Context Description: Posted Dec. 1, 2006

This draft report was prepared by NIST staff at the request of the Technical Guidelines Development Committee (TGDC) to serve as a point of discussion at the Dec. 4-5 meeting of the TGDC. Prepared in conjunction with members of a TGDC subcommittee, the report is a discussion draft and does not represent a consensus view or recommendation from either NIST or the TGDC. It reflects the conclusions of NIST research staff for purposes of discussion. The TGDC is an advisory group to the Election Assistance Commission, which produces voluntary voting system guidelines and was established by the Help America Vote Act. NIST serves as a technical advisor to the TGDC.

The NIST research and the draft report's conclusions are based on interviews and discussions with election officials, voting system vendors, computer scientists, and other experts in the field, as well as a literature search and the technical expertise of its authors. It is intended to help in developing guidelines for the next generation of electronic voting machine to ensure that these systems are as reliable, accurate, and secure as possible. Issues of certification or decertification of voting systems currently in place are outside the scope of this document and of the TGDC's deliberations.

Chapter 1: Access Control

1.1 Introduction/Scope

Access controls limit the rights of authorized users, systems, applications, or processes and prevent unauthorized use of a resource or use of a resource in an unauthorized manner. The core components of access control include identification, authentication, enforcement, and policy. Access control mechanisms authenticate, authorize, and log access to resources to protect voting system integrity, availability, confidentiality, and accountability. Access controls provide reasonable assurance that voting system resources such as data files, application programs, underlying operating systems, and voting system equipment are protected against unauthorized access, operation, modification, disclosure, loss, or impairment.

This section addresses documentation and voting system capabilities that limit and detect access to critical voting system components in order to guard against loss of system and data integrity, availability, confidentiality, and accountability in voting systems. Access controls may be implemented in the voting software or provided by the underlying operating system or separate application programs.
Access controls include physical controls, such as keeping voting devices in locked rooms to limit physical access, and technical controls, such as security software programs designed to prevent and detect unauthorized access to resources. The access controls contained in this section address security software programs; see Section X for further information on physical and hardware security for voting systems.

1.2 Access control requirements

This subsection defines the access control requirements for voting systems. It outlines the various measures that the vendors and the voting system shall perform to ensure the security of the voting system. These recommendations apply to the full scope of voting system functionality, including functionality for defining the ballot and other pre-voting functions, as well as functions for casting and storing votes, vote reporting, system logging, and maintenance of the voting system

1.2.1 General access control requirements

General requirements address the high level functionality of a voting system. These are the fundamental access control requirements upon which other requirements in this section are based.

→ **1.2.1-A** Access control capability requirement.

The voting system shall be capable of providing access control mechanisms designed to permit authorized access to the voting system and prevent unauthorized access to the voting system.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.1-B** Control to the access control mechanism capability requirement

The voting system shall be capable of providing access control mechanisms designed to prevent unauthorized access to the access control capabilities of the voting system itself.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.1-C** Access control general security support capability requirement

The voting system shall be capable of providing access controls that supports voting system security.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

↳ **1.2.1-C.1** Access control confidentiality support capability requirement

The voting system shall be capable of providing access controls that supports confidentiality of data including casting and storing votes and voter anonymity.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

↳ **1.2.1-C.2** Access control integrity support capability requirement

The voting system shall be capable of providing access controls that supports integrity of data such as vote reporting.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

↳ **1.2.1-C.3** Access control availability support capability requirement

The voting system shall be capable of providing access controls that supports availability of data such as the voting ballot and the ability to cast, store, and report votes.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

↳ **1.2.1-C.4** Voting system access control accountability support capability requirement

The voting system shall be capable of providing access controls that supports accountability of actions such as identifying and authentication users and performing voting system event logging.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

➞ **1.2.1-D** Access control for access to software and files capability requirement

