Mapping of VVSG 2007 System Event Logging Requirements to VVSG Cybersecurity Working Group Principles and Guidelines

After discussion of the System Event Logging gap analysis (http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/SystemEventLog-GapAnalysis-0612017-1.pdf), the Working Group decided to make the following changes to the principles and guidelines:

- 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.

- 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.

Other areas for future changes and development to the VVSG system event logging requirements include:

- Consider what system event logging requirements are needed for Remote Ballot Marking systems

5.7 System Event Logging

An event is something that occurs within a voting device and a log is a record of these events that have occurred. Each log entry contains information related to a specific event. Logs are used for error reporting, auditing, troubleshooting problems, optimizing performance, recording the actions of users, and providing data useful for investigating malicious activity.

Event logs are typically divided into two categories: system events and audit records. System events are operational actions performed by voting device components, such as shutting down the voting device, starting a service, usage information, client requests, and other information. Audit records contain security event information such as successful and failed authentication attempts, file accesses, and security policy changes. Other applications and third party software, such as antivirus software and intrusion detection software also record audit logs. For the purpose of this chapter system event logging will be used to include both system and audit logs for voting devices. System event logs are of equal importance in the output of an election as the electronic CVRs and vote totals.

This chapter describes voting device capabilities that perform system event logging to assist in voting device troubleshooting, recording a history of voting device activity, and detecting unauthorized or malicious activity. It also describes the use of log management to protect the confidentiality and integrity of logs while also ensuring their availability. The voting device software, operating system, and/or applications may perform the actual system event logging. There may be multiple logs in use on a single device.

The requirements in this section protect against the following intermediate attack goals:

1. The ability of an attacker to undetectably alter the logs;
2. The ability of an attacker to remove an entry from the log; and
3. The ability of an attacker to create an entry in the log.

This section defines the event logging requirements for voting devices. It outlines the various measures that the manufacturers and the voting device shall provide to ensure the functionality, performance, and security of the voting device event logging. These recommendations apply to the full scope of voting device functionality, including voting, pre- and post-voting activities, and maintenance of the voting device.

5.7.1 General system event logging

General requirements address the high-level functionality of a voting (programmed) device. These are the fundamental event logging requirements upon which other requirements in this section are based.

5.7.1-A Event logging mechanisms requirement

Requirement:	The voting device SHALL provide event logging mechanisms designed to record voting device activities.
Applies to:	Programmed device
Test Reference:	Part 3:4.3 “Verification of Design Requirements”
Discussion:	This requirement generalizes [VVSG2005] I.2.1.5.1, which provides a basic description of required event logging functionality.
Source:	[VVSG2005] I.2.1.5.1

Principle(s)/ Guideline(s):	*Security: Detection/Monitoring* Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing. **Justification:** The principle and guidelines maps directly to the requirement.

5.7.1-B Integrity protection requirement

Requirement:	The voting device SHALL enable file integrity protection for stored log files as part of the default configuration.
Applies to:	Programmed device
Test Reference:	Part 3:4.4 “Manufacturer Practices for Quality Assurance and Configuration Management”, 4.5 “Source Code Review”
Discussion:	File integrity protection includes techniques such as a digital signature that would alert to data modification and tampering. This requirement clarifies [VVSG2005] I.2.1.5.1-a-v, which requires that that the integrity of log files be maintained, by more specifically requiring that log files have integrity protection in their default configuration.
Source:	[VVSG2005] I.2.1.5.1-a
Principle(s)/ Guideline(s):	*Security: Auditability* Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. **Justification:** Log files could be defined as voting system records. *Security: Data Protection* Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. **Justification:** Similar to the previous guideline, there is close mapping if it means logs are included in the guideline.

