6.1 Scope

This section describes essential security capabilities for a voting system, encompassing the system's hardware, software, communications, and documentation. The Standards recognize that no predefined set of security standards will address and defeat all conceivable or theoretical threats. However, the Standards articulate requirements to achieve acceptable levels of integrity, reliability, and inviolability. Ultimately, the objectives of the security standards for voting systems are:

- To establish and maintain controls that can ensure that accidents, inadvertent mistakes, and errors are minimized,
- To protect the system from intentional manipulation and fraud, and from malicious mischief,
- To identify fraudulent or erroneous changes to the system, and
- To protect secrecy in the voting process.

The Standards are intended to address a broad range of risks to the integrity of a voting system. While it is not possible to identify all potential risks, the Standards identify several types of risk that must be addressed by a voting system. These include:

- Unauthorized changes to system capabilities for:
  - Defining ballot formats,
  - Casting and recording votes,
  - Calculating vote totals consistent with defined ballot formats, and
  - Reporting vote totals,
- Alteration of voting system audit trails,
- Changing, or preventing the recording of, a vote,
- Introducing data for a vote not cast by a registered voter,
- Changing calculated vote totals,
- Preventing access to vote data, including individual votes and vote totals, to unauthorized individuals, and
- Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes cast by the voter.

This section describes specific capabilities that vendors shall integrate into a voting system in order to address the risks listed above.

6.1.1 System Components and Sources

The requirements of this section apply to the broad range of hardware, software, communications components, and documentation that comprises a voting system. These requirements apply to components:

- Provided by the voting system vendor and the vendor's suppliers,
- Furnished by an external provider (for example providers of personal computers and commercial off-the-shelf (COTS) operating systems) where the components are capable of being used during voting system operation, and
- Developed by a voting jurisdiction.

6.1.2 Location and Control of Software and Hardware on Which it Operates

The requirements of this section apply to all software used in any manner to support any voting-related activity, regardless of the ownership of the software or the ownership and location of the hardware on which the software is installed or operated. These requirements apply to software that operates on:

- Voting devices and vote counting devices installed at polling places under the control or authority of the voting jurisdiction, and
- Ballot printers, vote counting devices, and other hardware typically installed at central or precinct locations (including contractor facilities).

However, some requirements are applicable only in circumstances specified by this section.

6.1.3 Elements of Security Outside Vendor Control

The requirements of this section apply to the capabilities of a voting system provided by the vendor. The Standards recognizes that effective security requires safeguards beyond those provided by the vendor. Effective security demands diligent security practices by the purchasing jurisdiction and the jurisdictions representatives. These practices include:

- Administrative and management controls for the voting system and election management, including access controls,
- Internal security procedures,
- Adherence to, and enforcement of, operational procedures (e.g., effective password management),
- Security of physical facilities, and

- Organizational responsibilities and personnel screening.

Because specific standards for these elements are not under the direct control of the vendor, they will be addressed in forthcoming Operational Guidelines that address best practices for jurisdictions conducting elections and managing the operation of voting systems.

6.1.4 Organization of this Section

The standards presented in this section are organized as follows:

- **Access Control**: These standards addresses procedures and system capabilities that limit or detect access to critical system components in order to guard against loss of system integrity, availability, confidentiality, and accountability.

- **Equipment and Data Security**: These standards address physical security measures and procedures that prevent disruption of the voting process at the poll site and corruption of voting data.

- **Software Security**: These standards address the installation of software, including firmware, in the voting system and the protection against malicious software.

- **Telecommunication and Data Transmission**: These standards address security for the electronic transmission of data between system components or locations over both private and public networks

- **Security for Transmission of Official Data Over Public Communications Networks**: These standards address security for systems that communicate individual votes or vote totals over public communications networks.

It should be noted that computer-generated audit controls facilitate system security and are an integral part of software capability. These audit requirements are presented in Section 4.

6.2 Access Control

Access controls are procedures and system capabilities that detect or limit access to system components in order to guard against loss of system integrity, availability, confidentiality, and accountability. Access controls provide reasonable assurance that system resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized operation, modification, disclosure, loss, or impairment. Unauthorized operations include modification of compiled or interpreted code, run-time alteration of flow control logic or of data, and abstraction of

raw or processed voting data in any form other than a standard output report by an authorized operator.
Access controls may include physical controls, such as keeping computers in locked rooms to limit physical access, and technical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. The access controls contained in this section of the Standards are limited to those controls required of system vendors. Access controls required of jurisdictions will be addressed in future documents detailing operational guidelines for jurisdictions.

6.2.1 Access Control Policy

The vendor shall specify the general features and capabilities of the access control policy recommended to provide effective voting system security.