The voting system shall be capable of providing controls that limit access to voting system software and files as well as third party software and files such as the operating system, drivers, databases, etc.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.1-E** Access control detection and record creation when accessing software and files capability requirement

The voting system shall be capable of providing controls that detect and record access to voting system software and files as well as third party software and files such as the operating system, drivers, databases, etc.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

See Section 2.6 for more information on access control logging.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.1-F** Voting system modes of operation capability requirement

The voting system shall be capable of distinguishing at least the following modes: pre-voting, activated, suspended, and post-voting.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

[include link to state diagram CRT Section 5.2 Figure 12 Vote-capture device states] The various modes are described in Table 1.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

Table 1 Voting System Modes

Mode	Description
Pre-voting	This mode includes activities that occur prior to voting,

	such as loading the ballot definition. This mode may enter Activated mode.
Activated	This mode includes voting activities such as casting, printing, or spoiling a ballot. This mode may enter Suspended mode or Post-voting mode.
Suspended	This mode suspends voting activities when entered from the Activated mode by an authorized voting official for reasons such as off hours during early voting. To resume voting activities an authorized voting official exits this mode and enters the Activated mode.
Post-voting	This mode includes activities that occur after voting, such as ballot counting and reporting. An authorized voting official enters this mode from Activated mode.

→ **1.2.1-G** Access control role creation capability for administrator role requirement

The voting system shall have the capability for the voting system administrator group or role to create additional modes.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.1-H** Access control role configuration capability for administrator role requirement

The voting system shall be capable of allowing the administrator group or role to configure the voting system functions available in each mode.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.1-I** Different access control for different voting system mode capability requirement

The voting system shall be capable of applying different access controls for each mode.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Activated mode should offer a strict subset of functions limited to voting only. Pre-voting and Post-voting modes and other defined modes 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 Table 3, Roles and Modes Access Matrix.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

1.2.2 Access control documentation requirements

Documentation requirements address the minimum access control information necessary for testing and implementation of the voting system. This includes both public and private information. User documentation includes all public information that is provided to the end users. The Technical Data Package (TDP) includes the user documentation along with other private information that is viewed only by the test labs.

→ **1.2.2-A** General user and TDP documentation requirement

Vendors shall provide user and TDP documentation of access control capabilities of the voting system.

Applies to: *Voting System*

Test Reference: *Volume V, Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.2-B** Access control implementation configuration and management user documentation requirement

Vendors shall provide user documentation containing guidelines and usage instructions on implementing, configuring, and managing access control capabilities.

Applies to: *Voting System*

Test Reference: *Volume V, Section 4.1*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.2-C** Access control policy template user documentation requirement

Vendors shall provide, within the user documentation, an access control policy template or instructions to facilitate the implementation of the access control policy and associated access controls on the voting system.

Applies to: *Voting System*

Test Reference: *Volume V, Section 4.1*

D I S C U S S I O N

Access control policy requirements include the minimum baseline policy definitions necessary for testing and implementation of the voting system. The policies may be pre-defined within the voting system or provided as guidelines in the documentation.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.2-D** Model access control policy user documentation requirement

Vendors shall provide, within the user documentation, a model access control policy under which the voting system was designed to operate and a description of the hazards of deviating from this policy.

Applies to: *Voting System*

Test Reference: *Volume V, Section 4.1*

D I S C U S S I O N

The model access control policy includes the assumptions that were made when the system was designed, the justification for the policy, and the hazards of deviating from the policy.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.2-E** General access control technical specification TDP documentation requirement

Vendors shall provide descriptions and specifications of all access control mechanisms of the voting system including management capabilities of authentication, authorization, and passwords in the TDP.

Applies to: *Voting System*

Test Reference: *Volume V, Section 4.4*

D I S C U S S I O N

Access control mechanisms include those that are designed to permit authorized access to the voting system and prevent unauthorized access to the voting system. Specific examples of access control measures include but are not limited to: Use of data and user authorization, security kernels, computer-generated password keys, special protocols, message encryption, secure data transmission, and prevention of data interception.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.2-F** Control to access control capabilities technical specification TDP documentation requirement

Vendors shall provide descriptions and specifications of methods to prevent unauthorized access to the access control capabilities of the voting system in the TDP.

