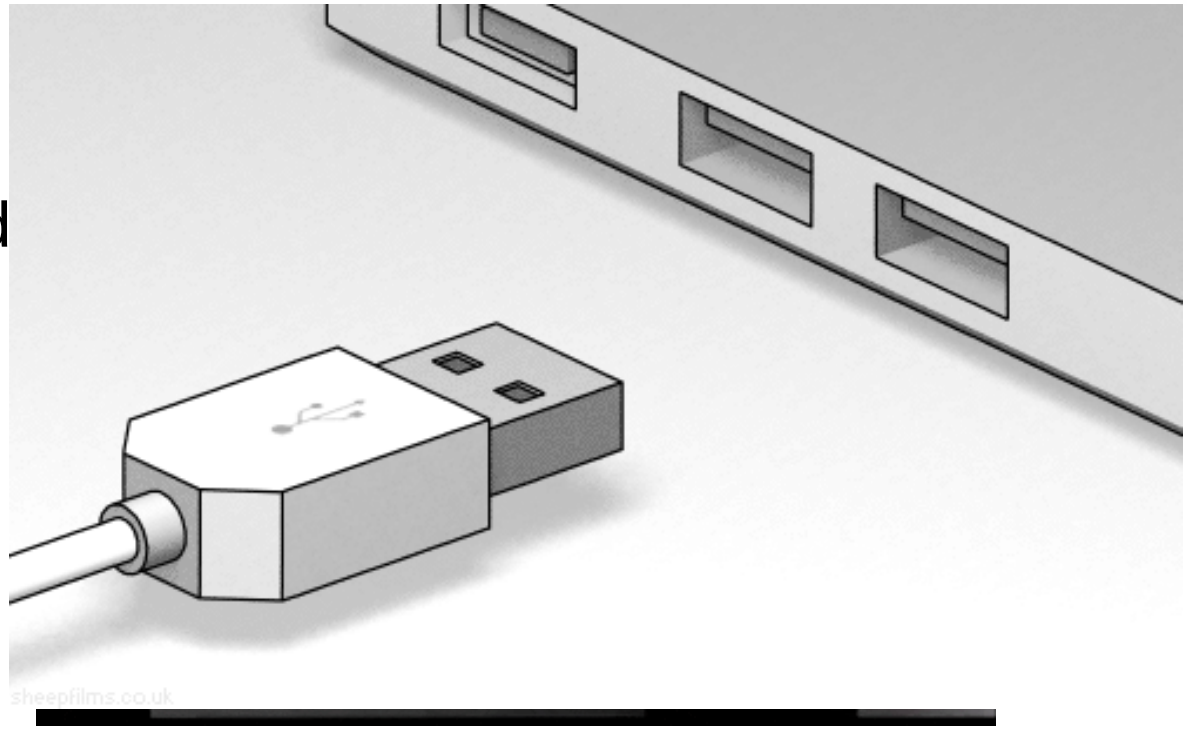
Logical access to voting system assets are revoked when no longer required.

- Requirements for timed access to the voting system and lockout options.
  - **11.5-A – Access time period**
  - **11.5-B – Account lockout**
  - 11.5-C – Lockout time duration

Principle 12 – Physical Security Overview

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

- 2 Guidelines
- 14 Requirements
- Mostly unchanged



Guideline 12.1 – Overview

The voting system supports mechanisms to detect unauthorized physical access.

- Requirements to control and detect physical access to the voting system
  - 12.1-A – Unauthorized physical access
  - 12.1-B – Unauthorized physical access alarm
  - 12.1-C – Disconnecting a physical device
  - **12.1-D – Logging of physical connections and disconnections**
  - 12.1-E – Logging door cover and panel status
  - **12.1-F – Secure containers**
  - 12.1-G – Secure physical locks
  - 12.1-H – Secure locking system key
  - **12.1-I – Backup power for power-reliant countermeasures**

Guideline 12.2 – Overview

The voting system only exposes physical ports and access points that are essential to voting operations.

- Requirements focus on exposed physical ports
  - 12.2-A – Physical port and access least functionality
  - 12.2-B – Physical port auto-disable
  - **12.2-C - Physical port restriction**
  - 12.2-D – Disabling ports
  - **12.2-E – Logging enabled and disabled ports**

Principle 13 – Data Protection Overview

The voting system protects sensitive data from unauthorized access, modification, or deletion.

- 4 Guidelines
- 17 Requirements
- Protection of election artifacts
- No hardware security requirements (e.g., TPM)

Guideline 13.1 – Overview

The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

- Requirements for authorized modifications and integrity protection of voting system data
  - **13.1.1-A – Authentication to access configuration file**
  - 13.1.1-B – Authentication to access configuration file on EMS
  - 13.1.1-C – Authentication to access configuration file for network appliances
  - **13.1.2-A – Integrity protection for election records**
  - 13.1.2-B – EMS integrity protection for election records

Guideline 13.2 – Overview

The source and integrity of electronic tabulation reports are verifiable.

