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 Logging of activities and resource access

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

Applies to: Voting system

Discussion
In the event of an error or incident, the user access log may assist in narrowing down the reason for the incident or error.

Status:	New
Updated:	Feb. 14, 2018
Source:	N/A
Gap notes:	

11.1-A.1 Voter information in log files

The voting system must prevent the logging of any voter identifying information.

Applies to: Voting system

Discussion
The logging and storing of voter identifying information after a ballot is cast is a violation of voter privacy.

Status:	New
Updated:	Feb. 14, 2018
Source:	N/A
Gap notes:	Voter privacy, Ballot secrecy

11.1-B Access control log timestamp

The voting system must include timestamps for all log entries.

Applies to: Voting system

Discussion

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

Status:	New
Updated:	Feb. 14, 2018
Source:	Derived from VVSG 2007 4.2.1-A
Gap notes:	

11.1-C Access attempt log

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

Applies to: Voting system

Discussion

A log of all attempts to access a voting system is necessary for analysis as mentioned in 11.1-B and 11.1-C.

Status:	New
Updated:	Feb. 14, 2018
Source:	N/A
Gap notes:	

11.1-D Disabling of logging

The voting system must prevent the logs from being disabled.

Applies to: Voting system

Discussion

This requirement promotes the integrity of the information logged by ensuring all activities are logged.

Status:	New
Updated:	Feb. 14, 2018
Source:	N/A
Gap notes:	

11.1-E Modification of log entries

The voting system must prevent log entries from being modified.

Applies to: Voting system

Discussion
This requirement promotes the integrity of the information logged by ensuring all activities and not modifiable.

Status: New
Updated: Feb. 14, 2018
Source: N/A
Gap notes:

11.1-F Logging of 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 or roles, and authentication methods.

Applies to: Voting system

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

Status: Updated
Updated: Feb. 14, 2018
Source: Derived from VVSG 2007 4.2.1-A
Gap notes:

11.1-G On-demand access to logs

The voting system must provide administrators access to logs on demand, allowing for continuous monitoring and periodic review.

Applies to: Voting system

Discussion
Enabling administrators to export and review the logs is a useful feature. Continuous monitoring and review of access control logs gives the administrator the opportunity to analyze and make changes to permissions and privileges, and quickly identify issues.

Status: Updated
Updated: Feb. 14, 2018
Source: Derived from VVSG 2007 4.2.1-A
Gap notes:

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

11.2-A Ensuring authorized access

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

Applies to: Voting system

Discussion

Authorized users include voters, election officials, and election workers.

Status:	New
Updated:	Feb. 14, 2018
Source:	N/A
Gap notes:	

11.2-B Modifying authorized user lists

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

Applies to: Voting system

Discussion

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

Status:	New
Updated:	Feb. 14, 2018
Source:	N/A
Gap notes:	

11.2-C Access control voting states

The voting system access control mechanisms must distinguish at least the following voting states from Table 2:

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

Applies to: Voting system

Discussion

The groups or roles in 11.2-G.1 (Table 2) will be given specific permissions which may be affected by the voting state (Table 1).

Status: Updated
Updated: Feb. 14, 2018
Source: [VVSG2005] I.7.2.1, I.7.2.1.1
Gap notes:

Table 1 - Voting State Descriptions

STATE	DESCRIPTION
Pre-voting	Powering-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	Occurring when an election official suspends voting
Post-voting	Closing polls, tabulating votes, printing records, powering-off

11.2-D Access control configuration

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

Applies to: Voting system

Discussion

For vote-capture devices, each group or role may or may not have permissions for every voting state. Additionally, the permissions that a group or role has for a voting state may be restricted to certain functions. Table 3 shows an example matrix of group/role to system 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 or group/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.

The administrator is the only user authorized to make major changes within a voting system. Administrators are given this group or role to ensure all other users have proper access to the information necessary to perform their duties.