Applies to: *Voting System*

Test Reference: *Volume V, Section 4.4*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.2-G** Voting system mechanisms dependant on the access control mechanisms TDP documentation requirement

Vendors shall provide descriptions and specifications of all other voting system mechanisms that are dependent upon, support, and interface with access controls, such as logging, in the TDP.

Applies to: *Voting System*

Test Reference: *Volume V, Section 4.4*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

1.2.3 Access control identification requirements

Identification requirements provide controls for accountability when operating and administering a voting system. Identification applies to users, systems, applications, and processes.

→ **1.2.3-A** Access control identification capability requirement

The voting system shall be capable of identifying users, systems, applications, and processes to which access is granted and the specific functions and data to which each entity holds authorized access. Identification shall be performed using identity-based or role-based methods.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Identity-based identification explicitly identifies a user, system, application, or process by the use of a unique system-wide identifier. Each identity has defined permissions in the voting system. Accountability is provided for each identity within the voting system. In this scenario, voters must remain anonymous and be identified through a double or triple blind generation process. Role-based identification identifies users, systems, applications, and processes based on roles in an organization. Each role has defined permissions within the voting system. Users authenticate to the voting system then assume a role. Accountability is provided for each user and assumed role within the voting system. Voters remain anonymous through the use of a generic voter role. Identity-based and role-based access control methods both use rules to define permissions. Rules may be used in a voting system to provide access policies for either identity-based or role-based access control.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.3-B** Roles based access control standard requirement

Voting systems that implement role-based access control shall follow the standards and recommendations outlined in the *ANSI INCITS 359-2004 American National Standard for Information Technology – Role Based Access Control* document.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.3-C** Access control roles identification capability requirement

The voting system shall be capable of identifying, at a minimum, the categories for groups or roles outlined in Table 2. These categories shall be identified by identity-based or role-based methods. Each category may apply to different modes and perform different functions.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

A group in a voting system is defined as a set of users, systems, applications, or processes who share the same set of privileges and access permissions. In role-based access control methods a role serves the same purpose as a group. In identity-based access control methods groups are created, members are assigned to the groups, and permissions and privileges are applied to the group as a whole. The term groups and roles are often used interchangeably.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.3-D** Group member identification requirement

Members within all groups except the voter group shall be identified individually and explicitly.

Applies to: *Voting System*

Test Reference: *Volume V, Section 4.4*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

Table 2 Voting System Groups/Roles and Descriptions

Group or Role	Description
Voter	The voter can only cast or cancel a ballot. The voter cannot activate a session; the poll worker activates the session by checking in the voter and activating the ballot format. Members of this group or role are not identified since voters must remain anonymous.

Election Judge	The election judge has the ability to open the polls, close the polls, and generate reports.
Poll Worker	The poll worker checks in voters and activates the ballot format.
Central Election Official	The central election official loads ballot definitions.
Administrator	The administrator configures the system and troubleshoots system problems.
System	The system includes applications and processes at interact with the voting system.

→ **1.2.3-E** Access control configuration capability requirement

The voting system shall be capable of allowing 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, and deletion.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Each group/role may or may not have permissions for every mode. Additionally the permissions that a group/role has for a mode may be restricted to certain functions. Table 3 shows an example matrix of group or role to mode access rights.

Each jurisdiction must create and maintain its own enrollment process procedures. These procedures are used to distribute account user names and passwords to users. If email is the preferred distribution method, is recommended to use two emails, one for the user name and the other for the password. The email containing the password must be encrypted. An alternative enrollment method is to send an email containing the user name and instructions on how to obtain the password over the phone. Absence of security in the enrollment process procedures can impact authentication and access control.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

Table 3 Roles and Modes Access Matrix

Role/Modes	Pre-voting	Activated	Suspended	Post-voting
Voter	N/A	Cast and cancel	N/A	N/A

		ballots		
Election Judge	Open polls	Close polls	Enter and Exit suspended state	Generate reports
Poll Worker	N/A	Activate ballot format	N/A	N/A
Central Election Official	Define and load ballot	N/A	N/A	N/A
Administrator	Full access	Full access	Full access	Full access
System	Custom per application or process	Custom per application or process	Custom per application or process	Custom per application or process

→ **1.2.3-F** Voter anonymity preservation requirement

The voting system shall be capable of preserving voter anonymity.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

1.2.4 Access control authentication requirements

Authentication establishes the validity of the identity of the user, system, application, or process interacting with the voting system. Authentication is based on the identification provided by the user, system, application, or process interacting with the voting system. Authentication is generally classified in one of the following three categories:

(a) Something the user knows – This is usually a password, pass phrase, or PIN.

(b) Something the user has – This is usually a security token that may be either hardware or software based, such as a smart card.

(c) Something the user is – This is usually a fingerprint, retina patter, voice pattern or other biometric data.

Traditional password authentication is a single factor authentication method. A more secure method of authentication combines the various methods of authentication into two-factor authentication, or multi-factor authentication. For example, a user may use a security token and a passphrase for authentication. Using multi-factor provides stronger authentication than single factor. There are also cryptographic-based authentication methods such as digital signatures and

challenge-response authentication which are either software based or security tokens.

→ **1.2.4-A** Minimum authentication mechanism capability requirement

The voting system shall be capable of authenticating users, systems, applications, and processes using authentication mechanisms at least as robust as username and password.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Table 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.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-B** Multiple authentication mechanism capability requirement

The voting system shall provide multiple authentication methods to support multi-factor authentication.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

This requirement is need to support the multi-factor authentication of the administrator group or role of requirement **1.2.4-C**.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-C** Administrator group or role multi-factor authentication requirement

The voting system shall be capable of authenticating the administrator group or role with a multi-factor authentication mechanism.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

Table 4 Minimum Authentication Methods for Groups and Roles

Group or Role	Minimum Authentication Method
Voter	User name and password
Election Judge	User name and password
Poll Worker	N/A - need to explain reason
Central Election Official	User name and password
Administrator	Two-factor authentication
System	User name and password

→ **1.2.4-D** Prohibition of hard coded authentication data requirement

Voting systems shall not contain hard coded authentication data.

Applies to: *Voting System*

Test Reference: *Volume V, Section 4.4*

DISCUSSION

Authentication data includes passwords, passphrases, and private keys.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-E** Encrypted storage of authentication data requirement

When private or secret authentication data is stored in the voting system, the voting system shall be capable of storing the data encrypted.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-F** Setting and changing of passwords, pass phases, and keys capability requirement

The voting system shall provide the capability for the administrator group or role to set and change passwords, pass phrases, and keys.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

This requirement support jurisdictions have different policies regarding passwords, pass phrases, and keys.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-G** Creation and disabling of privileged accounts capability requirement

The voting system shall provide the capability to allow privileged accounts to be disabled and allow new individual privileged accounts to be created.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Privileged accounts include any accounts within the operating system, voting system software, or other third party software with elevated privileges such as administrator, root, maintenance accounts, etc.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-H** Privileged account user documentation requirement

The vendor shall disclose and document information on all privileged accounts included on the voting system such as name of the account, purpose, capabilities and permissions, and how to disable the account in the user documentation.

