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

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

Applies to: Voting system

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

Status:	New
Updated:	Feb. 27, 2018
Source:	
Gap notes:	

15.1-B Log exportation

The voting system must be capable of exporting logs.

Applies to: Voting system

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

Status:	New
Updated:	Feb. 27, 2018
Source:	
Gap notes:	

15.1-C Logging of voter information

The voting system must not log any information identifying a specific voter.

Applies to: Voting system

Discussion
No voter information should not be stored anywhere within voting system logs. This would violate voter ballot secrecy because it may link a voter to their ballot selections.

Status:	New
Updated:	Feb. 27, 2018
Source:	
Gap notes:	Ballot Secrecy

15.1-D Logging of voter verifiable information

The voting system must not log any information that can be used to connect a voter to a specific ballot.

Applies to: Voting system

Discussion
Any ballot identifiers stored in log files will not violate the principle of ballot secrecy.

Status:	New
Updated:	Feb. 27, 2018
Source:	
Gap notes:	Ballot Secrecy

15.1-E Log event types

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

Applies to: Voting system

Discussion
Table 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.

Status:	New
Updated:	Feb. 27, 2018
Source:	
Gap notes:	Access Control, System Integrity, Data Protection

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 optical scanner 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

SYSTEM EVENT	DESCRIPTION	APPLIES TO
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 ▪ Changes to the access control configuration of the voting device	Programmed 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	Programmed device

System Event	Description	Applies To
	▪ 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	

15.1-F 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.

Applies to: Voting system

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

Status: Updated
Updated: Feb. 27, 2018
Source:
Gap 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.

Applies to: Voting system

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

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.2-B Documentation for error handling

The voting system must document procedures for handling errors.

Applies to: Voting system

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

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.2-C Logging of errors

The voting system must log all errors.

Applies to: Voting system

Discussion

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.2-D Creation of error reports

The voting system must be capable of creating error reports.

Applies to: Voting system

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

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

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 thereof.

Applies to: Vote capture and tabulation devices

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.

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes: System Integrity, Data Protection

15.3-B Malware protection mechanisms

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

Applies to: EMS Workstations

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

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.3-B.1 Updating malware protection mechanisms

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

Applies to: EMS Workstations, vote capture and tabulation devices

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.

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.3-B.2 Documentation of malware protection mechanisms

The process and procedures for updating malware protection mechanisms must be documented.

Applies to: EMS Workstations, vote capture and tabulation devices

Discussion

Providing documentation of the procedures to configure the malware protection mechanisms assist with ensuring the malware protection mechanisms are properly updated to achieve the previous requirement (15.3-B.1).

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.3-C Notification of malware detection

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

Applies to: EMS Workstations

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.

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.3-C.1 Logging malware detection

The voting system must log instances of detecting malware.

Applies to: Voting system

Discussion

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.3-D Notification of malware remediation

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

Applies to: EMS Workstation

Discussion

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

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.3-D.1 Logging malware remediation

The voting system must log malware remediation activities.

Applies to: Voting system

Discussion

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

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

The following requirements are specifically for voting systems with networking capabilities.

15.4-A Network architecture documentation

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

Applies to: Voting systems with networking capabilities

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

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.4-B Telecommunications documentation

The voting system must include documentation of 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 network architecture can assist with data flow analysis, proper network configuration, and architecture to properly support the voting system.

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.4-C Secure configuration documentation

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

Applies to: Voting systems with networking capabilities

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

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.4-C.1 Outside manufacturer guidance

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

Applies to: Voting systems with networking capabilities

Discussion
External network services need to be documented.

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.4-D Firewall and IDS

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

Applies to: Voting systems with networking capabilities

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

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes:

15.4-D.1 Least privilege

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

Applies to: Voting systems with networking capabilities

Discussion
The voting system must only provide the network access necessary to perform the desired function.

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes: Access Control

15.4-D.2 Rule and policy updates

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

Applies to: Voting systems with networking capabilities

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 may need to be modified to adjust to new capabilities.

Status: New
Updated: Feb. 27, 2018
Source:
Gap notes: