Principle 11
Access Control

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

11.1 - Access privileges, accounts, activities, and authorizations are logged, monitored, and reviewed periodically and modified as needed.

11.1-A Ensuring Authorized Access

The voting system must only allow authorized users to access the voting system.

Applies to: Voting system

Discussion

This includes voters, election officials, and pollworkers.

Status:	New
Updated:	Jan. 16, 2018
Source:	N/A
Gap notes:	

11.1-B Access control logging

The voting system must log any access to, and activities performed, on the voting system.

Applies to: Voting system

Discussion

Status:	New
Updated:	Jan. 16, 2018
Source:	N/A
Gap notes:	

11.1-B.1 Voter Information in Log Files

The voting system must not log any voter identifying information.

Applies to: Voting system

Discussion

Status:	New
Updated:	Jan. 16, 2018
Source:	N/A
Gap notes:	Voter privacy / Ballot secrecy

11.1-C Access Control Log Timestamp

The voting system must include timestamps on all log entries.

Applies to: Voting system

Discussion

Timestamps on the log entries will allow for easy auditing and review of access to the voting system.

Status:	New
Updated:	Jan. 16, 2018
Source:	Derived from VVSG 2007 4.2.1-A
Gap notes:	

11.1-D Access Attempt Log

The voting system must log all failed and successful attempts to access the voting system.

Applies to: Voting system

Discussion

Status:	New
Updated:	Jan. 16, 2018
Source:	N/A
Gap notes:	

11.1-E Access Control Modifications

The voting system must only allow an administrator to make modifications to access privileges, accounts, activities, and authorizations.

Applies to: Voting system

Discussion

Status: New
Updated: Jan. 16, 2018
Source: N/A
Gap notes:

11.1-F Log Access Control Modifications

The voting system must create log entries for all events which change the access control system including policies, privileges, accounts, users, groups, and roles.

Applies to: Voting system

Discussion

Access control logging supports accountability of actions by identifying and authenticating users.

Status: Updated
Updated: Jan. 4, 2018
Source: Derived from VVSG 2007 4.2.1-A
Gap notes:

11.1-G Access control log is usable

The voting system log entries must allow for continuous monitoring and periodic review.

Applies to: Voting system

Discussion

Status: Updated
Updated: Dec. 26, 2017
Source: Derived from VVSG 2007 4.2.1-A
Gap notes:

11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.2-A Data Isolation

The voting system must utilize a data isolation technology to enforce user and data separation on the voting system.

Applies to: Voting device

Discussion
This separation of data will assist in limiting accidental or intentional modification of vote data. One such example includes sandboxing.

Status:	New
Updated:	Jan. 16, 2018
Source:	N/A
Gap notes:	

11.2-B Authorized Users

The voting system must allow an administrator to establish or modify the list of authorized users.

Applies to: Voting device

Discussion
This requirement assists with ensuring only authorized users are given access to the voting system.

Status:	New
Updated:	Jan. 16, 2018
Source:	N/A
Gap notes:	

11.2-C Access control configuration

The voting device must allow the administrator group or role to configure the permissions and functionality for each identity, group or role to include account and group/role creation, modification, disablement, and deletion.

Applies to: Voting device

Discussion
For vote-capture devices, each group/role may or may not have permissions for every voting state. Additionally, the permissions that a group/role has for a voting state may be restricted to certain functions. Part 1: Table 5-3 shows an example matrix of group or role to voting state access rights; the table is not meant to include all activities. This requirement extends [VVSG2005] I.7.2.1.1-a by allowing configuration flexibility for permissions and functionality for each identity, group, or role.

Privileged accounts include any accounts within the operating system, voting device software, or other third-party software with elevated privileges such as administrator, root, and maintenance accounts. This requirement extends [VVSG2005] I.7.2.1.2 by allowing the creation and disabling of privileged accounts.

Status: Updated
Updated: Dec. 26, 2017
Source: VVSG 2007
Gap notes:

11.2-D Group or Role

The voting system must allow an administrator to establish or modify permissions assigned to specific groups or roles.

Applies to: Voting device

Discussion
The voting system should be capable of allowing an administrator to create specific groups or roles such as the ones shown below in Table 5-1.

Status: New
Updated: Jan. 16, 2018
Source: N/A
Gap notes:

Table 5-1 Voting system minimum groups and roles

GROUP OR ROLE	DESCRIPTION
Voter	The voter role is a restricted process in the vote-capture device. It allows the vote-capture device to enter the Activated state for voting activities.
Election Judge	The election judge has the ability to open the polls, close the polls, handle fled voters, recover from errors, and generate reports.
Poll Worker	The poll worker checks in voters and activates the ballot style.
Central Election Official	The central election official loads ballot definition files.
Administrator	The administrator updates and configures the voting devices and troubleshoots system problems.

11.2-E Access control voting states

The vote-capture device's access control mechanisms must distinguish at least the following voting states from Table 5-2:

a. Pre-voting;
b. Activated;
c. Suspended; and
d. Post-voting

Applies to: Voting device

Discussion

The groups/roles established in (11.2-__) will be given specific permissions which may be affected by the voting state (Table 5-2). Part 1: Table 5-2 shows the minimum states based on Part 1 Sections 8.1 and 8.2. See Part 1 Section 8.2 for additional description of the voting states for vote-capture devices.