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.
Applies to:	Programmed device
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	The device must be constructed so that the security of the system does not rely upon the secrecy of the event logs. It should be considered routine for event logs to be made available to election officials and possibly even to the public, if election officials so desire. The system must be designed to permit the election officials to do so without fear of negative consequences to the security and integrity of the election. For example, cryptographic secret keys or passwords must not be logged in event log records.
Source:	[VVSG2005] I.5.4
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 Event characteristics logging requirement

Requirement:	The voting device SHALL log at a minimum the following data characteristics for each type of event: 1. System ID; 2. Unique event ID and/or type; 3. Timestamp; 4. Success or failure of event, if applicable; 5. User ID triggering the event, if applicable; 6. Resources requested, if applicable.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This requirement clarifies and extends [VVSG2005] I.2.1.5.1-a and I.2.1.5.1-b by describing the required information that must be included with each event in the event log. [VVSG2005] 2.1.5.1-b is a requirement that discusses error messages and states that error messages must be logged. This document does not, in general, treat logging error messages differently than logging other events.
Source:	[VVSG2005] I.2.1.5.1-a, I.2.1.5.1-b
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 is identifying "important activities" of the voting process.

5.7.1-D.1 Timekeeping requirement

Requirement:	Timekeeping mechanisms SHALL generate time and date values.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This requirement generalizes [VVSG2005] I.2.1.5.1-a-ii, which requires the inclusion of a real-time clock in the hardware of voting systems.
Source:	[VVSG2005] I.2.1.5.1-a
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.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This requirement extends [VVSG2005] I.2.1.5.1-a by explicitly requiring that the timekeeping mechanism used to stamp audit records be precise enough to distinguish and properly order all events logged
Source:	[VVSG2005] I.2.1.5.1-a

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. **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.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Even if the accuracy of the clock leaves something to be desired, the seconds are useful to discern burst and gaps in the event stream. This requirement clarifies [VVSG2005] I.2.1.5.1-a by explicitly requiring that the date, hour, minute and second be recorded for each audit record timestamp.
Source:	[VVSG2005] I.2.1.5.1-a
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.4 Timestamp compliance requirement

Requirement:	Timestamps SHALL comply with ISO 8601 and provide all four digits of the year and include the time zone.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This requirement extends [VVSG2005] 2.1.5.1-a by requiring that timestamps comply with the ISO 8601 standard and include the time zone. The [VVSG2005] requires a timestamp, but does not specify a format.
Source:	[VVSG2005] I.2.1.5.1-a
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.5 Clock set requirement

Requirement:	Voting devices SHALL only allow administrators to set the clock.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This requirement is needed to adjust clocks for each election. Since a voting system architecture may not support complete access control capabilities due to resource constraints, this requirement may or may apply. For example, a voting

	system architecture may only support a single identity, group, or role, so the ability to distinguish administrators from other users may not possible. However, when the voting system architecture has the capability to distinguish administrators from other users, the requirement must be satisfied.
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system authenticates administrators, users, devices and services before granting access to sensitive functions. **Justification**: The principle itself maps to this requirement.

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.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	The accuracy of the timekeeping mechanism relative to UTC (Coordinated Universal Time) may depend on application of a manufacturer-specified clock set procedure. NIST and USNO time references are far more accurate, and higher accuracy is desirable, but many clock mechanism exhibit significant drift due to temperature, etc. and simple correction methods for a fast local clock might violate the monotonic time requirement.
Source:	[VVSG2005] I.5.4
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-E Minimum event logging requirement

Requirement:	The voting device SHALL log at a minimum the system events described in Part 1:Table 5-5.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Part 1:Table 5-5 presents a minimum list of system events to be logged. The table also includes an "applies to" reference specifying the class of devices that are subject to each requirement. This requirement clarifies and extends [VVSG2005] I.5.4.1, I.5.4.2, and I.5.4.3 by specifying a list of system events that must trigger an event log record. [VVSG2005] I.5.4.1 discusses required event log records for pre-election events. [VVSG2005] I.5.4.2 discusses required event log records for system readiness. [VVSG2005] I.5.4.3 discusses required event log records during the operation of diagnostic routines and the casting and tallying of ballots.
Source:	[VVSG2005] I.5.4.1, I.5.4.2-a, I.5.4.3-a
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 identifies “important activities” as system events.

