



- Requirements regarding the use of wireless communications
- Requirements for DREs with voter verifiable paper trail components

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

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

The requirements 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
- Ballot printers, vote counting devices, and other hardware typically installed at central or precinct locations (including contractor facilities)

### **7.1.1 Elements of Security Outside Vendor Control**

The requirements of this section apply to the capabilities of a voting system that must be provided by the vendor. However, an effective security program requires well-defined security practices by the purchasing jurisdiction and the personnel managing and operating the system. 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
- Organizational responsibilities and personnel screening

Because implementation of these elements is not under the control of the vendor, they will be addressed in the forthcoming Management Guidelines that will address the procedural aspects of conducting elections and managing the operation of voting systems. However, vendors must provide appropriate system capabilities to enable the implementation of management controls.

## 7.1.2 Organization of This Section

The guidelines presented in this section are organized as follows:

**Access Control:** These standards address 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.

**Physical Security:** These standards address physical security measures and procedures that prevent disruption of the voting process at the polling place 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. 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 Subsection 5.4.

**Telecommunications and Data Transmission:** These standards address security for the electronic transmission of data between system components or locations over private, public, and wireless networks.

**Use of Public Communications Networks:** These standards address security for systems that communicate individual votes or vote totals over public communications networks.

**Wireless Communications:** These standards address the security of the voting system and voting data when wireless is used.

**Independent Verification Systems:** This section provides an introduction to the concept of independent verification as a method to demonstrate voting system integrity. This discussion provides the context for the requirements for DREs with voter verifiable paper audit trails.

**Direct-Recording Electronic Systems with Voter Verifiable Paper Audit Trails (optional):** This capability is not required for national certification. These guidelines are provided for use by states that require this feature for DRE systems.

## 7.2 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 described in this section are limited to those controls required to be provided by system vendors.

## **7.2.1 General Access Control Policy**

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

Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for 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
- h. Any additional relevant characteristics

### **7.2.1.1 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
- c. Permit the voter to cast a ballot expeditiously, but preclude voter access to all aspects of the vote counting processes

### **7.2.1.2 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
- 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.

## **7.3 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.

### **7.3.1 Polling Place Security**

For polling place operations, vendors shall develop and provide detailed documentation of measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences.

The measures shall allow the immediate detection of tampering with vote casting devices and precinct ballot counters. They also shall control physical access to a telecommunications link if such a link is used

## **7.3.2 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 handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.

## **7.4 Software Security**

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

### **7.4.1 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 voting 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 voting 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 a computer chip) other than the component on which the operating system resides.
- e. After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.

### **7.4.2 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.

### **7.4.3 Software Distribution and Setup Validation**

Subsections 7.4.4, 7.4.5 and 7.4.6 specify requirements for the distribution of voting system software and the setup validation performed on voting system equipment. These requirements are applicable to voting systems that have completed certification testing. The goal of the software distribution requirements is to ensure that the correct voting system software has been distributed without modification. The goal of setup validation requirements, including requirements for verifying the presence of certified software and the absence of other software, is to ensure that voting system equipment is in a proper initial state before being used.

In general, a voting system can be considered to be composed of multiple associated systems including polling place systems, central counting/aggregation systems, and election management systems. These other systems may reside on different computer platforms at different locations and run different software. Voting system software is considered to be all executable code and associated configuration files critical for the proper operation of the voting system regardless of the location of installation and functionality provided. This includes third party software such as operating systems, drivers, and database management systems.

### **7.4.4 Software Distribution**

- a. The vendor shall document all software including voting system software, third party software (such as operating systems and drivers) to be installed on the certified voting system, and installation programs.
  - i. The documentation shall have a unique identifier (such as a serial number or part number) for the following set of information: documentation, software vendor name, product name, version, the certification application number of the voting system, file names and paths or other location information (such as storage addresses) of the software.
  - ii. The documentation shall designate all software files as static, semi-static or dynamic.

Discussion: Static voting system software such as executable code does not change based on the election being conducted or the voting equipment upon which it is installed. Semi-static voting system software contains configuration information for the voting system based on the voting equipment that is installed and the election being conducted. Semi-static software is only modified during the installation of (a) the voting system software on voting equipment or (b) the election-specific software such

as ballot formats. Dynamic voting system software changes over time once installed on voting equipment. However, the specific time or value of the change in the dynamic software is usually unknown in advance, making it impossible to create reference information to verify the software.

- b. The EAC accredited testing lab shall witness the final build of the executable version of the certified voting system software performed by the vendor.
- i. The testing lab shall create a complete record of the build that includes: a unique identifier (such as a serial number) for the complete record; a list of unique identifiers of unalterable storage media associated with the record; the time, date, location, names and signatures of all people present; the source code and resulting executable file names; the version of voting system software; the certification application number of the voting system; the name and versions of all (including third party) libraries; and the name, version, and configuration files of the development environment used for the build.
  - ii. The record of the source code and executable files shall be made on unalterable storage media. Each piece of media shall have a unique identifier.

Discussion: Unalterable storage media includes technology such as a CD-R, but not CD-RW. The unique identifiers appear on indelibly printed labels and in a digitally signed file on the unalterable storage media.