Applies to: *Voting System*

Test Reference: *Volume V, Section 4.1*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-I** Account lock out capability requirement

The voting system shall have the capability to lock out users, applications, or processes after a specified number of consecutive failed access attempts within a pre-defined time period.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-J** Account lock out configuration capability requirement

The voting system shall be capable of allowing 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 System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-K** Account lock out application capability requirement

The voting system shall be capable of allowing the administrator group or role to apply account lock out policies to specified accounts.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-L** User name and password management capability requirement

If the voting system uses a user name and password authentication method, it shall be capable of allowing the administrator to enforce password strength, histories, and expiration.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-L.1** Password strength configuration capability requirement

The voting system shall have the capability to 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 System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-L.2** Common word usage for password configuration capability requirement

The voting system shall be capable of restricting the use of common words for passwords.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-L.3** Password history configuration capability requirement

The voting system shall be capable of enforcing password histories and allowing the administrator to configure the history length.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-L.4** Account information for password restriction capability requirement

The voting system shall be capable of ensuring that the username or other associated information is not used in the password.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-L.5** Automated password expiration capability requirement

The voting system shall be capable of providing a means to automatically expire unchanged passwords in accordance with the voting jurisdiction's policies.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-L.6** Password expiration warning capability requirement

The voting system shall be capable of providing users advance warning that their passwords are going to expire if they are not changed.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-L.7** Length of time between password change and advance warning configuration capability requirement

The voting system shall permit system administrators to specify the length of time between password changes and the length of advance warning provided to users to change passwords.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-M** Security token management capability requirement

If the voting system uses security tokens for authentication, it shall be capable of allowing the administrator to program and reset the security token.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-M.1** Authentication between security token and voting equipment capability requirement

The voting system shall be capable of authenticating the security token to the voting equipment.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-M.2** Voting equipment to security token authentication capability requirement

The voting system shall be capable of authenticating the voting terminal to the security token.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-M.3** Security token encryption capability requirement

The voting system shall be capable of encrypting the contents, such as the keys, on the security tokens.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-M.4** Security token elevated access capability requirement

The voting system shall be capable of supporting an administrator security token that allows elevated access privileges, such as changing modes and ending the election.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-M.5** Security token personal identification number (PIN) capability requirement

The voting system shall be capable of enabling a personal identification number (PIN) on security tokens.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-M.6** Voter security token one time use capability requirement

The voting system shall be capable of resetting the voter security token to ensure that it can only be used for a single voting session.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.4-M.7** Voter security token functionality limit requirement

The voting system shall be capable of denying voter security tokens access to any functions beyond casting or spoiling a vote.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

1.2.5 Access control authorization requirements

Authorization is the process of determining access rights based on authentication of a user, system, application, or process within a voting system. Authorization permits or denies access to an object by a subject. Subjects may be users, systems, applications, or processes that interact with the voting system. Objects may be files or programs within the voting system.

→ **1.2.5-A** Account access to election data authorization requirement

The voting system shall be able to ensure that only authorized accounts have access to all election data.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.5-B** Separation of duties capability requirement

The voting system shall provide the ability to enforce separation of duty across subjects based on user identity, groups, or roles.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.5-C** Dual person control capability requirement

The voting system shall be capable of providing dual person control.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.5-D** Explicit authorization capability requirement

The voting system shall have the capability to explicitly authorize subjects' access based on access control lists or policies.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.5-E** Explicit deny capability requirement

The voting system shall have the capability to explicitly deny subjects access based on access control lists or policies.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.5-F** Authorization identification capability requirement

The voting system shall be capable of identifying each person, application, or process entity to who access is granted (other than voters, who shall be only identified generically), and restrict access to the specific functionality and data to which access is unauthorized..

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.5-G** Authorization limits capability requirement

The voting system shall have the capability to limit the length of authorization to a specific time, time interval, or voting mode.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

1.2.6 Access control logging requirements

Logging is the recording of activity within a voting system. Activities that should be logged within a voting system with regards to access control include access attempts, account creation and modification, and file creation, modification, and deletion. For more information on logging, see Section System Event Logging.

