Access Control

1 Introduction and 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.[i]

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. [ii] 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.

2 Access Control Requirements for Voting Systems

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.[iii]

2.1 General

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.

2.1.1 The voting system shall be capable of providing access controls that ensure voting system security in the following areas:

2.1.1.1 The voting system shall provide confidentiality of data including casting and storing votes and voter anonymity.

2.1.1.2 The voting system shall provide integrity of data such as vote reporting.

2.1.1.3 The voting system shall provide availability of data such as the voting ballot and the ability to cast, store, and report votes.

2.1.1.4 The voting system shall provide accountability of actions such as identifying and authenticating users and performing event logging.

2.1.2 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.

2.1.3 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.

2.1.4 The voting system shall be capable of operating in at least the following modes: pre-voting, open, suspended, and post-voting. [include link to state diagram 5.2 Vote-capture device state model]

Discussion: The various modes are described in Table 1.

Mode	Description
Pre-voting	Steps that occur prior to opening the polls, such as ballot definition.
Open	Steps that occur during voting such as casting or canceling a ballot.
Suspended	Voting may be suspended by an authorized voting official.
Post-voting	Steps that occur after the polls close, such as ballot counting and reporting.

Table 1 Voting System Modes

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

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

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

2.2 Documentation

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.

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

2.2.2 Vendors shall provide usage instructions on configuring and managing access control capabilities.

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

2.2.4 Vendors shall provide detailed descriptions of all other voting system mechanisms that support and interact with access control such as logging.

2.2.5 Vendors shall provide detailed descriptions of methods to prevent unauthorized access to the access control capabilities of the voting system.

2.3 Security Policy Template

Security 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.

2.3.1 Vendors shall provide an up-to-date access control policy template or instructions to facilitate the implementation of the access control policy and associated access controls on the voting system.

2.4 Identification

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

2.4.1 The voting system shall be capable of identifying users, systems, applications, and processes. Identification shall include identity-based or role-based methods.

Discussion: 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 shall 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. Accountability is provided for each role within the voting system and is not as granular as identity-based identification. Voters remain anonymous through the use of a generic voter role. Rules-based identification does not explicitly identify a user, system, application, or process, therefore accountability is lost. 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.

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

Discussion: 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. Members within all groups accept the voter group shall be identified explicitly. The term groups and roles are used interchangeably throughout this section.

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 giving the voter the smart card. Members of this group are identified generically.
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 and deactivates smart cards.
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.

Table 2 Voting System Groups/Roles and Descriptions

2.4.3 The voting system shall be capable of allowing the administrator role to configure the permissions and functionality for each identity and group, to include account and group creation, modification, and deletion. Each group may or may not have permissions for every mode. Additionally the permissions that a group has for a mode may be restricted to certain functions. Table 3 shows an example matrix of group to mode access rights.

Group/Modes	Pre-voting	Open	Suspended	Post-voting
Voter	N/A	Cast and cancel ballots	N/A	N/A
Election Judge	Open polls	Close polls	Enter and Exit suspended state	Generate reports
Poll Worker	N/A	N/A	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

Table 3 Roles and Modes Access Matrix

2.4.4 The voting system shall be capable of preserving voter anonymity.

2.5 Authentication

Authentication establishes the validity of the identity of the user, system, application, or process interacting with the voting system. Authentication is based on the provided identification and other security information, such as a password, provided by the user, system, application, or process interacting with the voting system.

2.5.1 The voting system shall be capable of authenticating users, systems, applications, and processes with a minimum of username and password. The voting system may provide additional authentication methods such as smartcard or biometrics.

2.5.2 The voting system shall be capable of authenticating the administrator role with a stronger authentication mechanism, such as two-factor authentication.

2.5.3 Authentication data shall not be stored hard coded in the voting system or kept unencrypted in a file or database on the same voting system.

2.5.4 If private or secret authentication data is stored in the voting system, the voting system shall be capable of storing the data encrypted. Authentication data includes passwords, passphrases, and private keys.

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

Discussion: Jurisdictions have different policies regarding passwords, pass phrases, and keys. This requirement allows for that flexibility.

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

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.

2.5.6.1 The vendor shall disclose information on all privileged accounts included on the voting system.

2.5.7 The voting system shall have the capability to allow the administrator 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.

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

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

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

2.5.11 The voting system shall be capable of providing a means to automatically expire unchanged passwords in accordance with the

voting jurisdiction's policies. Users shall be given advance warning that their passwords are going to expire if they are not changed. 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.

2.5.12 The voting system shall have the capability to lock out users, applications, or processes after *X* consecutive failed access attempts within a pre-defined time period. The voting system shall be capable of allowing the administrator 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. The voting system shall be capable of allowing the administrator role to apply account lock out policies to specified accounts.

2.6 Authorization

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.

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

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

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

2.6.4 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 authorized.

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

2.7 Logging

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.

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

2.7.2 The voting system shall be capable of logging changes to the security configuration of the voting system.

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

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

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

2.8 Access control enforcement

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.

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

2.8.2 In Open 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.

2.8.3 In Open mode the voting system shall have the capability to enforce that the voting session casts only one ballot.

2.8.4 In Open mode the voting system shall be capable of applying the appropriate access controls upon the termination and restart for each voting session.

2.8.5 In Open mode the voting system shall be capable of entering a system suspension or standby state after some fixed period of idle time configurable by the administrator role. In order to exit the suspension or standby state an authorized user must perform an action, such as entering a password, to enable the system.

2.9 Communications

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.

2.9.1 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.

2.9.2 The voting system shall be capable of encrypting all remote access communications, see Section *X* for further information on cryptography standards.

2.9.3 The voting system shall have the capability to limit the accounts, groups, or roles that are accessed remotely. For example, restricting the remote access capability to an administrator subgroup with limited permissions and functionality is a recommended security control.

2.9.4 The voting system shall have the capability to restrict remote access to certain modes. For example, denying remote access functionality during Open mode is a recommended security control.

2.9.5 The voting system shall have the capability to apply stronger authentication methods over remote access such as secure tokens or challenge/response methods.

---

[i] Federal Election Commission. *Voting Systems Performance and Test Standards: An Overview*. 2002

[ii] Federal Election Commission. *Voting Systems Performance and Test Standards: An Overview*. 2002

[iii] Federal Election Commission. *Voting Systems Performance and Test Standards: An Overview*. 2002