Principle 13
Data Protection

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

13.1 - The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.1-A Authentication to access configuration file

The voting system must allow only authenticated system administrators to access and modify voting device configuration file(s).

Applies to: Vote capture and tabulation system

Discussion
Voting system configuration files can include operating system and voting system application configuration files. These files can have a large impact on how the voting system functions and what election logic is being used. Therefore, accidental or malicious modification can have a large impact to the system and access to these files should be restricted to authorized individuals.

Status:	New
Updated:	Mar. 21, 2018
Source:	2007 VVSG 5.3-H
Gap notes:	13.2-A, 13.2-B

13.1-A.1 Authentication to access configuration file on EMS

The EMS must uniquely authenticate individuals associated with the role of system administrator before allowing them to access and modify EMS configuration files.

Applies to: EMS workstation

Discussion
EMS configuration files can include operating system and voting system application configuration files. These files can have a large impact on how an EMS tabulates and reports election results. Therefore, accidental or malicious modification can have a large impact to the system and access to these files should be restricted to authorized individuals.

Status:	New
Updated:	Mar. 21, 2018

Source: 2007 VVSG 5.3-H.1
Gap notes: Access Control

13.1-A.2 Authentication to access configuration file for network appliances

Network appliances must uniquely authenticate individuals before allowing them to access and modify configuration files.

Applies to: Network appliance

Discussion
Network appliances, such as routers such as firewalls, routers, switches, and VPN gateways are generally configurable. Individually authenticating users to the device, in lieu of using a shared password, is a standard practice for restricting access to these devices.

Status: New
Updated: Apr. 12, 2018
Source: New
Gap notes: Access Control

13.1-C Integrity Protection for Election Records

The vote capture and tabulation system must integrity protect the CVR and ballot images upon storage to the voting device.

Applies to: Vote capture and tabulation system

Discussion

Status: New
Updated: Mar. 21, 2018
Source:
Gap notes:

13.1-C.1 EMS Integrity Protection for Election Records

The EMS must integrity protect the CVR and ballot images upon storage to the device.

Applies to: Vote capture and tabulation system

Discussion

Status: New
Updated: Mar. 21, 2018
Source:
Gap notes:

13.2 – The source and integrity of electronic tabulation reports are verifiable.

13.2-A Signing stored electronic voting records

Cast vote records and ballot images must be digitally signed upon storage.

Applies to: Voting system

Discussion
Digital signatures address the threat that the records might be tampered with when stored. Cryptographic hashes do not sufficiently mitigate this threat, as election records could be altered and then re-hashed.

Status:	New
Updated:	Mar. 21, 2018
Source:	2007 VVSG 4.3.1-C
Gap notes:	

13.2-B Signing electronic voting records prior to transmission

Cast vote records and ballot images must be digitally signed prior to transmission.

Applies to: Voting system

Discussion
Digital signatures address the threat that the records might be tampered with when transmitted. Cryptographic hashes do not sufficiently mitigate this threat, as election records could be altered and then re-hashed.

Status:	New
Updated:	Mar. 21, 2018
Source:	2007 VVSG 4.3.1-C
Gap notes:	

13.2-C Cryptographic verification of electronic voting records

The EMS must be able to cryptographically verify all electronic voting records.

Applies to: Vote capture and tabulation system, EMS

Discussion
Verifying the authenticity and integrity record in large part mitigates attacks modifying the ballot in transit and unauthorized ballots being counted. This does not solely apply to transmitted records.

Status:	New
Updated:	Mar. 21, 2018

Source:
Gap notes:

13.3 - All cryptographic algorithms are public, well-vetted, and standardized.

13.3-A Cryptographic module validation

Cryptographic functionality must be implemented in a FIPS 140-2 validated cryptographic module operating in FIPS mode.

Applies to: Software cryptographic module

Discussion
Use of validated cryptographic modules ensures that the cryptographic algorithms used are secure and their correct implementation has been validated. Moreover, the security module security requirements have been validated to a specified security level. The current version of FIPS 140 and information about the NIST Cryptographic Module Verification Program are available at: http://csrc.nist.gov/cryptval/. Note that a voting device may use more than one cryptographic module, and quite commonly may use a software module for some functions, and a hardware module for other functions. This only applies to the software module – the underlying hardware platform is omitted from this requirement.

Status: New
Updated: Mar. 21, 2018
Source: 2007 VVSG 5.1.1-A

13.3-A.1 Use of Hardware Cryptographic Modules

Cryptography used within hardware-based cryptographic modules must be FIPS 140-2 validated.