Status: Updated
Updated: Feb. 14, 2018

Source: VVSG 2007
Gap notes:

11.2-E Administrator modified permissions

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

Applies to: Voting system

Discussion
The administrator's authority to create or modify permissions restricts user's from gaining unauthorized permissions.

Status: New
Updated: Feb. 14, 2018
Source: N/A
Gap notes:

11.2-F Authorized assigning groups or roles

The voting system must allow only an administrator to create or assign the groups or roles.

Applies to: Voting system

Discussion
Table 1 is a list of groups or roles that should be included within the voting system.

Status: New
Updated: Feb. 14, 2018
Source: N/A
Gap notes:

11.2-G 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 system

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: Feb. 14, 2018
Source: [VVSG2005] I.7.2.1.1

Gap notes:

11.2-G.1 Minimum groups or roles

At minimum, voting systems that implement RBAC must define the following groups or roles within Table 1.

Applies to: Voting system

Discussion

Table 2 is a baseline list of groups or roles that may be included within the voting system.

Status: New
Updated: February 14, 2018
Source: N/A
Gap notes:

Table 2 – Minimum Voting System Groups or Roles for RBAC

GROUP/ROLE	DESCRIPTION
Administrator	The administrator role updates and configures the voting devices and troubleshoots system problems.
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/Precinct Captain	The election judge role has the ability to open the polls, close the polls, handle fled voters, recover from errors, and generate reports
Election Worker	The election worker role checks in voters and activates the ballot style.
Central Election Official	The central election official role loads ballot definition files.

11.2-G.2 Minimum group or role permissions

At minimum, the voting system must use the groups or roles from Table 1 and the voting states from Table 2, to assign the minimum permissions in Table 3.

Applies to: Voting system

Discussion

Table 4 defines the minimum functions according to user, voting state, and system. Other capabilities can be defined as needed by jurisdiction.

Status: New
Updated: February 14, 2018
Source: N/A

Gap notes:

Table 3 - Minimum Permissions per Group or Role

GROUP/ROLE	SYSTEM	PRE-VOTING	ACTIVATED	SUSPENDED	POST-VOTING
Administrator	**EMS**	Full Access	Full Access	Full Access	Full Access
	BMD/Electronic	Full Access	Full Access	Full Access	Full Access
	PCOS	Full Access	Full Access	Full Access	Full Access
Voter	**EMS**	---	---	---	---
	BMD/Electronic	---	Cast and cancel ballots	---	---
	PCOS	---	Ballot Submission	---	---
Election Judge/Precinct Captain	**EMS**	---	---	---	---
	BMD/Electronic	Open polls, L&A	Close or suspend polls, Recover from errors	Exit suspended state	Generate reports
	PCOS	Open polls, L&A	Recover from errors	Exit suspended state	Generate reports
Election Worker	**EMS**	---	---	---	---
	BMD/Electronic	---	Activate ballot	---	---
	PCOS	---	---	---	---
Central Election Official	**EMS**	Define and load ballot	---	---	Reconcile Provisional-challenged ballots, write-ins, generate reports

	BMD/Electronic	---	---	---	---
	PCOS	---	---	---	---

11.2-H Applying permissions

The voting system must be capable of applying assigned groups or roles and permissions to authorized users.

Applies to: Voting system

Discussion

Once the user is assigned a group or role, the voting system must be capable of making the necessary changes to the user's permissions. The permissions are changed based on the assigned group or role.

Status: New
Updated: Feb. 14, 2018
Source: N/A
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 Access control mechanism application

The voting system 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:

- Limiting the actions of users, groups or roles, and processes to those that are authorized.
- Limiting entities to the functions for which they are authorized.
- Limiting entities to the data for which they are authorized.
- Accountability of actions by identifying and authenticating users

Most modern operating systems natively provide configurable access control mechanisms that the voting system application can use.