- iii. The testing lab shall retain this record until notified by the EAC that it can be archived.
- c. After EAC certification has been granted, the testing lab shall create a subset of the complete record of the build that includes a unique identifier (such as a serial number) of the subset, the unique identifier of the complete record, a list of unique identifiers of unalterable storage media associated with the subset, the vendor and product name, the version of voting system software, the certification number of the voting system, and all the files that resulted from the build and binary images of all installation programs.
- iii. The record of the software shall be made on unalterable storage media. Each piece of media shall have a unique identifier.
  - iv. The testing lab shall retain a copy, send a copy to the vendor, and send a copy to the NIST National Software Reference Library (NSRL)<sup>2</sup> and/or to any repository designated by a State.

---

<sup>2</sup> The National Software Reference Library (NSRL) is a repository of software maintained by the National Institute of Standards and Technology. It was designed to meet the need for court admissible evidence in the identification of software files. The EAC has designated the NSRL as a repository for voting system software. Information is available at [www.nsrl.nist.gov](http://www.nsrl.nist.gov).

- v. The NSRL shall retain this software until notified by the EAC that it can be archived.
- d. The vendor shall provide the NSRL and any repository designated by a state with a copy of the software installation disk, which the vendor will distribute to purchasers-- including the executable binary images of all third party software.
  - i. All voting system software, installation programs and third party software (such as operating systems and drivers) used to install or to be installed on voting system equipment shall be distributed using unalterable storage media.
  - ii. The vendor shall document that the process used to verify the software distributed on unalterable storage media is the certified software by using the reference information provided by the NSRL or other designated repository before installing the software.
- e. The voting system equipment shall be designed to allow the voting system administrator to verify that the software is the certified software by comparing it to reference information produced by the NSRL or other designated repository.
- f. The vendors and testing labs shall document to whom they provide voting system software.

### **7.4.5 Software Reference Information**

The NSRL or other repository designated by a state election office shall generate reference information using the binary images of the (a) certified voting system software received on unalterable storage media from testing labs and (b) election- specific software received on unalterable storage media from jurisdictions.

- a. The NSRL or other designated repository shall generate reference information in at least one of the following forms: (a) complete binary images, (b) cryptographic hash values or (c) digital signatures of the software.

Discussion: Although binary images, cryptographic hashes, and digital signatures can detect a modification or alteration in the software, they cannot determine if the change to the software was accidental or intentional.

- b. The NSRL or other designated repository shall create a record of the creation of reference information that includes: a unique identifier (such as a serial number) for the record; the file names of software and associated unique identifier(s) of the unalterable storage media from which reference information is generated; the time, date and name of people who generated reference information; the type of reference information created; the certification number of the voting system; the voting system software version; the product name; and the vendor name.

- c. The NSRL or other designated repository shall retain the unalterable storage media used to generate the reference information until notified by the EAC that it can be archived.

### **7.4.5.1 Hashes and Digital Signatures**

- a. The NSRL or other designated repository that generates hash value and/or digital signature reference information shall use FIPS-approved algorithms for hashing and signing.
  - i. The NSRL or other designated repository that generates hash values, digital signatures reference information or cryptographic keys shall use a FIPS 140-2 level 1 or higher validated cryptographic module.

Discussion: See <http://www.csrc.nist.gov/cryptval/> for information on FIPS 140-2.

- ii. The NSRL or other designated repository that generates sets of hash values and digital signatures for reference information shall include a hash value or digital signature covering the set of reference information.
- b. If the NSRL or other designated repository uses public key technology, the following requirements shall be met:
  - i. Public and private key pairs used by the repository to generate digital signatures shall be 2048-bits or greater in length
  - ii. The repository's private keys used to generate digital signature reference information shall be used for no more than three years
  - iii. Public keys used to verify digital signature reference information shall be placed on unalterable storage media if not contained in a signed non-proprietary format for distribution.

Discussion: Examples of non-proprietary standard formats include X.509 or PKCS#7.

- iv. All copies of public key unalterable storage media made by the repository shall be labeled so that they are uniquely identifiable, including at a minimum: a unique identifier (such as a serial number) for the unalterable storage media; the time, date, location and name(s) of the repository owning the associated private keys; documentation about its creation; and an indication that the contents are public keys.
  - v. The NSRL or other designated repository shall document to whom they provide unalterable storage media containing their public keys used to verify digital signature reference information including at a minimum: the uniquely identified

public keys, the time and date provided, the name of the organization, and the name and contact information (phone, address, email address) of the recipient.

- vi. When a private key used to generate digital signature reference information becomes compromised, the NSRL or other designated repository shall provide notification to recipients of the associated public key that the private key has been compromised and the date on which it was compromised.
- c. The NSRL or other designated repository shall make both the reference information available on unalterable storage media and its associated documentation that is labeled by the repository that created it uniquely identifiable by including at a minimum: a unique identifier (such as a serial number) for the storage media; the time, date, location and name of the creating repository; and an indication that the contents are reference information.

