Principle 15
Detection and Monitoring

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

Requirements for Principle 15

Principle 15 Detection and Monitoring The voting system provides mechanisms to detect anomalous or malicious behavior.

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

- 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

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

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

15.3 - The voting system employs mechanisms to protect against malware.

- 15.3-A – Software verification
- 15.3.1 – Malware protection
- 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

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

- 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

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

15.1-A – Event logging

The voting system must be capable of logging events that occur in a voting system.

Discussion

The ability to log events within a system allows for continuous monitoring of the voting system. These logs provide a way for administrators to analyze the voting system's activities, diagnose issues, and perform necessary recovery and remediation actions.

15.1-B – Exporting logs

The voting system must be capable of exporting logs.

Discussion

Exporting logs offers the opportunity for external review, clearing storage, and a method to compare with future logs.

15.1-C – Logging voter information

The voting system must not log any information:

1. identifying a specific voter
2. connecting a voter to a specific ballot

Discussion

No voter information is stored anywhere within voting system logs. This would violate voter ballot secrecy because it can link a voter to their ballot selections.

Related requirements: 11.1-B and Ballot secrecy

15.1-D – Logging event types

At minimum, the voting system must log the events included in Table 15-1.

Discussion

Table 15-1 provides a list of events that will be included in the voting system event logs. The voting system is not limited to the events in the table.

Related requirements: Access Control, System Integrity, Data Protection

Notes: Things to add:

Information associated with configuration file access: Date/Time of access, Config file name, Indication of modification, Location of config file (directory path/memory address)The voting system must log malware detection activities, malware remediation activities, Network functionality is enabled or disabled, Wireless network functionality is enabled or disabled.

Table 15-1 – System events to log

System Event	Description	Applies To
General system functions		
Device generated error and exception messages	Includes but is 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 is 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 scanner and communications equipment operation • Printer errors • Detection or remediation of malware or other malicious software • Cryptographic boot validation success/failure	Programmed device

System Event	Description	Applies To
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 can 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 is 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 is not limited to: • Login/logoff events (both successful and failed attempts) • Account lockout events • Password changes	Programmed device
Access control related events	Includes but is not limited to:	Programmed device

System Event	Description	Applies 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 • Changes to the access control configuration of the voting device	
User account and role (or groups) management activity	Includes but is 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, and permissions • Administrator account and role password resets	Programmed device
Networking		
Enabling or disabling networking functionality	Includes but is not limited to: • Wired networking • Wireless networking	Programmed device
Software		
Installing, upgrading, patching, or modifying software or firmware	Logging for installation, upgrading, patching, or modifying 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 is not limited to: • Changes to critical function settings. At a minimum, critical function settings include location of election definition file, contents of the election 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 used).	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		

System Event	Description	Applies To
Ballot definition and modification	During election definition and ballot preparation, the device can provide logging information for preparing the baseline ballot formats and modifications to them, including a description of the modification and corresponding dates. Includes but is 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 • Success or failure of log and election results exportation • Note: for paper-based devices, these requirements might need to be met procedurally	Programmed device

15.1-E – Configuration file access log

When a system administrator is accessing a configuration file, the voting system must log identifying information of the individual and group or role accessing that file.

Discussion
A record of who modified a configuration file is important for auditing and accountability. The identifying information should include the username or the name of the user.

Notes: Access Control

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

15.2-A – Presentation of errors

The voting system must provide immediate notification to the user when an error occurs.

Discussion
Immediate notification of an issue or an error allows for prompt recovery and remediation.

15.2-B – Documenting error handling

The voting system documentation must include procedures for handling errors.

Discussion
Documentation will assist election officials with steps to properly address errors.

15.2-C – Logging errors

The voting system must log all errors.

15.2-D – Creating error reports

The voting system must be capable of creating error reports.

Discussion
Error reports allow system administrators to easily analyze the errors that occurred within a system.

15.3 - The voting system employs mechanisms to protect against malware.

15.3-A – Software verification

Vote capture and tabulation devices must verify software using digital signatures, application whitelisting, or some combination of the two.