Status: Updated
Updated: Dec. 26, 2017
Source: [VVSG2005] I.7.2.1,I.7.2.1.1
Gap notes:

Table 5-2 Vote-capture device minimum states

STATE	DESCRIPTION
Pre-voting	Power-on, loading and configuring device software, maintenance, loading election-specific files, preparing for election day usage.
Activated	Activating the ballot, printing, casting, spoiling the ballot.
Suspended	Entered when an election official suspends voting.
Post-voting	Closing polls, tabulation, printing records, power-off.

11.2-F Assign User

The voting system must allow an administrator to assign a group/role to an authorized user.

Applies to: Voting device

Discussion

Status: New
Updated: Jan. 16, 2018
Source: N/A
Gap notes:

11.2-G Apply Permissions

The voting system must apply assigned roles and permissions to authorized users.

Applies to: Voting device

Discussion

Status: New
Updated: Jan. 16, 2018
Source: N/A
Gap notes:

11.2-H Role-based access control standard

Voting systems that implement role-based access control must support the recommendations for Core RBAC in the ANSI INCITS 359-2004 American National Standard for Information Technology – Role Based Access Control document.

Applies to: Voting device

Discussion

This requirement extends [VVSG2005] I. 7.2.1.1-a by requiring role-based methods to follow ANSI INCITS 359-2004.

Status:	Updated
Updated:	Dec. 26, 2017
Source:	[VVSG2005] I.7.2.1.1
Gap notes:	

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.3-A General Access Control Mechanisms

The voting device must provide access control mechanisms.

Applies to: Voting system

Discussion

Access controls support the following concepts:

1. Limiting the actions of users, roles, and processes (entities) to those that are authorized.
2. Limiting entities to the functions for which they are authorized.
3. Limiting entities to the data for which they are authorized.
4. Accountability of actions by identifying and authenticating users

Status:	Updated
Updated:	Jan. 17, 2017
Source:	VVSG2005 I.7.2.1.2-1, I.7.2.1.2-2
Gap notes:	

11.3-B Access Control Mechanism Application

The voting device must use access control mechanisms to permit authorized access or prevent unauthorized access to the voting system.

Applies to: Voting system

Discussion

Access controls support the following concepts:

1. Limiting the actions of users, roles, and processes (entities) to those that are authorized.
2. Limiting entities to the functions for which they are authorized.
3. Limiting entities to the data for which they are authorized.
4. Accountability of actions by identifying and authenticating users

Status:	Updated
Updated:	Dec. 26, 2017
Source:	VVSG2005 I.7.2.1.2-1, I.7.2.1.2-2
Gap notes:	

11.3-C Multi-factor authentication

The voting system must be capable of using multi-factor authentication to verify a user has authorized access to perform critical operations. Critical operations include:

- Software updates to the voting system
- Aggregation and Tabulation
- Enabling network functions, and sending / receiving public telecommunications
- Changing device states, including opening and closing the polls

Applies to: Voting system

Discussion

The voting system should be utilize the specifications mentioned in *NIST SP 800-63-3 Digital Identity Guidelines* to fulfill this requirement.

Status:	New
Updated:	Jan. 16, 2018
Source:	N/A
Gap notes:	

11.3-D Critical Operations

The voting system must require multi-factor authentication for all pre-voting and post-voting activities defined in Table 5-2.

Applies to: Voting system

Discussion

The voting system should be utilize the specifications mentioned in *NIST SP 800-63-3 Digital Identity Guidelines* to fulfill this requirement.

Status:	New
Updated:	Jan. 17, 2018
Source:	N/A
Gap notes:	

11.3-E Administrator group or role multi-factor authentication

The voting system must authenticate the administrator group or role with a multi-factor authentication mechanism.

Applies to: Voting system

Discussion

This requirement extends [VVSG2005] I.7.2.1.2-e by requiring multi-factor authentication for the voting device administrator group or role.

Status:	New
Updated:	Jan. 17, 2018
Source:	N/A
Gap notes:	

11.3-F User name and password management

If the voting system uses a user name and password authentication method, the voting device must allow the administrator to enforce password strength, histories, and expiration.

Applies to: Voting device

Discussion

This requirement extends [VVSG2005] I.7.2.1.2-e by requiring strong passwords, password histories, and password expiration.

Status:	Updated
Updated:	Jan. 2, 2018
Source:	[VVSG2005] I.7.2.1.2-1

Gap notes:

11.3-F.1 Password strength configuration

The voting device must allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline standards.

Applies to: Voting device

Discussion

This requirement extends [VVSG2005] I.7.2.1.2-e by allowing the administrator group or role flexibility in configuring password strength. It also requires the use of NIST 800-63 standards.

Status: Updated
Updated: Jan. 2, 2018
Source: [VVSG2005] I.7.2.1.2-1
Gap notes:

11.3-F.2 Password history configuration

The voting device must enforce password histories and allow the administrator to configure the history length.