#### **7.4.6 Software Setup Validation**

- a. Setup validation methods shall verify that no unauthorized software is present on the voting equipment.
- b. The vendor shall have a process to verify that the correct software is loaded, that there is no unauthorized software, and that voting system software on voting equipment has not been modified, using the reference information from the NSRL or from a State designated repository.
  - i. The process used to verify software should be possible to perform without using software installed on the voting system.
  - ii. The vendor shall document the process used to verify software on voting equipment.
  - iii. The process shall not modify the voting system software on the voting system during the verification process.
- c. The vendor shall provide a method to comprehensively list all software files that are installed on voting systems.
- d. The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system vendor.
  - i. If the process uses hashes or digital signatures, then the verification software shall use a FIPS 140-2 level 1 or higher validated cryptographic module.
  - ii. The verification process shall either (a) use reference information on unalterable storage media received from the repository or (b) verify the digital signature of the reference information on any other media.

- e. Voting system equipment shall provide a means to ensure that the system software can be verified through a trusted external interface, such as a read-only external interface, or by other means.
  - i. The external interface shall be protected using tamper evident techniques
  - ii. The external interface shall have a physical indicator showing when the interface is enabled and disabled
  - iii. The external interface shall be disabled during voting
  - iv. The external interface should provide a direct read-only access to the location of the voting system software without the use of installed software
- f. Setup validation methods shall verify that registers and variables of the voting system equipment contain the proper static and initial values.
  - i. The vendor should provide a method to query the voting system to determine the values of all static and dynamic registers and variables including the values that jurisdictions are required to modify to conduct a specific election.
  - ii. The vendor shall document the values of all static registers and variables, and the initial starting values of all dynamic registers and variables listed for voting system software, except for the values set to conduct a specific election.

## **7.5 Telecommunications and Data Transmission**

There are four areas that must be addressed by telecommunications and data transmission security capabilities: access control, data integrity, detection and prevention of data interception, and protection against external threats.

### **7.5.1 Maintaining Data Integrity**

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.

- a. 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.

- b. Voting systems that use telecommunications to communicate between system components and locations before the polling place is officially closed shall:
  - i. Implement an encryption standard currently documented and validated for use by an agency of the U.S. government
  - ii. Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System

## **7.5.2 Protection Against External Threats**

- a. Voting systems that use public telecommunications networks shall implement protections against external threats to which commercial products used in the system may be susceptible.
- b. 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 operating systems, communications routers, modem drivers and dial-up networking software.
  - i. Such documentation shall identify the name, vendor, and version used for each such component.
- c. Voting systems that use public telecommunications networks shall use protective software at the receiving-end of all communications paths to:
  - i. Detect the presence of a threat in a transmission
  - ii. Remove the threat from infected files/data
  - iii. Prevent against storage of the threat anywhere on the receiving device
  - iv. Provide the capability to confirm that no threats are stored in system memory and in connected storage media
  - v. Provide data to the system audit log indicating the detection of a threat and the processing performed
- d. Vendors shall use multiple forms of protective software as needed to provide capabilities for the full range of products used by the voting system.

## **7.5.3 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), and the Federal Computer Incident Response Capability (FedCIRC), for which additional information can be found at [www.us-cert.gov](http://www.us-cert.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 test labs 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 within the timeframe established by the state
- f. Address threats emerging too late to correct the system by:
  - i. Providing prompt, emergency notification to the accredited test labs and the affected states and user jurisdictions
  - ii. Assisting client jurisdictions directly or advising them through detailed written procedures to disable the public telecommunications mode of the system
  - iii. Modifying the system after the election to address the threat, submitting the modified system to an accredited test lab and the EAC or 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

## **7.5.4 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. Control system access by means of passwords, and restrict account access to necessary functions only
- d. Have capabilities in place to control the flow of information, precluding data leakage through shared system resources

## **7.5.5 Incomplete Election Returns**

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

- a. Be designed to provide external access to incomplete election returns (for equipment that operates in a central counting environment), 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. Design voting system software and its security environment such that data accessible to interactive queries resides in an external file or database created and maintained by the elections software under the restrictions applying to any other output report:
  - i. The output file or database has no provision for write access back to the system
  - ii. 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

## **7.6 Use of Public Communications Networks**

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

### **7.6.1 Data Transmission**

All systems that transmit data over public telecommunications networks shall:

- a. Preserve the secrecy of voter ballot selections and prevent anyone from violating ballot privacy

- b. Employ digital signatures for all communications between the vote server and other devices that communicate with the server over the network
- c. Require that at least two authorized election officials activate any critical operation regarding the processing of ballots transmitted over a public communications network, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of votes

## **7.6.2 Casting Individual Ballots**

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 polling places 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.

### **7.6.2.1 Documentation of Mandatory Security Activities**

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

- a. All activities mandatory to ensuring effective voting system security to be performed in setting up the system for operation, including testing of security before an election
- b. All activities that should be prohibited during voting equipment setup and during the timeframe for voting operations, including both the hours when polls are open and when polls are closed

### **7.6.2.2 Ability to Operate During Interruption of Service**

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

- a. Detect the occurrence of a telecommunications interruption at the polling place and switch to an alternative mode of operation that is not dependent on the connection between polling place voting devices and external system components
- b. Provide an alternate mode of operation that includes the functionality of a conventional electronic voting system 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 electronic voting system mode

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

## 7.7 Wireless Communications

This section provides requirements for implementing and using wireless communications within a voting system. These requirements reduce, but do not eliminate, the risk of using wireless communications for voting systems.