Discussion
Digital signatures and whitelists assist in ensuring the vote capture and tabulation devices are using the correct software. If unauthorized software is found on the device, the appropriate malware remediation and response procedures will be implemented.

Related requirements: System Integrity, Data Protection
Applies to: Vote capture and tabulation devices

15.3.1 – Malware protection

15.3.1-A – Malware protection mechanisms

COTS devices providing EMS functionality must deploy mechanisms to protect against malware.

Discussion
NIST SP 800-83 Revision 1 *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* might be useful as supplemental guidance for protecting against malware. Digital signatures and whitelists can also be useful protection mechanisms.

External reference: NIST SP 800-83 Revision 1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops
Applies to: EMS Workstations

15.3.1-B – Updatable malware protection mechanisms

The voting system's malware protection mechanisms must be updatable.

Discussion
Malware protection mechanisms typically use software signatures to identify malware. As new malware signatures are received, the malware protection mechanism needs to be updated with the new signatures to ensure it is identifying all known malware.

Applies to: EMS Workstations, vote capture and tabulation devices

15.3.1-C – Documenting malware protection mechanisms

The voting system documentation must include the process and procedures for updating malware protection mechanisms.

Discussion

Providing documentation of the procedures to configure the malware protection mechanisms assists with ensuring the malware protection mechanisms are properly updated to meet *15.3.1-B-Updatable malware protection mechanisms.*

Applies to:	EMS Workstations, vote capture and tabulation devices
Related requirements:	[TK – Documentation]

15.3.1-D – Notification of malware detection

COTS devices providing EMS functionality must promptly notify an election official when malware is detected.

Discussion

Malware on an EMS device can disrupt the integrity of the data on the EMS device. Notification of malware detection allows election officials to promptly take the proper action to avoid data integrity issues.

Applies to:	EMS Workstations

15.3.1-E – Logging malware detection

The voting system must log instances of detecting malware.

15.3.1-F – Notification of malware remediation

COTS devices providing EMS functionality must provide a notification upon the removal or remediation of malware.

Discussion

Once malware it is identified on a device, operations can cease until the malware is remediated. This notification allows administrators and officials to know when it is safe to resume normal operations.

Applies to:	EMS Workstation

15.3.1-G – Logging malware remediation

The voting system must log malware remediation activities.

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

15.4-A – Network architecture documentation

The voting system documentation must include the network architecture of any internal network used by any portion of the voting system.

Discussion
Documentation of the network architecture can assist with data flow analysis, proper network configuration, and architecture to properly support the voting system.

Applies to: Voting systems with networking capabilities
Related requirements: [TK – Documentation]

15.4-B – Telecommunications documentation

The voting system documentation must include how any public telecommunications networks are used by any portion of the voting system, including vote capture devices and EMS workstations.

Applies to: Voting systems with networking capabilities

Discussion
Documentation of the public telecommunication network architecture can assist with data flow analysis, proper network configuration, and architecture to properly support the voting system.

Related requirements: [TK – Documentation]
Applies to: Voting systems with networking capabilities

15.4-C – Secure configuration documentation

The voting system documentation must list security relevant configurations and be accompanied by network security best practices.

If outside manufacturers provide guidance and best practices exist, these need to be documented and used to the extent practical.

Discussion
A variety of documentation providing secure configurations for network devices is publicly available from the US government.

External network services need to be documented.

Related requirements: [TK – Documentation]

Applies to:	Voting systems with networking capabilities

15.4-D – Firewall and IDS

The voting system must include a firewall or intrusion detection system (IDS).

Discussion
This requirement does not include point-to-point networks which do not typically use network appliances.

Applies to:	Voting systems with networking capabilities

15.4-E – Least privilege

Default configurations for the voting system must implement the principle of least privilege.

Discussion
Network access is only as much as is necessary to perform the desired function.

Related requirements	Access Control
Applies to:	Voting systems with networking capabilities

15.4-F – Rule and policy updates

The voting system must be capable of regularly updating rules and policies for firewalls and other network appliances.

Discussion
Network appliances and the voting system are constantly receiving improvements and information related to current threats. As this information is released, rules and policies might need to be modified to adjust to new capabilities.

Applies to:	Voting systems with networking capabilities