→ **1.2.6-A** System access logging capability requirement

The voting system shall be capable of logging each system access with a timestamp and identifying data.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.6-B** Access control configuration change logging capability requirement

The voting system shall be capable of logging changes to the access control configuration of the voting system.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.6-C** Access control account, groups, and role configuration change logging capability requirement

The voting system shall be capable of logging the creation, deletion, and modification of accounts, groups, and roles including disabling accounts and changing account privileges.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.6-D** Access to file logging capability requirement

The voting system shall be capable of logging the addition, modification, and deletion of files.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.6-E** Access control logging configuration capability requirement

The voting system shall be capable of allowing the administrator group or role to configure logging policies, including logged events and logging granularity.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

1.2.7 Access control enforcement requirements

Access control is enforced based on authentication and access rights. Access rights are applied by an access control list (ACL) or access control matrix that defines permission and capabilities within a voting system based on authentication. Within a voting system access controls differ based on the voting mode.

→ **1.2.7-A** Access control application and enforcement capability requirement

The voting system shall be capable of applying and enforcing access controls for each voting mode.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.7-B** Voter access control capability requirement

In Activated mode, the voting system shall be capable of applying the voter access controls upon the termination and restart for each voting session.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Within the Activated mode a voting session is defined as the period of time between ballot activation and printing, casting, or spoiling a ballot. For more information see the Vote-capture device states diagram in Section 5.2 of the CRT.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.7-C** One cast ballot per voting session capability requirement

In Activated mode, the voting system shall have the capability to enforce that only one ballot is cast within the voting session.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.7-D** Limitation of voter access capability requirement

In Activated mode, the voting system shall be capable of permitting a voter to cast a ballot while precluding voter access to all aspects of the voting system not required by the voter to cast a ballot.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.7-E** Stand by mode timeout configuration capability requirement

In Activated mode, the voting system shall be capable of entering a system standby state after some fixed period of idle time configurable by the administrator group or role.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.7-F** Exit of stand by mode capability requirement

In order to exit the suspension or standby state, an authorized user shall perform an action, such as entering a password, to enable the system.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

D I S C U S S I O N

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

Impact: *Click here to add the Impact*

1.2.8 Access control enforcement requirements

Voting systems may use telecommunications to communicate between system components and locations. For example, voting systems may communicate on a network to transmit data to a central system. The voting systems may also be accessed remotely for administration and software installation. When using network communications with a voting system, additional security controls should be implemented to protect the data in transit, including authentication and access control information.

→ **1.2.8-A** Access control for remote access capability requirement

Voting systems that use network communications between components or other forms of remote access shall be subject to the same access control requirements as standalone voting systems.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.8-B** Remote access encryption capability requirement

The voting system shall be capable of encrypting all remote access communications.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.8-C** Remote access cryptography requirement

The voting system shall implement Section X cryptographic requirements for remote access communications.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

Click here and type the discussion about this requirement

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.8-D** Remote access account, group, and roles restriction capability requirement

The voting system shall have the capability to limit the accounts, groups, or roles that are accessed remotely.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

For example, restricting the remote access capability to an administrator subgroup with limited permissions and functionality is a recommended security control.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.8-E** Remote access mode restriction capability requirement

The voting system shall have the capability to restrict remote access to certain modes.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

For example, denying remote access functionality during Activated mode is a recommended security control.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*

→ **1.2.8-F** Remote access strong authenication capability requirement

I The voting system shall have the capability to apply strong authentication methods over remote access per *NIST 800-63 Electronic Authentication Guideline* standards for Level 4 authentication.

Applies to: *Voting System*

Test Reference: *Volume V, Section 5.2*

DISCUSSION

The *NIST 800-63 Electronic Authentication Guideline* recommends Level 4 authentication to provide the highest practical remote network authentication

assurance. Level 4 authentication requires a physical hardware token and is based on proof of possession of the token through a FIPS 140-2 Level 2 or higher cryptographic protocol.

Source: *Click here to add the Source*

Impact: *Click here to add the Impact*