Wireless is defined as any means of communications that occurs without wires. This normally covers the entire electromagnetic spectrum. For the purposes of this section, wireless includes radio frequency, infrared, and microwave. This section provides requirements and considerations that apply to external wireless communications capabilities existing on voting equipment or as a component within a voting system. These requirements may be applied to internal wireless communications, but this is not required when the physical container that houses the voting equipment or voting system is considered adequate to protect the internal wireless between or among voting system components.

Since the wireless communications path on which the signals travel is via the air and not a wire or cable, devices other than those intended to receive the wireless signal (e.g. voting data) can receive (intentionally and unintentionally) the wireless signals. Some of the wireless communications paths (i.e. signals) are weakened by walls and distance, but are not stopped. This makes it possible to eavesdrop from a distance as well as transmit wireless signals (e.g., interference or intrusive data) from a distance. In many cases, the wireless signals cannot be seen, heard, or felt, thus making the presence of wireless communication hard to determine by the human senses. The requirements in this section mitigate the risks associated with wireless by controlling and identifying usage, and protecting the transmitted data and path.

There are other concerns when evaluating wireless usage; specifically radio frequency (RF). A device's radio frequencies usage and the power output are governed by Federal Communications Commission (FCC) regulations and therefore all RF wireless communications devices are subject to the applicable FCC requirements. However, these FCC regulations do not fully address RF wireless interference caused by multiple FCC compliant devices. That is, the RF wireless used in a voting system may be using the same radio frequency as another non-voting wireless system and which may potentially cause a degradation of the wireless performance or a complete wireless failure for the voting system.

Sometimes a particular wireless technology permits a power output range, which may be used to overcome interference received from another device. A radio emissions site test can

determine the extent of potential existing interference at the location where the wireless voting system is to be used. A radio emission site test can also determine the extent that the RF wireless transmission of the voting system escapes the building in which the RF wireless voting system is used.

### **7.7.1 Controlling Usage**

- a. If wireless communications are used in a voting system, then the vendor shall supply documentation describing how to use all aspects of wireless communications in a secure manner. This documentation shall include:
  - i. A complete description of the uses of wireless in the voting system including descriptions of the data elements and signals that are to be carried by the wireless mechanism
  - ii. A complete description of the vulnerabilities associated with this proposed use of wireless, including vulnerabilities deriving from the insertion, deletion, modification, capture or suppression of wireless messages
  - iii. A complete description of the techniques used to mitigate the risks associated with the described vulnerabilities including techniques used by the vendor to ensure that wireless cannot send or receive messages other than those situations specified in the documentation. Cryptographic techniques shall be carefully and fully described, including a description of cryptographic key generation, management, use, certification, and destruction
  - iv. A rationale for the inclusion of wireless in the proposed voting system, based on a careful and complete description of the perceived advantages and disadvantages of using wireless for the documented uses compared to using non-wireless approaches

Discussion: In general, convenience is not a sufficiently compelling reason, on its own, to justify the inclusion of wireless communications in a voting system. Convenience must be balanced against the difficulty of working with cryptographic keys.
- b. The details of all cryptographic protocols used for wireless communications, including the specific features and data, shall be documented.
- c. The wireless documentation shall be closely reviewed for accuracy, completeness, and correctness.

- d. There shall be no undocumented use of the wireless capability, nor any use of the wireless capability that is not entirely controlled by an election official.

Discussion: This can be tested by reviewing all of the software, hardware, and documentation, and by testing the status of wireless activity during all phases of testing.

- e. If a voting system includes wireless capabilities, then the voting system shall be able to accomplish the same function if wireless capabilities are not available due to an error or no service.
  - i. The vendor shall provide documentation how to accomplish these functions when wireless is not available.
- f. The system shall be designed and configured so it is not vulnerable to a single point of failure using wireless communications that causes a total loss of any voting capabilities.
- g. If a voting system includes wireless capabilities, then the system shall have the ability to turn on the wireless capability when it is to be used and to turn off the wireless capability when the wireless capability is not in use.
- h. If a voting system includes wireless capabilities, then the system shall not activate the wireless capabilities without confirmation from an elections official.

### **7.7.2 Identifying Usage**

Since there are a wide variety of wireless technologies (both standard and proprietary) and differing physical properties of wireless signals, it is important to identify some of the characteristics of the wireless technologies used in the voting system.

- a. If a voting system provides wireless communications capabilities, then there shall be a method for determining the existence of the wireless communications capabilities.
- b. If a voting system provides wireless communications capabilities, then there shall be an indication that allows one to determine when the wireless communications (such as radio frequencies) capability is active.
- c. The indication shall be visual.
- d. If a voting system provides wireless communications capabilities, then the type of wireless communications used (such as radio frequencies) shall be identified either via a label or via the voting system documentation.

### 7.7.3 Protecting Transmitted Data

The transmitted data, especially via wireless communications, needs to be protected to ensure confidentiality and integrity. Examples of election information that needs to be protected include: ballot definitions, voting device counts, precinct counts, opening of poll signal, and closing of poll signal. Examples of other information that needs to be protected include: protocol messages, address or device identification information, and passwords.