Applies to: Voting device

Discussion

Password histories are a log of previously used passwords for automatic comparison with a new chosen password. The password history is used to ensure that recently used passwords are not used again within a pre-defined number of password changes (i.e., history length). This requirement extends [VVSG2005] I.7.2.1.2-e by allowing the administrator group or role flexibility in configuring password history.

Status: Updated
Updated: Jan. 2, 2018
Source: [VVSG2005] I.7.2.1.2-1
Gap notes:

11.3-F.3 Account information for password restriction

The voting device must ensure that the username is not used in the password.

Applies to: Voting device

Discussion

This requirement extends [VVSG2005] I.7.2.1.2-e by restricting the use or usernames and related information in passwords.

Status: Updated
Updated: Jan. 2, 2018
Source: [VVSG2005] I.7.2.1.2-1
Gap notes:

11.3-F.4 Automated password expiration

The voting device must provide a means to automatically expire passwords in accordance with the voting jurisdiction's policies.

Applies to: Voting device

Discussion
Jurisdiction policies often expire passwords after each election. This requirement extends [VVSG2005] I.7.2.1.2-e by requiring the expiration of unchanged passwords.

Status: Updated
Updated: Jan. 2, 2018
Source: [VVSG2005] I.7.2.1.2-1
Gap notes:

11.4 - Default access control policies enforce the principles of least privilege and separation of duties.

11.4-A Least Privilege

By default, the voting system must deny access to functions and data unless explicitly permitted.

Applies to: Voting system

Discussion
This requirement extends [VVSG2005] I.7.2.1.2-a by requiring explicit authorization of subjects based on access control policies.

Status: Updated
Updated: Dec. 27, 2017
Source: [VVSG2005] I.7.2.1.2-1
Gap notes:

11.4-B Minimum permissions default

The voting device's default access control permissions must implement the minimum permissions needed for each role or group

Applies to: Voting device

Discussion
Minimum permissions restrict the group or role to access only the information and resources that are necessary for its purpose. This requirement extends [VVSG2005] I. 7.2.1.1 and I.7.2.1.2 by requiring minimum default access control permissions.

Status:	Updated
Updated:	Dec. 27, 2017
VVSG 1.1:	[VVSG2005] I.7.2.1.1, I.7.2.1.2-1
Gap notes:	

11.4-C Privilege escalation prevention

The voting device must prevent a lower-privilege process from modifying higher-privilege processes and data.

Applies to: Voting device

Discussion
This requirement extends [VVSG2005] I.7.2.1 by preventing unauthorized process modification

Status:	Updated
Updated:	Dec. 27, 2017
VVSG 1.1:	[VVSG2005] I.7.2.1 and [VVSG2005] II.6.4.1
Gap notes:	

11.4-D Privileged operations authorization

The voting device must ensure that an administrator authorizes each privileged operation.

Applies to: Voting device

Discussion
This requirement extends [VVSG2005] I.7.2 by requiring authorization of privileged operations.

Status:	Updated
Updated:	Dec. 27, 2017
VVSG 1.1:	[VVSG2005] I.7.2.1 and [VVSG2005] II.6.4.1
Gap notes:	

11.4-E Default Access Modification

The voting system must only allow an administrator to modify the default permissions given to a user.

Applies to: Voting system

Discussion

Status: New
Updated: Jan. 16, 2018
Source: New
Gap notes:

11.4-F Separation of duties

The voting device must enforce separation of duty across subjects based on user identity, groups, or roles.

Applies to: Voting device

Discussion
This requirement extends [VVSG2005] I.7.2.1.2 by requiring separation of duty.

Status: Updated
Updated: Dec. 27, 2017
Source: [VVSG2005] I.7.2.1.2-1
Gap notes:

11.5 - Logical access to voting system assets are revoked when no longer required.

11.5-A Access Time Period

The voting system must only allow user's authorized access within a time period specified by the administrator.

Applies to: Voting system

Discussion

Status: New
Updated: Jan. 16, 2017
Source: N/A

Gap notes:

11.5-B Access Time-out

The voting system must require a user to re-authenticate once the specified time period from 11.5-A has timed out.

Applies to: Voting system

Discussion

Status: New
Updated: Jan. 16, 2017
Source: N/A
Gap notes:

11.5-C Account lock out

The voting device must lock out groups, roles, or individuals after an administrator specified number of consecutive failed authentications attempts within an administrator defined time period, and for an administrator specified duration.

Applies to: Voting device

Discussion

This requirement extends [VVSG2005] I.7.2.1.2 by allowing the administrator group or role flexibility in configuring the account lockout policy.

Status: Updated
Updated: Jan. 2, 2018
VVSG 1.1: [VVSG2005] I.7.2.1.2-1
Gap notes:

11.5-D Re-instate Administrator(s)

The voting system must require administrators to be re-instated for every election.

Applies to: Voting system

Discussion

Status: New
Updated: Jan. 17, 2018
Source: N/A

Gap notes:

11.5-E Re-authenticate

The voting system must require re-authentication of users for every election.

Applies to: Voting system

Discussion

Status: New
Updated: Jan. 17, 2018
Source: N/A

Gap notes: