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 Access control logging

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

Moved down [1]: **11.1-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 poll workers. ¶
Status: →New¶
Updated:→Jan. 16, 2018¶
Source:→N/A ¶
Gap notes:→¶

11.1-A.1 Voter Information in Log Files

The voting system must not log 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: Jan. 16, 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.

Deleted: ps on the

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

Deleted: 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¶

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

Status: →New¶

Updated:→Jan. 16, 2018¶

Source:→N/A ¶

Gap notes:→¶

11.1-D 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, roles, and authentication methods.

Deleted: and

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-E Access control log is usable

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 permission, privileges, and quickly identify issues.

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 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 poll workers.

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

11.2-B Authorized Users

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:	Jan. 16, 2018

Deleted: The voting system should e

Deleted: e

Moved (insertion) [1]

Deleted: 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 system¶
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:¶

Commented [FJM(4]: Consider deleting?

Source: N/A
Gap notes:

11.2-C Access control configuration

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

Applies to: voting system

Discussion

For vote-capture devices, each role may or may not have permissions for every voting state. Additionally, the permissions that a role has for a voting state may be restricted to certain functions. Table 3 shows an example matrix of 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 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 role to ensure all other users have proper access to the information necessary to perform their roles.

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

11.2-D Permissions

The voting system must allow only an administrator to create or modify permissions assigned to specific 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: Jan. 16, 2018
Source: N/A

Deleted: 11.4-D Permission and Privilege Modification ¶
The voting system must allow only administrators to modify the permissions and privileges of other roles, users and processes.¶
Applies to: voting system¶
Discussion¶
¶
Status: →New→¶
Updated:→Jan. 16, 2018¶
Source:→New → ¶
Gap notes:

Gap notes:

11.2-E Roles

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

Applies to: voting system

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

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

11.2-F Minimum Roles

At minimum, the voting system must define the roles within Table 1.

Applies to: voting system

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

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

Table 1 – Minimum Voting System Roles

ROLE	DESCRIPTION
Administrator	The administrator 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 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.

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

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

Table 2 - Voting State Descriptions

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-H Minimum Role Permissions

At minimum, the voting system must use the 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: Jan. 30, 2018
Source: N/A
Gap notes:

Table 3 - Minimum Permissions per Role

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
Poll 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	---	---	---	---

Deleted: *Table 4 - Example Access Capabilities per Role and Voting State*

Deleted: ROLE ... [1]

11.2-I Assign User

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

Applies to: voting system

Discussion

The administrator needs to have the authority to assign users to a specific role.

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

11.2-J Apply Permissions

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

Applies to: voting system

Discussion

Once the user is assigned a 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 or role.

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

11.2-K 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:	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.

Deleted: 11.3-A General Access Control Mechanisms
The voting system must provide access control mechanisms.
Applies to: voting system
Discussion
Access controls support the following concepts:
Limiting the actions of users, roles, and processes (entities) 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
Status: Updated
Updated: Jan. 17, 2017
Source: VVSG2005 I.7.2.1.2-1, I.7.2.1.2-2
Gap notes:

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:

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

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

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

11.3-B 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, wireless, and use of telecommunications

Deleted: sending / receiving

Deleted: public

- 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.

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

11.3-C Administrator multi-factor authentication

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 role.

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

11.3-D User name 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:	Jan. 2, 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 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-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:	Jan. 2, 2018
Source:	[VVSG2005] I.7.2.1.2-1
Gap notes:	

11.3-D.3 Account information for password restriction

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 or usernames and related information in 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 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: Dec. 27, 2017
Source: [VVSG2005] I.7.2.1.2-1
Gap notes:

11.4-B Separation of Duties Documentation

Voting system documentation must include suggested practices for dispersing critical operations across multiple 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: Jan. 25, 2018
Source:
Gap notes:

Deleted: **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:

Deleted: **11.4-B Minimum permissions default**
The voting system's default access control permissions must implement the minimum permissions needed for each role or group.
Applies to: voting System
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:

Deleted: **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:

Deleted: **11.4-C Critical Operations Authorization**
The voting system must ensure that an administrator authorizes each critical operation.
Applies to: voting system
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-C Separation of Duties

Other than the administrator, the voting system must not allow a single user to perform all critical operations.

Applies to: Voting system

Discussion
Proper implementation of separation of duties should assist in reducing or removing conflict of interest, fraud, and the risk of collusion.

Status:	New
Updated:	Jan. 25, 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 should 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:	Jan. 16, 2017
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

Deleted: 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¶
Once a user's access has timed-out, the user must re-authenticate to the voting system. This ensures the accessing users is authorized. ¶
Status: →New→¶
Updated:→Jan. 16, 2017¶
Source:→N/A ¶
Gap notes:¶

Discussion

This requirement prevents password guessing attacks.

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

Deleted: **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:

Page 8: [1] Deleted Franklin, Joshua M. (Fed) 2/1/18 9:39:00 PM

ROLE	PRE-VOTING	ACTIVATED	SUSPENDED	POST-VOTING
Administrator	Full Access	Full Access	Full Access	Full Access
Voter	N/A	Cast and cancel ballots	N/A	N/A
Election Judge/Precinct Captain	Open polls	Close polls, enter suspended state, handle fled voters, and recover from errors	Exit suspended state	Generate reports
Poll Worker	N/A	Activate ballot	N/A	N/A
Central Election Official	Define and load ballot	N/A	N/A	Reconcile Provisional-challenged ballots, write-ins, generate reports
Application or Process	Custom per application or process	Custom per application or process	Custom per application or process	Custom per application or process