Since radio frequency wireless signals radiate in all directions and pass through most construction material, anyone may easily receive the wireless signals. In contrast, infrared signals are line of sight and do not pass through most construction material. However, infrared signals can still be received by other devices that are in the line of sight. Similarly, wireless signals can be transmitted by others to create unwanted signals. Thus, encryption is required to protect the privacy and confidentiality of the voting information.

- a. All information transmitted via wireless communications shall be encrypted and authenticated--with the exception of wireless T-coil coupling--to protect against eavesdropping and data manipulation including modification, insertion, and deletion.
  - i. The encryption shall be as defined in Federal Information Processing Standards (FIPS) 197, "Advanced Encryption Standard (AES)."
  - ii. The cryptographic modules used shall comply with FIPS 140-2, Security Requirements for Cryptographic Modules.
- b. The capability to transmit non-encrypted and non-authenticated information via wireless communications shall not exist.
- c. If audible wireless communication is used, and the receiver of the wireless transmission is the human ear, then the information shall not be encrypted.

Discussion: This specifically covers wireless T-Coil coupling for assistive devices used by people who are hard of hearing.

### 7.7.4 Protecting the Wireless Path

If wireless communications are used, then the following capabilities shall exist in order to mitigate the effects of a denial of service (DoS) attack:

- a. The voting system shall be able to function properly throughout a DoS attack, since the DoS attack may continue throughout the voting period.
- b. The voting system shall function properly as if the wireless capability were never available for use.
- c. Alternative procedures or capabilities shall exist to accomplish the same functions that the wireless communications capability would have done.
- d. If infrared is being used, the shielding shall be strong enough to prevent escape of the voting system signal, as well as strong enough to prevent infrared saturation jamming.

Discussion: Since infrared has the line-of-sight property, securing the wireless path can be accomplished by shielding the path between the communicating devices with an opaque enclosure. However, this is only practical for short distances. This shielding would also help prevent accidental eye damage from the infrared signal.

### **7.7.5 Protecting the Voting System**

Physical security measures to prevent access to a voting system are not possible when using a wireless communications interface because there is no discrete physical communications path that can be secured.

- a. The security requirements in Subsection 2.1.1 shall be applicable to systems with wireless communications.
- b. The accuracy requirements in Subsection 2.1.2 shall be applicable to systems with wireless communications.
- c. The use of wireless communications that may cause impact to the system accuracy through electromagnetic stresses is prohibited.
- d. The error recovery requirements in Subsection 2.1.3 shall be applicable to systems with wireless communications.
- e. All wireless communications actions shall be logged.
  - i. The log shall contain at least the following entries: times when the wireless is activated and deactivated, services accessed, identification of device to which data was transmitted to or received from, identification of authorized user, and successful and unsuccessful attempts to access wireless communications or service.

Discussion: Other information such as the number of frames or packets transmitted or received at various logical layers may be useful, but is dependent on the wireless technology used.

- f. Device authentication shall occur before any access to, or services from, the voting system are granted through wireless communications.

Discussion: Authentication is an important element to protect the security of wireless communications. Authentication verifies the identity and legitimacy of users, devices, and services.

- i. User authentication shall be at least level 2 as per NIST Special Publication 800-63 Version 1.0.1, Electronic Authentication Guideline.

## 7.8 Independent Verification Systems

### 7.8.1 Overview

Independent verification (IV) systems are electronic voting systems that produce multiple independent cast vote records of voter ballot selections, which can be audited to a high level of precision. For this to happen, the cast vote records must be handled according to the following protocol:

- At least two cast vote records of the voter's selections are produced and one of the records is then stored in a manner that it cannot be modified by the voting system. For example, the voting system creates a record of the voter's selections and then copies it to unalterable storage media.
- The voter must be able to verify that both cast vote records are correct and match before leaving the polling place, e.g., verify his or her selections on the voting machine summary screen and also verify the second record on the unalterable storage media.
- The verification processes for the two cast vote records must be independent of each other, and at least one of the records must be verified directly by the voter.
- The contents of the two cast vote records also can be checked later for consistency through the use of unique identifiers that allow the records to be linked.

The cast vote records would be formatted so that at least one set is usable in an efficient counting process by the electronic voting system and the other set is usable in an efficient process of auditing or verifying the agreement between the two sets.

Given these conditions, the multiple cast vote records are considered to be distinct and independently verifiable, that is, both records are not under the control of the same system processes. As a result of this independence, the audit records can be used to check the accuracy of the counted records. Because the records are separately stored, an attacker who can compromise one will also have to compromise the other.

The voter verifiable paper audit trail (VVPAT) methodology is one of several classes of IV systems. In this approach, the voter can directly compare the electronic summary screen of the voting machine with the printed paper audit record. (This is not to be confused with the

paper ballot that is produced by optical scan voting systems that the voter visually verifies before placing it in the ballot box or tabulator.) Requirements for DREs with a VVPAT feature are provided below to reflect the fact that a number of States currently require this feature.