5.7.1-E.1 Minimum logging disabling requirement

Requirement:	The voting device SHALL ensure that the minimum event logging in Part 1:Table 5-5 cannot be disabled.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005] I.5.4
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 ensures the logging of “important activities” cannot be disabled.

Table 5-5 Minimum events to log

SYSTEM EVENT	DESCRIPTION	APPLIES TO
GENERAL SYSTEM FUNCTIONS		
Device generated error and exception messages	Includes but not limited to: ▪ The source and disposition of system interrupts resulting in entry into exception handling routines. ▪ Messages generated by exception handlers. ▪ The identification code and number of occurrences for each hardware and software error or failure. ▪ Notification of physical violations of security. ▪ Other exception events such as power failures, failure of critical hardware components, data transmission errors or other types of operating anomalies. ▪ All faults and the recovery actions taken. ▪ Device generated error and exception messages such as ordinary timer system interrupts and normal I/O system interrupts do not need to be logged.	Programmed device
Critical system status messages	Critical system status messages other than information messages displayed by the device during the course of normal operations. Includes but not limited to: ▪ Diagnostic and status messages upon startup ▪ The "zero totals" check conducted before opening the polling place or counting a precinct centrally ▪ For paper-based systems, the initiation or termination of card reader and communications equipment operation ▪ Printer errors	Programmed device
Non-critical status messages	Non-critical status messages that are generated by the device's data quality monitor or by software and hardware condition monitors.	Programmed device
Events that require election official intervention	Events that require election official intervention, so that each election official access can be monitored and access sequence can be constructed.	Programmed device
Device shutdown and restarts	Both normal and abnormal device shutdowns and restarts.	Programmed device
Changes to system configuration settings	Configuration settings include but are not limited to registry keys, kernel settings, logging settings, and other voting device configuration settings.	Programmed device
Integrity checks for executables, configuration files, data, and logs.	Integrity checks that may indicate possible tampering with files and data.	Programmed device with file systems
The addition and deletion of files.	Files that are added or deleted from the voting device.	Programmed device with file systems
System readiness results	Includes but not limited to: ▪ System pass or fail of hardware and software test for system readiness ▪ Identification of the software release, identification of the election to be processed, polling place identification, and the results of the software and hardware diagnostic tests ▪ Pass or fail of ballot style compatibility and integrity test ▪ Pass or fail of system test data removal ▪ Zero totals of data paths and memory locations for vote recording	Programmed device
Removable media events	Removable media that is inserted into or removed from the voting device.	Programmed device
Backup and restore	Successful and failed attempts to perform backups and restores.	Election Management Systems
AUTHENTICATION AND ACCESS CONTROL		
Authentication related events	Includes but not limited to: ▪ Login/logoff events (both successful and failed attempts) ▪ Account lockout events ▪ Password changes	Programmed device
Access control related events	Includes but not limited to: ▪ Use of privileges (such as a user running a process as an administrator) ▪ Attempts to exceed privileges ▪ All access attempts to application and underlying system resources	Programmed device

System Event	Description	Applies To
	▪ Changes to the access control configuration of the voting device	
User account and role (or groups) management activity	Includes but not limited to: ▪ Addition and deletion of user accounts and roles ▪ User account and role suspension and reactivation ▪ Changes to account or role security attributes such as password length, access levels, login restrictions, permissions, etc. ▪ Administrator account and role password resets	Programmed device
Software		
Installation, upgrading, patching, or modification of software or firmware	Logging for installation, upgrading, patching, or modification of software or firmware include logging what was installed, upgraded, or modified as well as a cryptographic hash or other secure identifier of the old and new versions of the data.	Programmed device
Changes to configuration settings	Includes but not limited to: ▪ Changes to critical function settings. At a minimum critical function settings include location of ballot definition file, contents of the ballot definition file, vote reporting, location of logs, and voting device configuration settings. ▪ Changes to device settings including but not limited to enabling and disabling services. ▪ Starting and stopping processes.	Programmed device
Abnormal process exits	All abnormal process exits.	Programmed device
Successful and failed database connection attempts (if a database is utilized).	All database connection attempts.	Programmed device with database capabilities
Cryptographic Functions		
Changes to cryptographic keys	At a minimum critical cryptographic settings include key addition, key removal, and re-keying.	Programmed device
Voting Functions		
Ballot definition and modification	During election definition and ballot preparation, the device may provide logging information for the preparation of the baseline ballot formats and modifications to them including a description of the modification and corresponding dates. Includes but not limited to: ▪ The account name that made the modifications. ▪ A description of what was modified including the file name, location, and the content changed. ▪ The date and time of the modification.	Programmed device
Voting events	Includes: ▪ Opening and closing polls ▪ Casting a vote ▪ Canceling a vote during verification ▪ Fled voters ▪ Success or failure of log and election results exportation ▪ Note: for paper-based devices, these requirements may need to be met procedurally	Programmed device

