# Principle 13
# Data Protection

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

## Requirements for Principle 13

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

- 13.1.1 – Configuration file
- 13.1.1-A – Authentication to access configuration file
- 13.1.1-B – Authentication to access configuration file on EMS
- 13.1.1-C – Authentication to access configuration file for network appliances
- 13.1.2 – Election records
- 13.1.2-A – Integrity protection for election records
- 13.1.2-B – EMS integrity protection for election records

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

- 13.2-A – Signing stored electronic voting records
- 13.2-B – Signing electronic voting records prior to transmission
- 13.2-C – Cryptographic verification of electronic voting records

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

- 13.3-A – Cryptographic module validation
- 13.3-B– E2E Cryptographic Voting Protocols
- 13.3-C – Additional E2E Requirements from Certification Authority
- 13.3-D – Cryptographic strength
- 13.3-E – Key Management Documentation

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

- 13.4-A – Mutual authentication of endpoints
- 13.4-B – Confidentiality protection for transmitted data
- 13.4-C – Integrity protection for transmitted data
- 13.4-D – Cryptographic verification of election data

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

### 13.1.1 – Configuration file

#### 13.1.1-A – Authentication to access configuration file

The voting system must allow only authenticated system administrators to access and modify voting device configuration files.

**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 on the system and access to these files should be restricted to authorized individuals.

| | |
|---|---|
| Prior VVSG source: | 2007 VVSG 5.3-H |
| Related requirements: | 13.2-A, 13.2-B |
| Applies to: | Vote capture and tabulation system |

#### 13.1.1-B – 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.

**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 on the system and access to these files should be restricted to authorized individuals.

| | |
|---|---|
| Prior VVSG source: | 2007 VVSG 5.3-H.1 |
| Related requirements: | Access Control |
| Applies to: | EMS workstation |

#### 13.1.1-C – Authentication to access configuration file for network appliances

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

**Discussion**

Network appliances, 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.

| | |
|---|---|
| Related requirements: | Access Control |
| Applies to: | Network appliance |

## 13.1.2 – Election records

### 13.1.2-A – Integrity protection for election records

The vote capture and tabulation system must integrity protect the CVR and ballot images when they are stored in the voting device.

### 13.1.2-B – EMS integrity protection for election records

The EMS must integrity protect the CVR and ballot images when they are stored in the device.

## 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 when stored.

**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.

Prior VVSG Source: 2007 VVSG 4.3.1-C

### 13.2-B – Signing electronic voting records prior to transmission

Cast vote records and ballot images must be digitally signed before being transmitted.

**Discussion**

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

Prior VVSG Source: 2007 VVSG 4.3.1-C

### 13.2-C – Cryptographic verification of electronic voting records

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

**Discussion**

Verifying the authenticity and integrity record can mitigate attacks that could modify the ballot in transit and allow unauthorized ballots to be counted. This does not solely apply to transmitted records.

Applies to: Vote capture and tabulation system, EMS

## 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.

This applies to:

1. A software cryptographic module
2. A hardware cryptographic module

**Discussion**

Use of validated cryptographic modules ensures that the cryptographic algorithms used are secure and their correct implementation has been validated. It also ensures that 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 can use more than one cryptographic module, and quite commonly can 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.

| | |
|---|---|
| External references: | FIPS 140<br>NIST Cryptographic Module Verification Program |
| Prior VVSG source: | 2007 VVSG 5.1.1-A |
| Applies to: | Cryptographic modules |

### 13.3-B– E2E cryptographic voting protocols

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

**Discussion**

Commonplace cryptographic operations used within E2E systems, such as encryption, decryption, and hashing, are not subject to the FIPS 140-2 validation requirement.

These new types of systems might need additional requirements to be deployed in a secure manner.

| | |
|---|---|
| External references: | FIPS 140-2 |
| Prior VVSG source: | 2007 VVSG 5.1.1-A |
| Applies to: | E2E voting systems |

### 13.3-C – Cryptographic strength

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

**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.

External references: SP 800-57, Part 1
Prior VVSG source: 2007 VVSG 5.1.1-B

### 13.3-D – 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.

**Discussion**

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

Prior VVSG Source: 2007 VVSG 5.1.1-B

### 13.3-E – Key management documentation

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

**Discussion**

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

Related requirements: [TK – Documentation]

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

### 13.4-A – Mutual authentication of endpoints

Data must only be transmitted by a mutually authenticated connection.

**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.

| | |
|---|---|
| Prior VVSG source: | 2007 VVSG 5.6.3-B |
| Related requirements: | Access Control, Detection & Monitoring |
| Applies to: | Voting systems with networking capabilities |

### 13.4-B – Confidentiality protection for transmitted data

A voting system transmitting data must cryptographically protect the confidentiality of all data sent over a network at the transport layer or higher.

**Discussion**

This does not prevent the use of “double encrypted” connections employing cryptography at multiple layers of the network stack.

### 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.

**Discussion**

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

| | |
|---|---|
| Applies to: | EMS, Vote capture and tabulation system |

### 13.4-D – Verification of election data

A receiving voting system must…

1. Cryptographically verifying the integrity and authenticity of all election data received.
2. Immediately log onscreen any verification error of received election results.

3. Immediately present on-screen any verification errors.
4. Not tabulating or aggregating any data that fails verification.

**Discussion**

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

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

Applies to: EMS, Vote capture and tabulation system