There are a variety of other IV approaches for the voter to verify his or her selections with systems that produce an electronic record for verification. Appendix C describes the characteristics of these systems in more detail. They include:

- Split process systems, which use separate devices for the voters to record and verify their ballot selections
- Cryptographic systems, which provide voters with coded receipts that can be used to verify their ballot selections
- Witness systems, which use an independent module to create the second record

## 7.8.2 Basic Characteristics of IV Systems

This section describes a preliminary set of basic characteristics that apply to all types of IV systems. This information is provided for the purpose of introducing these concepts for consideration in voting system design. It is anticipated that future voting systems will be required to provide some type of independent verification feature to enable voters to have confidence that their ballot selections are correctly recorded and counted.

An independent verification system produces at least two independent cast vote records of ballot selections via interactions with the voter, such that one record can be compared against the other to check their equality of content.

Discussion: This is the fundamental characteristic of IV systems. The records can be checked against one another to determine whether or not the voter selections are correctly recorded.

The voter verifies the content of each cast vote record and either (a) verifies at least one of the records directly or (b) verifies both records indirectly if the records are each under the control of independent processes.

Discussion: Direct verification involves using human senses; for example, directly reading a paper record via one's eyesight. Indirect verification involves using an intermediary to perform the verification; for example, verifying an electronic ballot image on the voting machine.

The creation, storage and handling of the cast vote records are sufficiently separate that the failure or compromise of one record does not cause the failure or compromise of another.

Discussion: The records must be stored on different media and handled independently of each other so that no one process could compromise all records. If an attack can alter one record, it should still be very difficult to alter the other record.

Both cast vote records are highly resistant to damage or alteration and capable of long-term storage.

Discussion: The records should be difficult to alter or damage so that they could be used in case the counted records are damaged or lost.

The processes of verification for the cast vote records do not all depend on the same device, software module, or system for their integrity, and are sufficiently separate that each record provides evidence of the voter's selections independently of its corresponding record.

Discussion: For example, the verification of the summary screen (electronic record) of a DRE is sufficiently separate from the verification of a paper record printed by a VVPAT component or a copy of the electronic record stored on a separate system.

The multiple cast vote records are linked to their corresponding audit records by including a unique identifier within each record.

Discussion: The identifier serves the purpose of uniquely identifying and linking the records for cross-checking.

Each cast vote record includes information identifying the following:

- An identification of the polling place and precinct
- Whether the balloting is provisional, early, or on election day
- Ballot style
- A timestamp generated when the voting machine is enabled to begin a voting session that can be used to correctly group the cast vote records
- A unique identifier associated with the voting machine

Discussion: The identifier could be a serial number or other unique ID.

The cryptographic software used in IV systems is approved by the U.S. Government's Cryptographic Module Validation Program, as applicable.

Discussion: IV voting systems may use cryptographic software for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and for digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program (CMVP). There may be cryptographic voting schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP-approved software shall be used where feasible. The CMVP website is <http://csrc.nist.gov/cryptval>.

## 7.9 Voter Verifiable Paper Audit Trail Requirements

This section contains requirements for DREs with a Voter Verifiable Paper Audit Trail (VVPAT) component. VVPAT capability is not required for national certification. However, these requirements will be applied for certification testing of DRE systems that are intended for use in states that require DREs to provide this capability. The vendor's certification testing application to the EAC must indicate whether the system being presented for testing includes this capability, as provided under Subsection 1.6.2.5 extensions.

### 7.9.1 Display and Print a Paper Record

- a. The voting system shall print and display a paper record of the voter ballot selections prior to the voter making his or her selections final by casting the ballot.

Discussion: This is the basic requirement for VVPAT capability. It requires the paper record to be created as a distinct representation of the voter ballot selections. It requires the paper record to contain the same information as the electronic record and be suitable for use in verifications of the voting machine's electronic records.

- b. The paper record shall constitute a complete record of ballot selections that can be used to assess the accuracy of the voting machine's electronic record, to verify the election results, and, if required by state law, in full recounts.

Discussion: This requirement exists to make clear that it is possible to use the paper record for checks of the voting machine's accuracy in recording voter ballot selections, as well as usable for election audits (such as mandatory 1% recounts). The paper record shall also be suitable for use in full recounts of the election if required by state law.

- c. The paper record shall contain all voter selection information stored in the electronic (ballot image) record.

Discussion: The electronic ballot image record cannot hide any information related to ballot selections; all information relating to voter selections must be equally present in both records. The electronic record may contain other items that don't necessarily need to be on the paper record, such as digital signature information.

### 7.9.2 Approve or Void the Paper Record

- a. The voting equipment shall allow the voter to approve or void the paper record.

Discussion: There are three possible scenarios regarding the voter's disposition of the paper record.

- The voter can verify that the ballot selections displayed on the DRE summary screen and those printed on the paper record are the same. If they are, and the voter is satisfied with these selections, the voter can proceed to cast his or her ballot, thereby approving the paper record.
  - If the selections match, but the voter wishes to change one or more selections, the paper record must be voided so a new paper record can be created to compare to the new summary screen displayed after the voter changes his or her ballot selections.
  - In the event the selections do not match between the summary screen and the paper record, the voter shall immediately request assistance from a poll worker. A non-match could indicate a potential voting machine or printer malfunction.
- b. The voting equipment shall, in the presence of the voter, mark the paper record as being approved by the voter if the ballot selections are accepted; or voided or if the voter decides to change one or more selections.
- c. If the records do not match, the voting equipment shall mark and preserve the paper record and shall provide a means to preserve the corresponding electronic record so the source of error or malfunction can be analyzed.
- Discussion: The voting machine shall be withdrawn from service immediately and its use discontinued in accordance with jurisdiction procedures.
- d. The voting machine shall not record the electronic record until the paper record has been approved by the voter.
- e. Vendor documentation shall include procedures to enable the election official to return a voting machine to correct operation after a voter has used it incompletely or incorrectly. This procedure shall not cause discrepancies between the tallies of the electronic and paper records.

### **7.9.3 Electronic and Paper Record Structure**

- a. All cryptographic software in the voting system shall be approved by the U.S. Government's Cryptographic Module Validation Program, as applicable.

Discussion: Cryptographic software may be used for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program (CMVP). There may be cryptographic voting schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP approved software should be used where feasible but is not required. The CMVP website is <http://csrc.nist.gov/cryptval>.

- b. The electronic ballot image and paper records shall include information about the election.
- i. The voting equipment shall be able to include an identification of the particular election, the voting site and precinct, and the voting machine.

Discussion: If the voting site and precinct are different, both should be included.

- ii. The records shall include information identifying whether the balloting is provisional, early, or on election day, and information that identifies the ballot style in use.
- iii. The records shall include a voting session identifier that is generated when the voting equipment is placed in voting mode, and that can be used to identify the records as being created during that voting session.

Discussion: If there are several voting sessions on the same voting machine on the same day, the voting session identifiers must be different. They should be generated from a random number generator.

- c. The electronic ballot image and paper records shall be linked by including a unique identifier within each record that can be used to identify each record uniquely and each record's corresponding record.

Discussion: The identifier serves the purpose of uniquely identifying and linking the records for cross-checking.

- d. The voting machine should generate and store a digital signature for each electronic record.
- e. The electronic ballot image records shall be able to be exported for auditing or analysis on standards-based and /or COTS information technology computing platforms.
- i. The exported electronic ballot image records shall be in a publicly available, non-proprietary format.

Discussion: It is advantageous when all electronic records, regardless of manufacturer, use the same format or can easily be converted to a publicly available, non-proprietary format; for example, the OASIS Election Markup Language (EML) Standard.

- ii. The records should be exported with a digital signature, which shall be calculated on the entire set of electronic records and their associated digital signatures.

Discussion: This is necessary to determine if records are missing or substituted.

- iii. The voting system vendor shall provide documentation as to the structure of the exported ballot image records and how they shall be read and processed by software.
  - iv. The voting system vendor shall provide a software program that will display the exported ballot image records and that may include other capabilities such as providing vote tallies and indications of undervotes.
  - v. The voting system vendor shall provide full documentation of procedures for exporting electronic ballot image records and reconciling those records with the paper audit records.
- f. The paper record should be created in a format that may be made available across different manufacturers of electronic voting systems.

Discussion: There may be a future requirement for some commonality in the format of paper records.

- g. The paper record shall be created such that its contents are machine readable.

Discussion: This can be done by using specific OCR fonts or barcodes.

- i. The paper record shall contain error correcting codes for the purpose of detecting read errors and for preventing other markings on the paper record from being misinterpreted when machine reading the paper record.

Discussion: This requirement is not mandatory if a state prohibits the paper record from containing any information that cannot be read and understood by the voter. This requirement serves the purpose of detecting scanning errors and preventing stray or deliberate markings on the paper from being interpreted as valid data.

- h. If barcode is used, the voting equipment shall be able to print a barcode with each paper record that contains the human-readable contents of the paper record.

Discussion: This requirement is not mandatory if a state prohibits the paper record from containing any information that cannot be read and understood by the voter.

- i. The barcode shall use an industry standard format and shall be able to be read using readily available commercial technology.

Discussion: Examples of such codes are Maxi Code or PDF417.

- ii. If the corresponding electronic record contains a digital signature, the digital signature shall be included in the barcode on the paper record.

- iii. The barcode shall not contain any information other than the paper record's human-readable content, error correcting codes, and digital signature information.

## 7.9.4 Equipment Security and Reliability

- a. The voting machine shall provide a standard, publicly documented printer port (or the equivalent) using a standard communication protocol.

Discussion: Using a standard, publicly documented printer protocol assists in security evaluations of system software.

- b. Tamper-evident seals or physical security measures shall protect the connection between the printer and the voting machine.
- c. If the connection between the voting machine and the printer has been broken, the voting machine shall detect this event and record it in the DRE internal audit log.
- d. The paper path between the printing, viewing and storage of the paper record shall be protected and sealed from access except by authorized election officials.
- e. The printer shall not be permitted to communicate with any system or machine other than the voting machine to which it is connected.
- f. The printer shall only be able to function as a printer; it shall not contain any other services (e.g., provide copier or fax functions) or network capability.
- g. The voting machine shall detect errors and malfunctions such as paper jams or low supplies of consumables such as paper and ink that may prevent paper records from being correctly displayed, printed or stored.

Discussion: This could be accomplished in a variety of different ways; for example, a printer that is out of paper or jammed could issue a different audible alarm for each condition.