5.7.2 System event log management

Log management is the process for generating, transmitting, storing, analyzing, and disposing of log data. Log management primarily involves protecting the integrity of logs while also ensuring their availability. It also ensures that records are stored in sufficient detail for an appropriate period of time.

A log management infrastructure consists of the hardware, software, networks, and media used to generate, transmit, store, and analyze log data. The events outlined in this section may be logged as part of the underlying operating system, the voting device software, or other third party applications.

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.
Applies to:	Voting device
Test Reference:	Part 3:4.1 "Initial Review of Documentation"
Discussion:	
Source:	[VVSG2005] I.5.4
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-B Reporting log failures, clearing, and rotation requirement

Requirement:	The voting device SHALL log logging failures, log clearing, and log rotation.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	A secondary logging mechanism may be used to log failures, clearing, and rotation.
Source:	[VVSG2005] I.5.4
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. The voting system generates, stores, and reports to the user or election official, all error messages as they occur. **Justification:** These are "important activities" and should be logged. Logging failures should notify the system administrator.

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.
Applies to:	Programmed device
Test Reference:	Part 3:4.3 "Verification of Design Requirements"
Discussion:	In some cases, election officials may be required to or may choose to disclose event logs in electronic form to investigators, candidates, observers, or to the public. The voting device must be designed to permit recipients of the event logs to understand and interpret the contents of the event logs and to write their own software tools to parse and analyze those event logs.
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*1.* *Security: Transparent* 2. Data reported by the voting system is in a publicly documented format. ***3.*** **Justification:** Near identical mapping, to the interoperability principle titled Transparent.

5.7.2-D Event log free space requirement

Requirement:	The manufacturer SHALL ensure that the voting device is supplied with enough free storage to include several maximum size event logs.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	The manufacturer should declare an upper limit on how much storage an event log might require during an election, referred to as the maximum size event log.
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*4. Security: Auditability* 5. Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. **6. Justification:** This helps to prevent accidental errors.

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.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	In practice, previous event logs are typically cleared prior to the start of a new election. In some cases, jurisdictions may want to maintain previous event logs on the voting device. Event log data may be retained according to various methods including log file size, log entry counts, and time settings.
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*7.*

5.7.2-F Log retention settings capability requirement

Requirement:	The voting device SHALL only allow administrators to modify the log data retention settings including the actions to take when a log reaches its maximum retention such as overwriting logs, rotating logs, or halting logging.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Many event logs have a maximum size for storage, such as storing the 10,000 most recent events, or keeping 100MB of log data. When the log storage capacity is reached, the log may overwrite old data with new data or stop logging altogether. Since a voting system architecture may not support complete access control capabilities due to resource constraints, this requirement may or may apply. For example, a voting system architecture may only support a single identity, group, or role, so the ability to distinguish administrators from other users may not possible. However, when the voting system architecture has the capability to distinguish administrators from other users, the requirement must be satisfied.
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system authenticates administrators, users, devices and services

	before granting access to sensitive functions. **Justification:** The principle itself maps to this requirement.

5.7.2-G Log rotation capability requirement

Requirement:	The voting device SHALL be capable of rotating the event log data to manage log file growth.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Log file rotation may involve regular (e.g., hourly, nightly, or weekly) moving of an existing log file to some other file name and/or location and starting fresh with an empty log file. Jurisdictions should ensure that the log rotation procedure includes a labeling method to identify the type of log, the system that created the logs, and the date of the logs.
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*8. Security: Auditability* 9. Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. **10. Justification:** This helps to prevent accidental errors, but may be better mapped to nothing.

