System Event Logging Requirements Gap Analysis

An overarching goal of the next VVSG is to have each requirement mapped to a principle and its associated guidelines. During the mapping activity for the system event logging requirements, some requirements did not map to the current list of principles and guidelines. Others mapped directly to a principle and not any of the sub-guidelines. New guidelines may be necessary to completely map to all the requirements below.

Possible modifications for the System Event Logging requirements and/or guidelines include:

- The second Ballot Secrecy guideline should be amended to include other election artifacts, reading as follows:

  *Records **and other election artifacts** produced by the voting system do not reveal how a voter voted.*

  This ensures that election logs do not violate ballot secrecy.

  Requirement(s): 5.7.1-C

- Add "election artifacts (e.g., logs)" to the second and third Auditability guidelines, reading as follows:

  *The voting system produces records **and other election artifacts (e.g., logs)** 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 **and other election artifacts** are resilient in the presence of intentional forms of tampering and accidental errors.*

  The definition of voting system records, or election records may not necessarily include voting system event logs, or other types of logs. This ensures that logs are included within the scope of these guidelines.

  Requirement(s): 5.7.1-D.2,

- Add "accurately" to the second auditability guideline and the first detection and monitoring guideline, reading as follows:

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

This allows the timekeeping and other time-oriented requirements to be mapped to this auditability guideline.

Requirement(s): 5.7.1-D.1, 5.7.1-D.2, 5.7.1-D.3, 5.7.1-D.4, 5.7.1-D.5, 5.7.1-D.6

- There are some requirements in this section that would benefit from a guideline on record durability and retention. Do we need to have a guideline on the retention of election records and other artifacts?

  Requirement(s): 5.7.2-E,

- There are some requirements that did not fit well with any principles and guidelines:

  Requirement(s): 5.7.2-A, 5.7.2-J

- We found two requirements that may be repeats:

  Requirement(s): 5.7.3-A, 5.7.3-B

Below is a list of the event logging requirements that did not map directly to a principle and/or guideline. If a guideline is listed, NIST found that it did not fully map to the requirement, although partial applicability is noted. It is possible that requirements without an associated guideline may be superfluous and should be deleted. For more information about each requirement, please reference the full event logging requirements document.

5.7.1-C Voter privacy and ballot secrecy requirement

Requirement:	The voting device logs SHALL NOT contain information that, if published, would violate ballot secrecy or voter privacy or that would compromise voting system security in any way.
Principle(s)/ Guideline(s):	*Security: Ballot Secrecy* Records produced by the voting system do not reveal how a voter voted **Justification:** This requirement ensures that ballot secrecy should not be violated.

5.7.1-D.1 Timekeeping requirement

Requirement:	Timekeeping mechanisms SHALL generate time and date values.
Principle(s)/ Guideline(s):	*Security: Detection and Monitoring* Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing. **Justification:** This may not necessarily have a principle or guideline.

5.7.1-D.2 Time precision requirement

Requirement:	The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all audit records.

Principle(s)/ Guideline(ss):	*Security: Auditability* 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 and other election artifacts are resilient in the presence of intentional forms of tampering and accidental errors. **Justification:** This is a stretch, but if the time and date are off it may make it difficult to perform some types of audits.

5.7.1-D.3 Timestamp data requirement

Requirement:	Timestamps SHALL include date and time, including hours, minutes, and seconds.
Principle(s)/ Guideline(s):	*Security: Auditability* 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. *Security: Detection and Monitoring* Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing. **Justification:** This may not necessarily have a principle or guideline, but if we modify it to say "accurately' then time could be included.

5.7.1-D.4 Timestamp compliance requirement

Requirement:	Timestamps SHALL comply with ISO 8601 and provide all four digits of the year and include the time zone.
Principle(s)/ Guideline(s):	*Security: Detection and Monitoring* Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing. **Justification:** This may not necessarily have a principle or guideline, but if we modify it to say "accurately' then time could be included.

5.7.1-D.6 Clock drift minimum requirement

Requirement:	The voting device SHALL limit clock drift to a minimum of 1 minute within a 15 hour period after the clock is set.
Principle(s)/ Guideline(s):	*Security: Detection and Monitoring* Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing. **Justification:** This may not necessarily have a principle or guideline, but if we modify it to say "accurately' then time could be included.

5.7.2-A Default logging policy requirement

Requirement:	The voting device SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.

Principle(s)/ Guideline(s):	*Security: Detection and Monitoring* Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing. **Justification:** This requirement categorizes secure log management activities as "important activities". May not fit well.

5.7.2-C Log format requirement

Requirement:	The voting device SHALL store logs in a publicly documented log format, such as XML, or include a utility to export the logs into a publicly documented format for offline viewing.
Principle(s)/ Guideline(s):	*Interoperability Principle: Transparent* Data reported by the voting system is in a publicly documented format. **Justification:** Near identical mapping, to the interoperability principle titled Transparent.

5.7.2-E Event log retention capability requirement

Requirement:	The voting device SHALL be capable of retaining the event log data from previous elections.
Principle(s)/ Guideline(s):	

5.7.2-J Event log separation requirement

Requirement:	The voting device SHALL ensure that each election's event logs and each device's event logs are separable from each other.
Principle(s)/ Guideline(s):	*Interoperability: Transparent* Data used in critical device operations such as for cast vote records, tabulations, and event logs includes all elements necessary for verification of the data, and analysis and auditability of the operations. **Justification:** This requirement may map to this guideline but a more direct guideline may be necessary.

5.7.2-L Log viewing and analysis requirement

Requirement:	The voting device SHALL include an application or program to view, analyze, and search event logs.
Principle(s)/ Guideline(s):	*Interoperability: Transparent* Data reported by the voting system is in a publically documented format. **Justification:** We did not find a guideline that mapped well to this requirement. We will send this to interoperability group.

****We would like to confirm that the next two requirements are repeat requirements. ****

5.7.3-A General event log protection requirement

Requirement:	The voting device SHALL protect event log information from unauthorized access, modification, and deletion.
Applies to:	Programmed device

Test Reference:	Part 3:4.3 “Verification of Design Requirements”
Discussion:	
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*Security: Data Protection* Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. **Justification:** This requirement directly aligns with this guideline.

5.7.3-B Modification protection requirement

Requirement:	The voting device SHALL protect logs from unauthorized modification.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	There are several ways to protect logs from modification including using operating system level security mechanisms to prevent deletion of the logs and enforce append-only access, use of append-only media, and use of cryptographic techniques.
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*Security: Data Protection* Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. **Justification:** This requirement directly aligns with this guideline.