- h. If an error or malfunction occurs, the voting machine shall suspend voting operations and should present a clear indication to the voter and election officials of the malfunction.
- i. The voting machine shall not record votes if an error or malfunction occurs.
- j. Printing devices should contain sufficient supplies of paper and ink to avoid reloading or opening equipment covers or enclosures and thus potential circumvention of security features; or be able to reload paper and ink with minimal disruption to voting and without circumvention of security features such as seals.

- k. Vendor documentation shall include procedures for investigating and resolving printer malfunctions including, but not limited to; printer operations, misreporting of votes, unreadable paper records, and power failures.
- l. Vendor documentation shall include printer reliability specifications including Mean Time Between Failure estimates, and shall include recommendations for appropriate quantities of backup printers and supplies.
- m. Protective coverings intended to be transparent on voting equipment shall be maintainable via a predefined cleaning process. If the coverings become damaged such that they obscure the paper record, they shall be replaceable.
- n. The paper record shall be sturdy, clean, and of sufficient durability to be used for verifications, reconciliations, and recounts conducted manually or by automated processing.

## 7.9.5 Preserving Voter Privacy

VVPAT records can be printed and stored by two different methods:

- Printed and stored on a continuous spool-to-spool paper roll where the voter views the paper record in a window
- Printed on separate pieces of paper, which are deposited in a secure receptacle.

If a requirement applies to only one method, that will be specified. Otherwise, the requirement applies to both.

- a. Voter privacy shall be preserved during the process of recording, verifying and auditing his or her ballot selections.

Discussion: The privacy requirements from Section 3 also apply to voting equipment with VVPAT.

- b. When a VVPAT with a spool-to-spool continuous paper record is used, a means shall be provided to preserve the secrecy of the paper record of voter selections.
- c. When a VVPAT with a spool-to-spool continuous paper record is used, no record shall be maintained of which voters used which voting machine or the order in which they voted.
- d. The electronic and paper records shall be created and stored in ways that preserve the privacy of the voter.

Discussion: For VVPAT systems that use separate pieces of paper for the record, this can be accomplished in various ways including shuffling the order of the records or other methods to separate the order of stored records.

- e. The privacy of voters whose paper records contain an alternative language shall be maintained.
- f. Unique identifiers shall not be displayed in a way that is easily memorable by the voter.

Discussion: Unique identifiers on the paper record are displayed or formatted in such a way that they are not memorable to voters, such as by obscuring them in other characters.

- g. Both paper rolls and paper record secure receptacles shall be controlled, protected, and preserved with the same security as a ballot box.

### **7.9.6 VVPAT Usability**

- a. All usability requirements from Subsection 3.1 shall apply to voting machines with VVPAT.

Discussion: The requirements in this section are in addition to those in Subsection 3.1.

- b. The voting equipment shall be capable of showing the information on the paper in a font size of at least 3.0 mm and should be capable of showing the information in at least two font ranges; 3.0-4.0 mm, and 6.3-9.0 mm, under control of the voter or poll worker.

Discussion: In keeping with requirements in Subsection 3.1, the paper record should use the same font sizes as displayed by the voting machine, but at least be capable of 3.0 mm. While larger font sizes may assist voters with poor vision, certain disabilities such as tunnel vision are best addressed by smaller font sizes.

- c. The voting equipment shall display, print and store the paper record in any of the written alternative languages chosen for the ballot.
  - i. To assist with manual auditing, candidate names on the paper record shall be presented in the same language as used on the DRE summary screen.
  - ii. Information on the paper record not needed by the voter to perform verification shall be in English.

Discussion: In addition to the voter ballot selections, the marking of the paper record as accepted or void, and the indication of the ballot page number need to be printed in the alternative language. Other information, such as precinct and election identifiers, shall be in English to facilitate use of the paper record for auditing.

- d. The paper and electronic records shall be presented to allow the voter to read and compare the records without the voter having to shift his or her position.
- e. If the paper record cannot be displayed in its entirety on a single page, a means shall be provided to allow the voter to view the entire record.

Discussion: Possible solutions include scrolling the paper or printing a new sheet of paper. The voter should be notified if it is not possible to scroll in reverse, so they will know to complete verification in one pass.

- f. If the paper record cannot be displayed in its entirety on a single page, each page of the record shall be numbered and shall include the total count of pages for the record.

Discussion: Possible numbering schemes include “Page X of Y.”

- g. The instructions for performing the verification process shall be made available to the voter in a location on the voting machine.

Discussion: All instructions must meet the usability requirements contained in Subsection 3.1.

### **7.9.7 VVPAT Accessibility**

- a. All accessibility requirements from Subsection 3.2 shall apply to voting machines with VVPAT.
- b. If the normal voting procedure includes VVPAT, the accessible voting equipment should provide features that enable voters who are visually impaired and voters with an unwritten language to perform this verification. If state statute designates the paper record produced by the VVPAT to be the official ballot or the determinative record on a recount, the accessible voting equipment shall provide features that enable visually impaired voters and voters with an unwritten language to review the paper record.

Discussion: For example, the accessible voting equipment might provide an automated reader that converts the paper record contents into audio output.