6.2.1.1 General Access Control Policy

Although the jurisdiction in which the voting system is operated is responsible for determining the access policies applying to each election, the vendor shall provide a description of recommended policies for:

a. Software access controls,

b. Hardware access controls,

c. Communications,

d. Effective password management,

e. Protection abilities of a particular operating system,

f. General characteristics of supervisory access privileges,

g. Segregation of duties, and

h. Any additional relevant characteristics.

6.2.1.2 Individual Access Privileges

Voting system vendors shall:

a. Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access,

b. Specify whether an individual's authorization is limited to a specific time, time interval, or phase of the voting or counting operations, and

c. Permit the voter to cast a ballot expeditiously, but preclude voter access to all other aspects of the vote-counting processes.

6.2.2 Access Control Measures

Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include:

a. Use of data and user authorization,

b. Program unit ownership and other regional boundaries,

c. One-end or two-end port protection devices,

d. Security kernels,

e. Computer-generated password keys,

f. Special protocols,

g. Message encryption, and

h. Controlled access security.

Vendors also shall define and provide a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself.

6.3 Physical Security Measures

A voting system's sensitivity to disruption or corruption of data depends, in part, on the physical location of equipment and data media, and on the establishment of secure telecommunications among various locations. Most often, the disruption of voting and vote counting results from a physical violation of one or more areas of the system thought to be protected. Therefore, security procedures shall address physical threats and the corresponding means to defeat them.

6.3.1 Polling Place Security

For polling place operations, vendors shall develop and provide detailed documentation of measures to anticipate and counteract vandalism, civil disobedience, and similar occurrences. The measures shall:

a. Allow the immediate detection of tampering with vote casting devices and precinct ballot counters, and

b. Control physical access to a telecommunications link if such a link is used.

6.3.2 Central Count Location Security

Vendors shall develop and document in detail the measures to be taken in a central counting environment. These measures shall include physical and procedural controls related to the:

a. Handling of ballot boxes,

b. Preparing of ballots for counting,

c. Counting operations, and

d. Reporting data.

6.4 Software Security

Voting systems shall meet specific security requirements for the installation of software and for protection against malicious software.

6.4.1 Software and Firmware Installation

The system shall meet the following requirements for installation of software, including hardware with embedded firmware:

a. If software is resident in the system as firmware, the vendor shall require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations,

b. To prevent alteration of executable code, no software shall be permanently installed or resident in the system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware,

c. The system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote-counting program, and its associated exception handlers,

d. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as computer chip) other than the component on which the operating system resides; and

e. After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.

6.4.2 Protection Against Malicious Software

Voting systems shall deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs. Vendors shall develop and document the procedures to be followed to ensure that such protection is maintained in a current status.

6.5 Telecommunications and Data Transmission

There are four areas that must be addressed by telecommunications and data transmission security capabilities:

- Access control for telecommunications capabilities,
- Data integrity,
- Detection and prevention of data interception, and
- Protection against external threats to which commercial products used by a voting system may be susceptible.

6.5.1 Access Control

Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function.

6.5.2 Data Integrity

Voting systems that use electrical or optical transmission of data shall ensure the receipt of valid vote records is verified at the receiving station. This should include standard transmission error detection and correction methods such as checksums or message digest hashes. Verification of correct transmission shall occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.

6.5.3 Data Interception Prevention

Voting systems that use telecommunications as defined in Section 5 to communicate between system components and locations before the poll site is officially closed shall:

a. Implement an encryption standard currently documented and validated for use by an agency of the U.S. Federal Government; and

b. Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System.

6.5.4 Protection Against External Threats

Voting systems that use public telecommunications networks shall implement protections against external threats to which commercial products used in the system may be susceptible.

6.5.4.1 Identification of COTS Products

Voting systems that use public telecommunications networks shall provide system documentation that clearly identifies all COTS hardware and software products and communications services used in the development and/or operation of the voting system, including:

a. Operating systems,

b. Communications routers,

c. Modem drivers, and

d. Dial-up networking software.

Such documentation shall identify the name, vendor, and version used for each such component.

6.5.4.2 Use of Protective Software

Voting systems that use public telecommunications networks shall use protective software at the receiving-end of all communications paths to:

a. Detect the presence of a threat in a transmission,

b. Remove the threat from infected files/data,

c. Prevent against storage of the threat anywhere on the receiving device,

d. Provide the capability to confirm that no threats are stored in system memory and in connected storage media, and

e. Provide data to the system audit log indicating the detection of a threat and the processing performed.

Vendors shall use multiple forms of protective software as needed to provide capabilities for the full range of products used by the voting system.

