Auditability – The voting system is auditable and provides a robust evidence trail to verify the election outcome.

- An undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results.
- 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.
- Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.
- The voting system efficiently supports a variety of audit types and methods throughout the election lifecycle.

Relevant Notes on changes to the *Auditability* Principle & Guidelines:

- Near complete re-write.
- Incorporated the "evidence trail" concept into the principle description, and producing records into other principles.
- Included the definition of software independence as the first guideline, although an explicit mention of paper may be viewed as necessary by the working group.
- Included the concept of "efficient audits", meant to ensure audits are easy to perform by the voting system and the election official.
- Highlighted the need to be able to support multiple types of audits, which may occur at the pre, during, and post-election process.

Ballot Secrecy - The voting systems protects the secrecy of voters' ballot selections.

- Cast vote records are stored in a manner that does not reveal how a particular voter voted.
- Voting systems preserve the secrecy of voter selections when transmitted over networks.

Relevant Notes on changes to the *Ballot Secrecy* Principle & Guidelines:

- Minor additions and deletions

Ballot Integrity - The voting system protects cast vote records from modification or deletion.

- Cast vote records must be stored in a manner that does not reveal how a particular voter voted.
- Voting systems preserve the integrity of voter selections when transmitted over networks.

Relevant Notes on changes to the *Ballot Integrity* Principle & Guidelines:

- The principle, as well as the principle description, is sound.
- The guidelines are copy and pasted from the Ballot Secrecy section.
- These concepts are supported by other areas such as Data Protection and Communications Security. Suggest deletion of the principle.

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

- 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.
- The voting system supports authentication mechanisms and allow administrators to configure them.
- Default access control policies enforce the principle of least privilege.

Relevant Notes on changes to the *Access Control* Principle & Guidelines:

- Minor additions and deletions.

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

- Any unauthorized physical access must leave physical evidence.
- Voting systems must only expose physical ports and access points that are essential to voting operations, testing, or auditing.

Relevant Notes on changes to the *Physical Security* Principle & Guidelines:

- Changed "have" to "expose" to allow for COTS products to be used, where unnecessary physical ports are likely built into the voting system hardware. It is common for these ports / interfaces to be physically sealed or covered in some fashion.
- Many in the working group felt that the voting system should prevent and/or detect unauthorized modification to the ballots. Should unauthorized access leave behind physical evidence? These concepts are currently unincorporated.
- Some in the working group felt as if an additional guideline about securing the ballot box would be necessary. This is currently unincorporated.

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

- Voting systems must prevent unauthorized access to or manipulation of configuration data, cast vote records, or audit records.
- The source and integrity of electronic tabulation reports must be verifiable.
- All cryptographic algorithms must be public, well-vetted, and standardized.

Relevant Notes on changes to the *Data Protection* Principle & Guidelines:

- Changed "vote data" to "cast vote records" to be more precise.

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

- The integrity of network communications must be cryptographically verified.
- Telecommunications must be encrypted and authenticated to protect against eavesdropping and data manipulation.

- Wireless channels must be encrypted and authenticated to protect against eavesdropping and data manipulation.

Relevant Notes on changes to the *Communications Security* Principle & Guidelines:

- Noted the need for cryptographic integrity protection mechanisms, which ensures integrity checks such as cyclic redundancy checks are not utilized.
- This may be able to be condensed into a single guideline.
- Removed the guideline on cryptographic algorithms, as it was duplicated from the Data Protection section.
- May want to include a guideline on the mechanism providing the cryptographic protection must be part of the voting system. For instance, can the voting system rely on a cellular network to provide confidentiality and integrity protection? The cellular network is not necessarily encrypted, and isn't part of the voting system

Software Quality - Voting system software is free of defects or vulnerabilities that may significantly disrupt the election, compromise election integrity, or violate ballot secrecy.

- Voting systems must be implemented using modern, high-level languages that provide common control constructs.
- Voting system software must adhere to published, credible coding conventions.
- Voting system software must be designed in a modular fashion.
- Voting system software source code must be documented.
- Voting system software must detect, avoid and prevent well-known types of errors.

Relevant Notes on changes to the *Software Quality* Principle & Guidelines:

- This principle and associated guidelines may be better suited for a different group. Ben Long of NIST is currently working in this area.
- Many of the guidelines are related to current VVSG requirements, and are style based.
- Since manual software review can be expensive, and this group is focusing on evidence trails and audits, it may be best to err on the side of fewer guidelines.

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

- Voting systems must provide methods to verify only authorized software is present on voting systems.
- The authenticity and integrity of software updates must be verified by the voting system prior to installation and authorized by an administrator.
- All software installed on voting system equipment must be identified.

Relevant Notes on changes to the *Software Integrity* Principle & Guidelines:

- No specific mention of whitelisting, although this seems like what the guidelines are hinting at.
- Unclear what "identified" software and equipment means.

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

- Voting system equipment records important activities through event logging mechanisms.
- System and election logs are protected from unauthorized modification or deletion.
- The voting system generates, stores, and reports to the user or election official, all error messages as they occur.
- Voting systems employ mechanisms to protect against malware.
- Voting systems monitor network traffic to identify and protect against attempted attacks.

Relevant Notes on changes to the *Detection & Monitoring* Principle & Guidelines:

- Does protecting system and election logs need to be duplicated here? The concept is present within the Data Protection principle.
- Does monitoring network traffic mean that a firewall is part of a voting system?

The following are concepts discussed with the Working Group that are not reflected within the principles and guidelines:

- Vulnerability management
- Timeliness of software updates
- Ensuring only supported software is used on the voting system
- Transparency of voting system software