Applies to: Hardware cryptographic module

Discussion
Test test test

Status: New
Updated: Apr 12, 2018
Source:

13.3-A.2 E2E Cryptographic Voting Protocols

Cryptographic functions specific to E2E cryptographic voting protocols are omitted from FIPS 140-2 validation and must adhere to requirements set forth by the Election Assistance Commission.

Applies to: E2E voting systems

Discussion

Commonplace cryptographic operations used within E2E systems, such as encryption, decryption, and hashing, are subject to the FIPS 140-2 validation requirement.

Status:	New
Updated:	Mar. 21, 2018
Source:	2007 VVSG 5.1.1-A
Gap notes:	

13.3-B Cryptographic strength

Devices using cryptography must employ NIST approved algorithms with a security strength of at least 112-bits.

Applies to: Voting system

Discussion

At the time of this writing, NIST specifies the security strength of algorithms in SP 800- 57, Part 1 <http://csrc.nist.gov/publications/nistpubs/index.html>. This NIST recommendation will be revised or updated as new algorithms are added, and if cryptographic analysis indicates that some algorithms are weaker than presently believed. The security strengths of SP 800-57 are based on estimates of the amount of computation required to successfully attack the particular algorithm. The specified strength should be sufficient for several decades.

This requirement is not intended to forbid all incidental use of non-approved algorithms by OS software or standardized network security protocols.

Status:	New
Updated:	Mar. 21, 2018
Source:	2007 VVSG 5.1.1-B
Gap notes:	

13.3-B.1 MAC Cryptographic strength

The key used with Message Authentication Codes must also have a security strength of at least 112 bits and use a 96-bit tag length.

Applies to: Voting system

Discussion

Message Authentication Codes of 96-bits are conventional in standardized secure communications protocols, and acceptable to protect voting records and systems.

Status: New
Updated: Mar. 21, 2018
Source: 2007 VVSG 5.1.1-B
Gap notes:

13.3-C Key Management Documentation

The voting system must provide documentation describing how key management is to be performed.

Applies to: Voting system

Discussion

This document provides procedural steps that can be taken to ease the burden of key management and safely perform these operations.

Status: New
Updated: Mar. 21, 2018
Source:
Gap notes:

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

<blurb about internal application and external application to networks>

13.4-A Mutual Authentication of Endpoints

Data must only be transmitted via a mutually authenticated connection.

Applies to: Voting systems with networking capabilities

Discussion

Mutual authentication provides assurance that each electronic device is legitimate. Mutual authentication can be performed using various protocols, such as IPsec and SSL/TLS.

Status: New
Updated: Mar. 21, 2018
Source: 2007 VVSG 5.6.3-B
Gap notes: Access Control, Detection & Monitoring

13.4-B Confidentiality Protection for Transmitted Data

A voting system transmitting data must cryptographically protect the confidentiality all data sent over a network.

Applies to:

Discussion

Status: New
Updated: Mar. 21, 2018
Source:
Gap notes:

13.4-B.1 Transport-Layer Protection

All data must be confidentiality protected at the transport layer or higher.

Applies to:

Discussion
This does not prevent the use of dual encrypted connections.

Status: New
Updated: Apr. 12, 2018
Source:
Gap notes:

13.4-C Integrity Protection for Transmitted Data

A voting system transmitting data must cryptographically protect the integrity of all election data sent over the network.

Applies to: EMS, Vote capture and tabulation system

Discussion
Integrity protection ensures that any inadvertent or intentional alterations to data are detected by the recipient. Integrity protection for data in transit may be provided through the use of various protocols, such as IPsec VPNs and SSL/TLS.

Status: New
Updated: Mar. 21, 2018
Source:
Gap notes:

13.4-D Cryptographic Verification of Election Data

A receiving voting system must cryptographically verify the integrity and authenticity of all election data received.

Applies to: EMS, Vote capture and tabulation system

Discussion

Status: New
Updated: Mar. 21, 2018
Source:
Gap notes:

13.4-D.1 Presentation of Verification Errors

A verification error of received election results must be immediately logged and presented onscreen.

Applies to:

Discussion
This information is a first line of defense against accidental errors or a malicious incident regarding modified or false election records.

Status: New
Updated: Mar. 21, 2018
Source:
Gap notes:

13.4-D.2 Use of Unverified Data

The voting system must not tabulate or aggregate data that fails verification.

Applies to: Voting system

Discussion
This prevents the use of election results that did not pass cryptographically verification.

Status: New
Updated: Mar. 21, 2018
Source:
Gap notes: