Access Control Requirements Gap Analysis

During the mapping activity for the Access Control requirements, most requirements fit into the existing principles and guidelines. One potential modification was identified, although not strictly necessary.

The potential modification to the principles is:

- The Access Control requirements reference the following "voting states" which could be used to restrict access to various system operations during certain periods of the election.

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.

The second Access Control guideline could be amended to include consideration of the voting state, reading as follows:

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

Other areas for future changes and development to the VVSG access control requirements include:

- Duplicate requirements were found regarding the identification and authentication of users, roles, and processes throughout this section. The NIST team is looking to abstract requirements for placement in the General Access Control section.
- Requirement 5.4.2-B discusses the Role-based access control standard. NIST would like the Working Group's feedback on whether we should require adherence to this external standard (*Core RBAC in the ANSI INCITS 359-2004 American National Standard for Information Technology – Role Based Access Control*).
- Some requirements belong in other sections outside of Access Control (5.4.1-H - System Integrity and 5.4.3-D - Data Protection).
- Requirement 5.4.3-A states users should be authenticated based on the minimum authentication methods based on specifications of Table 5-4. The NIST team would like to discuss the below Table with the Working Group:

Table 5-4 Minimum authentication methods for groups and roles

GROUP OR ROLE	MINIMUM AUTHENTICATION METHOD
Election Judge	User name and password
Poll Worker	N/A – poll worker does not authenticate to voting system
Central Election Official	User name and password
Administrator	Two-factor authentication
Application or Process	Digital certificate or signature

- Requirement 5.4.3-F can be removed as it appears to be subsumed under 5.4.2-E.
- The requirements (5.4.3-G and 5.4.3-H) covering account lock out can be combined.
- Requirement 5.4.3-I and the associated sub-requirements could be placed under their own section of Access Control. This new section would cover password configuration. Also, 5.4.3-I and 5.4.3-I.1 can be combined for simplification.
- Requirement 5.4.4-C can be removed based on feasibility issues.
- Requirements 5.4.4-D and 5.4.4.-E are both covered under other requirements and the NIST team would like to discuss if these are necessary.
- The VVSG contains no requirements for any sort of biometric or token-based authentication.

5.4.1-C Access control voting states

Requirement:	The vote-capture device's access control mechanisms SHALL distinguish at least the following voting states from Part 1:Table 5-2: a. Pre-voting; b. Activated; c. Suspended; and d. Post-voting
Applies to:	Vote-capture device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	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.
Source:	[VVSG2005] I.7.2.1,I.7.2.1.1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access **Justification:** This guideline may need to be amended to include, "during the correct voting state."

5.4.1-D Access control state policies

Requirement:	The vote-capture device SHALL allow the administrator group or role to configure different access control policies available in each voting state.
Applies to:	Vote-capture device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Activated state should offer a strict subset of functions limited to voting only. Prevoting and post-voting states and other defined states may be used for other functions such as defining the ballot, collecting votes, updating software, and performing other administrative and maintenance functions. For more examples, see Part 1:Table 5-3. This requirement extends [VVSG2005] I. 7.2 by establishing vote-capture device policies for each voting state in relation to access control.
Source:	[VVSG2005] I.7.2.1.1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access **Justification:** The authentication mechanisms are configurable. This requirement allows the administrators to configure these mechanisms. The second guideline mentioned limits access based on the voting state.

5.4.1-H Software and firmware modification prevention

Requirement:	The voting device SHALL prevent modification to or tampering with software or firmware through any means other than the documented procedure for software upgrade.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement is intended to ensure that there are no ways, other than the documented procedure for software upgrade, to upgrade or modify the software. This requirement aims to protect against software vulnerabilities that would allow an unauthorized individual to secretly update, modify, or tamper with the installed software. This requirement extends [VVSG2005] I.7.2 by requiring prevention of modification and tampering with software and firmware.
Source:	[VVSG2005] I.7.2.1 and [VVSG2005] II.6.4.1
Principle(s)/ Guideline(s):	*Security: System Integrity* The voting system maintains and verifies the integrity of software, firmware, and other critical components. **Justification:** This requirement belongs under the system integrity section.

5.4.2-B Role-based access control standard

Requirement:	Voting devices that implement role-based access control SHALL 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
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I. 7.2.1.1-a by requiring role-based methods to follow ANSI INCITS 359-2004.
Source:	[VVSG2005] I.7.2.1.1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions **Justification:** The principle description describes identifying and authenticating users before granting access to system functions.

5.4.3-D Secure storage of authentication data

Requirement:	When private or secret authentication data is stored in the voting device, the data SHALL be protected to ensure that the confidentiality and integrity of the data is not violated
Applies to:	Voting device
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	Ensuring the privacy and secrecy of stored data may involve the use of encryption. This requirement extends [VVSG2005] I.7.2.1.2-g by requiring securely stored private or secret authentication data.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Data Protection* The voting system protects sensitive data from unauthorized access, modification, or deletion. **Justification:** This requirement belong under the data protection section.

5.4.3-A Minimum authentication mechanism

Requirement:	The voting device SHALL authenticate users per the minimum authentication methods outlined in Part 1:Table 5-4.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Part 1:Table 5-4 provides the minimum authentication methods required for each group or role. Stronger authentication methods than the minimum may be used for each group or role. This requirement extends [VVSG2005] I.7.2.1.2-e by requiring a minimum level of robustness for user authentication mechanisms.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations **Justification:** This guideline discusses the authentication mechanism supported by the voting system and the table mention in this guideline should be reviewed.

5.4.3-F Creation and disabling of privileged groups or roles

Requirement:	The voting device SHALL allow privileged groups or roles to be disabled and allow new individual privileged groups or roles to be created.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	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.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. **Justification:** This guideline allows the authentication mechanism to be configurable so the administrator can modify groups and roles, and their privileges.

5.4.3-G Account lock out

Requirement:	The voting device SHALL lock out groups, roles, or individuals after a specified number of consecutive failed authentications attempts within a pre-defined time period.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2 by allowing the administrator group or role flexibility in configuring the account lockout policy.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. **Justification:** This guideline allows the authentication mechanism to be configured.

5.4.3-H Account lock out configuration

Requirement:	The voting device SHALL allow the administrator group or role to configure the account lock out policy including the time period within which failed attempts must occur, the number of consecutive failed access attempts allowed before lock out, and the length of time the account is locked out.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2 by allowing the administrator group or role flexibility in configuring the account lockout policy.
Source:	[VVSG2005] I.7.2.1.2-1

Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. **Justification:** This guideline allows the authentication mechanism to be configured.

5.4.3-I User name and password management

Requirement:	If the voting device uses a user name and password authentication method, the voting device SHALL allow the administrator to enforce password strength, histories, and expiration.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2-e by requiring strong passwords, password histories, and password expiration.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. Justification: This guideline allows the authentication mechanism to be configured.

5.4.3-I.1 Password strength configuration

Requirement:	The voting device SHALL 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 nonalphanumeric characters per NIST 800-63 Electronic Authentication Guideline standards.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
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.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. Justification: This guideline allows the authentication mechanism to be configured.

5.4.4-C Dual person control

Requirement:	The voting device SHALL provide dual person control for administrative

	activities.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2-a by requiring dual person control for administrative activities.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	

5.4.4-D Explicit authorization

Requirement:	The voting device SHALL explicitly authorize subjects’ access based on access control lists or policies.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2-a by requiring explicit authorization of subjects based on access control policies.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	

5.4.4-E Explicit deny

Requirement:	The voting device SHALL explicitly deny subjects access based on access control lists or policies.
Applies to:	Voting device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement extends [VVSG2005] I.7.2.1.2-a by requiring explicit denying of subjects access based on access control policies.
Source:	[VVSG2005] I.7.2.1.2-1
Principle(s)/ Guideline(s):	**Access Control** Default access control policies enforce the principle of least privilege.