Status: Updated

Updated: Feb. 14, 2018
Source: VVSG2005 I.7.2.1.2-1, I.7.2.1.2-2
Gap notes:

11.3-B Multi-factor authentication for critical operations

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 certified voting system
- Aggregation and tabulation
- Enabling network functions, wireless, and use of telecommunications
- Changing device states, including opening and closing the polls
- Deleting or modifying the audit trail
- Modifying authentication mechanisms

Applies to: Voting system

Discussion

NIST SP 800-63-3 Digital Identity Guidelines provides additional information useful in fulfilling this requirement. NIST SP 800-63-3 defines Multi-factor authentication (MFA) as follows:

"An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors.

The three authentication factors are something you know, something you have, and something you are."

Multifactor authenticators may include, but are not limited to the following:

- *Username & password*
- *Smartcard (for example, voter access card)*
- *iButton*
- *Biometric authentication (for example, fingerprint)*

Status: New
Updated: Feb. 14, 2018
Source: N/A
Gap notes:

11.3-C Multi-factor authentication for administrators

The voting system must authenticate the administrator 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 system administrator group or role.

Status:	New
Updated:	Feb. 14, 2018
Source:	N/A
Gap notes:	

11.3-D Username and password management

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

Applies to: Voting system

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

Status:	Updated
Updated:	Feb. 14, 2018
Source:	[VVSG2005] I.7.2.1.2-1
Gap notes:	

11.3-D.1 Password complexity

The voting system must allow only the administrator 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 system

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:	Feb. 14, 2018

Source: [VVSG2005] I.7.2.1.2-1
Gap notes:

11.3-D.2 Minimum password complexity

The voting system must compare all passwords against a manufacturer specified list of well-known weak passwords.

Applies to: Voting system

Discussion
Examples of common weak passwords include 0000, 1111, 1234.

Status: Updated
Updated: Feb. 14, 2018
Source: [VVSG2005] I.7.2.1.2-1
Gap notes:

11.3-D.3 Usernames within passwords

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

Applies to: Voting system

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

Status: Updated
Updated: Feb. 14, 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 implement the principle of least privilege including, denying 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: Feb. 14, 2018
Source: [VVSG2005] I.7.2.1.2-1
Gap notes:

11.4-B Separation of duties

Voting system documentation must include suggested practices for dispersing critical operations across multiple groups or roles.

Applies to: Voting system

Discussion
Guidance for implementing separation of duties within the voting system is imperative to implement the separation of duties principle. Separation of duties is meant to divide user functions and roles so that there is no conflict of interest.

Status: New
Updated: Feb. 14, 2018
Source:
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
After authentication, a user's access to a voting system will time-out after a specified period of time. This will avoid unauthorized access to the voting system by unauthorized users. Once a user's access has timed-out, the user must re-authenticate to the voting system.

Status: New
Updated: Feb. 14, 2018
Source: N/A
Gap notes:

11.5-B Account lockout

The voting system must lockout roles or individuals after an administrator specified number of consecutive failed authentications attempts.

Applies to: Voting system

Discussion

This requirement can be implemented using a technique such as exponential backoff. Exponential backoff requires that after each unsuccessful authentication attempt, the time period before another authentication attempt can be made grows exponentially. For instance, after 1 unsuccessful authentication attempt, the user must wait 0 seconds before trying again. After 2 unsuccessful authentication attempts, the user must wait 2 seconds. 3 unsuccessful attempts requires 4 seconds, and so on. This requirement prevents certain classes of password guessing attacks.

Status:	Updated
Updated:	Feb. 14, 2018
VVSG 1.1:	[VVSG2005] I.7.2.1.2-1
Gap notes:	

11.5-B.1 Lockout time duration

The voting system must allow only an administrator to define the lockout duration.

Applies to: Voting system

Discussion

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

Status:	Updated
Updated:	Feb. 14, 2018
VVSG 1.1:	[VVSG2005] I.7.2.1.2-1
Gap notes:	