5.7.2-H Event log deletion capability requirement

Requirement:	The voting device SHALL be capable of only allowing the administrator to delete previous event logs prior to starting a new election.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Since a voting system architecture may not support complete access control capabilities due to resource constraints, this requirement may or may not apply. For example, a voting system architecture may only support a single identity, group, or role, so the ability to distinguish administrators from other users may not possible. However, when the voting system architecture has the capability to distinguish administrators from other users, the requirement must be satisfied.
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system authenticates administrators, users, devices and services before granting access to sensitive functions. **Justification**: The principle itself maps to this requirement.

5.7.2-I Event log access requirement

Requirement:	The voting device SHALL restrict event log access to write or append-only for privileged logging processes and read-only for administrator accounts or roles.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"

Discussion:	Certain applications and processes need write and/or append access to system event logs in order to create entries. Administrator accounts or roles need read access for log analysis and other log management activities. Since a voting system architecture may not support complete access control capabilities due to resource constraints, this requirement may or may apply. For example, a voting system architecture may only support a single identity, group, or role, so the ability to distinguish administrators from other users may not possible. However, when the voting system architecture has the capability to distinguish administrators from other users, the requirement must be satisfied.
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*11. Security: Access Control* 12. 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. **13. Justification:** This requirement specifies different functions and activities that are available for different user roles

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.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*Interoperability: Transparent* 14. 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. 15. **Justification:** This requirement did not map to our principles.

5.7.2-K Event log export requirement

Requirement:	The voting device SHALL digitally sign and export event logs at the end of an election, along with all other election results from the device.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 "Functional Testing"
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:** Although digital signatures are not the only way to meet this requirement, it falls under the heading.

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.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*16.* *Interoperability: Transparent* 17. Data reported by the voting system is in a publically documented format. **18.** **Justification:** We did not find a guideline that mapped well to this requirement. We will send this to interoperability group.

5.7.2-M Event logging malfunction requirement

Requirement:	The voting device SHALL halt voting activities and create an alert if the logging system malfunctions or is disabled.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*19.* *Security: Detection and Monitoring* 20. The voting system generates, stores, and reports to the user or election official, all error messages as they occur. **21.** **Justification:** Near exact mapping

5.7.2-N Log file capacity requirement

Requirement:	The voting device SHALL create an alert at user-defined intervals as the logs begin to fill.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	User defined intervals for system event log capacity may include alerting when logs are 50%, 75%, and 95% full.
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*22.* *Security: Detection and Monitoring* 23. The voting system generates, stores, and reports to the user or election official, all error messages as they occur. *24.* **Justification:** This requirement aligns with this guideline.

5.7.2-O Event logging suspension requirement

Requirement:	The voting device SHALL suspend voting if the logs fill to a pre-defined capacity.
Applies to:	Programmed device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	[VVSG2005] I.5.4
Principle(s)/ Guideline(s):	*25.* *Security: Detection and Monitoring* *26.* The voting system provides mechanisms to detect and remediate anomalous or malicious behavior. *27.* **Justification:** This requirement maps to the principle itself.

5.7.3 System event log protection

Because logs contain voting device event records, they need to be protected from breaches of their integrity and availability. Logs that are secured improperly in storage or in transit might also be susceptible to intentional and unintentional alteration and destruction. This could cause a variety of impacts, including allowing malicious activities to go unnoticed and manipulating evidence to conceal the identity of a malicious party. For example, many rootkits are specifically designed to alter logs to remove any evidence of the rootkits' installation or execution.

Data retention requirements might require log storage for a longer period of time than the original log sources can support, which necessitates establishing log archival processes. The integrity and availability of the archived logs also need to be protected.

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.

5.7.3-C Event log archival protection requirement

Requirement:	If the voting device provides log archival capabilities, it SHALL ensure the integrity and availability of the archived logs.
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.