6.5.4.3 Monitoring and Responding to External Threats

Voting systems that use public telecommunications networks may become vulnerable, by virtue of their system components, to external threats to the accuracy and integrity of vote recording, vote counting, and vote consolidation and reporting processes. Therefore, vendors of such systems shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to:

a. Monitor threats, such as through the review of assessments, advisories, and alerts for COTS components issued by the Computer Emergency Response Team (CERT), for which a current listing can be found at http://www.cert.org, the National Infrastructure Protection Center (NIPC), for which a current listing can be found at http://www.nipc.gov/warnings/warnings.htm, and the Federal Computer Incident Response Capability (FedCIRC), for which additional information can be found at http://www.fedcirc.gov/,

b. Evaluate the threats and, if any, proposed responses,

c. Develop responsive updates to the system and/or corrective procedures,

d. Submit the proposed response to the ITAs and appropriate states for approval, identifying the exact changes and whether or not they are temporary or permanent,

e. After implementation of the proposed response is approved by the state, assist clients, either directly or through detailed written procedures, how to update their systems and/or to implement the corrective procedures no later than one month before an election, and

f. Address threats emerging too late to correct the system at least one month before the election, including:

   1) Providing prompt, emergency notification to the ITAs and the affected states and user jurisdictions,

   2) Assisting client jurisdictions directly, or advising them through detailed written procedures, to disable the public telecommunications mode of the system, and

   3) After the election, modifying the system to address the threat, submitting the modified system to an ITA and appropriate state certification authority for approval, and assisting client jurisdictions directly, or advising them through detailed written procedures, to update their systems and/or to implement the corrective procedures after approval.

6.5.5 Shared Operating Environment

Ballot recording and vote counting can be performed in either a dedicated or non-dedicated environment. If ballot recording and vote counting operations are performed in

an environment that is shared with other data processing functions, both hardware and software features shall be present to protect the integrity of vote counting and of vote data. Systems that use a shared operating environment shall:

a. Use security procedures and logging records to control access to system functions,

b. Partition or compartmentalize voting system functions from other concurrent functions at least logically, and preferably physically as well,

c. Controlled system access by means of passwords, and restriction of account access to necessary functions only, and

d. Have capabilities in place to control the flow of information, precluding data leakage through shared system resources.

6.5.6 Access to Incomplete Election Returns and Interactive Queries

If the voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, the system shall:

a. For equipment that operates in a central counting environment, be designed to provide external access to incomplete election returns only if that access for these purposes is authorized by the statutes and regulations of the using agency. This requirement applies as well to polling place equipment that contains a removable memory module, or that may be removed in its entirety to a central place for the consolidation of polling place returns.

b. Use voting system software and its security environment designed such that data accessible to interactive queries resides in an external file, or database, that is created and maintained by the elections software under the restrictions applying to any other output report, namely, that:

   1) The output file or database has no provision for write-access back to the system.

   2) Persons whose only authorized access is to the file or database are denied write-access, both to the file or database, and to the system.

6.6 Security for Transmission of Official Data Over Public Communications Networks

DRE systems that transmit data over public telecommunications networks face security risks that are not present in other DRE systems. This section describes standards applicable to DRE systems that use public telecommunications networks.

6.6.1 General Security Requirements for Systems Transmitting Data Over Public Networks

All systems that transmit data over public telecommunications networks shall:

a. Preserve the secrecy of a voter's ballot choices, and prevent anyone from violating ballot privacy,

b. Employ digital signature for all communications between the vote server and other devices that communicate with the server over the network, and

c. Require that at least two authorized election officials activate any critical operation regarding the processing of ballots transmitted over a public communications network takes place, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of votes.

6.6.2 Voting Process Security for Casting Individual Ballots over a Public Telecommunications Network

Systems designed for transmission of telecommunications over public networks shall meet security standards that address the security risks attendant with the casting of ballots from poll sites controlled by election officials using voting devices configured and installed by election officials and/or their vendor or contractor, and using in-person authentication of individual voters.

6.6.2.1 Documentation of Mandatory Security Activities

Vendors of systems that cast individual ballots over a public telecommunications network shall provide detailed descriptions of:

a. All activities mandatory to ensuring effective system security to be performed in setting up the system for operation, including testing of security before an election; and

b. All activities that should be prohibited during system setup and during the time frame for voting operations, including both the hours when polls are open and when polls are closed.

6.6.2.2 Capabilities to Operate During Interruption of Telecommunications Capabilities

These systems shall provide the following capabilities to provide resistance to interruptions of telecommunications service that prevent voting devices at the poll site from communicating with external components via telecommunications:

a. Detect the occurrence of a telecommunications interruption at the poll site and switch to an alternative mode of operation that is not dependent on the connection between poll site voting devices and external system components,

b. Provide an alternate mode of operation that includes the functionality of a conventional DRE machine without losing any single vote,

c. Create and preserve an audit trail of every vote cast during the period of interrupted communication and system operation in conventional DRE system mode,

d. Upon reestablishment of communications, transmit and process votes accumulated while operating in conventional DRE system mode with all security safeguards in effect, and

e. Ensure that all safeguards related to voter identification and authentication are not affected by the procedures employed by the system to counteract potential interruptions of telecommunications capabilities.