- Requirements for verifying the integrity of voting system data
  - 13.2-A – **Signing stored electronic voting records**
  - 13.2-B – Signing electronic voting records prior to transmission
  - **13.2-C – Cryptographic verification of electronic voting records**

Guideline 13.3 – Overview

All cryptographic algorithms are public, well-vetted, and standardized.

- Requirements for the cryptographic algorithms used within the voting system
  - **13.3-A – Cryptographic module validation**
  - **13.3-B– E2E cryptographic voting protocols**
  - 13.3-C – Cryptographic strength
  - 13.3-D – MAC cryptographic strength
  - 13.3-E – Key management documentation

Guideline 13.4 – Overview

The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.

- Requirements for protecting transmitted data
  - **13.4-A – Mutual authentication of endpoints**
  - **13.4-B – Confidentiality protection for transmitted data**
  - **13.4-C – Integrity protection for transmitted data**
  - 13.4-D – Verification of election data

Principle 14 – System Integrity Overview

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

- 4 Guidelines
- 30 Requirements
- New section of the VVSG to include strategies and techniques to protect the voting system as a whole

Guideline 14.1 – Overview

The voting system uses multiple layers of controls to provide redundancy against security failures or vulnerabilities.

- Requirements discuss how to identify the necessary controls
  - **14.1-A – Risk assessment documentation**
  - **14.1-B – Addressing and accepting risk**
  - 14.1-C – System security architecture description
  - 14.1-D – Procedural and operational security

Guideline 14.2 – Overview

The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports, and by using other technical controls.

- Requirements focus on applying the technical controls
  - **14.2-A – Extraneous processes and services**
  - 14.2-B – Non-essential features
  - 14.2-C – Network status indicator
  - 14.2-D – Wireless network status indicator
  - 14.2-E – **Secure configuration and hardening**
  - 14.2-F – Secure configuration and hardening documentation
  - **14.2-G – Unused code**
  - 14.2-H – Exploit mitigation technologies within platform
  - 14.2-I – Application use of exploit mitigation technologies
  - 14.2-J – Importing software libraries
  - **14.2-K – Physical port restriction**
  - **14.2-L – Known vulnerabilities**
  - 14.2-M – List of known vulnerabilities

Guideline 14.3 – Overview

The voting system maintains and verifies the integrity of software, firmware, and other critical components.

- Requirements cover the integrity of the hardware, software, and other critical components
  - **14.3-A – Supply chain risk management strategy**
  - **14.3-B – Criticality analysis**
  - **14.3-B.1 –Bill of Materials**
  - **14.3.1-A – Cryptographic boot verification**
  - 14.3.1-B – Preventing of boot on error
  - 14.3.1-C – Logging of verification failure
  - 14.3.2-A – Installing software
  - **14.3.2-B – Software verification for installation**
  - 14.3.2-C – Software whitelisting
  - 14.3.2-D – Integrity protection for software whitelists

Guideline 14.4 – Overview

Software updates are authorized by an administrator prior to installation.

- Requirements for authorized installation
  - **14.4-A – Authenticated operating system updates**
  - **14.4-B – Authenticated application updates**
  - **14.4-C – Authenticated firmware updates**

Principle 15 – Detection and Monitoring Overview

The voting system provides mechanisms to detect anomalous or malicious behavior.

- 4 Guidelines
- 23 Requirements
- Moderately updated, including
  - Additional log types
  - Updatable and configurable detection and monitoring systems

Guideline 15.1 – Overview

Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

- Requirements for voting system event logging
  - **15.1-A – Event logging**
  - 15.1-B – Exporting logs
  - 15.1-C – Logging voter information
  - **15.1-D – Logging event types**
  - 15.1-E – Configuration file access log

Guideline 15.2 – Overview

The voting system generates, stores, and reports all error messages as they occur.

- Requirements for handling error messages
  - **15.2-A – Presentation of errors**
  - 15.2-B – Documenting error handling
  - **15.2-C – Logging errors**
  - 15.2-D – Creating error reports

Guideline 15.3 – Overview

The voting system employs mechanisms to protect against malware.

- 15.3-A – Software verification
- **15.3.1-A – Malware protection mechanisms**
- **15.3.1-B – Updatable malware protection mechanisms**
- 15.3.1-C – Documenting malware protection mechanisms
- 15.3.1-D – Notification of malware detection
- **15.3.1-E – Logging malware detection**
- 15.3.1-F – Notification of malware remediation
- 15.3.1-G – Logging malware remediation

Guideline 15.4 – Overview

A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.

- Requirements for protecting against network-based attacks
  - **15.4-A – Network architecture documentation**
  - 15.4-B – Telecommunications documentation
  - **15.4-C – Secure configuration documentation**
  - **15.4-D – Firewall and IDS**
  - 15.4-E – Least privilege
  - 15.4-F – Rule and policy updates

Open Areas in Cybersecurity Requirements

Indirect Voter Associations

Decision Points

- Are indirect voter associations necessary for certain voting systems?

Primary Concerns

- Violation of Ballot Secrecy Principle
  - The indirect voter association may be used to link a voter to their ballot selections

10.2 - The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.

Use Cases

- Handling conditional/provisional ballots within a paperless system

Indirect Voter Associations

Potential Mitigations

- External Paper Process
  - Not within VVSG - does not utilize the physical voting system and is administered by the local jurisdictions
- Airgap provisional machine
- IVA stored within the voting system and ballot is encrypted until eligibility is determined
  - When eligibility is confirmed, decrypt ballot and include in tabulation

Potential Benefit

- Increase voter privacy

Barcode and Encoding Schemes

Decision Points

- What information can be encoded or stored in barcodes?
- What does the voting system use to count the votes?

Primary Concerns

- Lack of Transparency, Violation of Ballot Secrecy
- Interoperability
- Auditability, Misinformation used for tabulation

Use Cases

- Ballot Activation
- Apply Usability Configurations
- Store Ballot Selections
- Transfer Tabulation Results
- Pre-voting
- Store Identifiers/Digital Signatures

Barcode and Encoding Schemes

Potential Mitigations

- Provide barcode standard and implementation information
  - Allow external review of barcode creation and contents
- Include human readable information for voter and auditor verification
- Ensure audits reference the human readable information

Potential Benefits

- Apply Accessibility settings
- Allow voters to vote at home using their own accessibility tools
- Support voters with disabilities, such as lack of sight or low vision
- Faster input of election data instead of manual input

Wireless Technology

Decision Points

- Is wireless technology appropriate for use within voting systems?
- Is the presence of wireless hardware appropriate within voting systems?

Primary Concerns

- Modification of voter choices
- Modification of results
- Eavesdropping
- Injection of malware
- Technical expertise required to apply secure configuration

Use Cases

- Print ballot from printer (Wi-Fi)
- Activation Card or token for authentication (NFC)
- Assistive technology, peripheral devices (e.g., mouse, keyboard) - (Bluetooth)

Wireless Technology

Potential Mitigations

- No wireless hardware; Physical connections only
  - Senate Intelligence Committee report – "*…at minimum, any machine purchased going forward should have a voter-verified paper trail and remove (or render inert) any wireless networking capability*.'
- Enable/disable wireless as needed
- Sophisticated security awareness and ongoing secure configuration management

Potential Benefits

- Automation and efficiency
  - Less hardware and potentially less physical setup
  - Configure and update multiple systems at the same time rather than manually configure each machine

Internet Connectivity

Decision Points

- Is internet connectivity appropriate for use within voting systems?
- Is the presence of internet connectivity technology appropriate within voting systems?

Primary Concerns

- Remote/Nation-state attacks
- Modification of results
- Eavesdropping
- Injection of malware
- Technical expertise required to apply secure configuration

Use Cases

- Remote Access Software
- Transmit election results (Cellular)
- Software Updates
- Remote ballot marking

Internet Connectivity

Potential Mitigations

- No internet connectivity
  - Use sneaker-net process
  - Telephone communication (call/text)
- Airgap at both ends of communication + Sophisticated security awareness and ongoing secure configuration management

Potential Benefits

- Assist with geographical restrictions

Cryptographic End-to-End (E2E) Verifiable Systems

Decision Points

- What's the right level of detail? - We want the requirements to be clear, but also allow for open innovation because we know that there is active research and development in this area
- What would the certification process look like for E2E systems?

Primary Concerns

- Unclear if current requirements are sufficient
- Assessment criteria &Adequate testing
- Dispute resolution
- Forward Secrecy – A flaw found after the election that reveals voters and selections

About E2E Verifiable Voting Systems

- A software independent option that can be paper-based or paperless.
- Allow voters to verify their ballot selections are correctly recorded and tabulated, without revealing their selections.
- Examples: Scantegrity, Scratch & Vote, Punchscan, Prêt à Voter (PaV)

Cryptographic End-to-End (E2E) Verifiable Systems

Potential Mitigations

- Require submission of documentation that includes:
  - Coverage of the E2E properties (Cast as Intended, Recorded as Cast, Preserve Ballot Secrecy, Tallied as Recorded)
  - Utilize an open standard and provide reference implementation information, including a sample verifier
  - Report of External Expert Evaluation

Potential Benefits

- Another software independent option
- Public verification feature
- Accessibility benefits if voters do not have to rely on paper

Questions?