6.0 Security

Section 6.0 addresses four new, specific aspects of voting systems security:

1. Independent Dual Verification Voting Systems: definition and characteristics of voting systems that produce multiple records of votes. A future version of the VVSG will require that voting systems produce multiple records of ballots or receipts for auditing purposes (Section 6.0.1, Informative).

2. Security Requirements for Voter Verified Paper Audit Trails: requirements for voter verified paper audit trails, if a State chooses to require them (Section 6.0.2, Normative).

3. Use of Wireless Networking in Voting Systems: requirements for wireless networks and the data sent across wireless networks (Section 6.0.3, Normative).

4. Security Requirements for Software Distribution and Setup Validation of Voting System: requirements for (a) the secure distribution of voting systems software and (b) for verifying that voting systems are operating with the correct software configuration (Section 6.0.4, Normative).

1. Security Overview (Informative)

This section is a discussion of independent verification systems followed by characteristics of independent verification systems which will be used as the basis for future requirements. The characteristics are preliminary and will be evolving with further research.

1. Independent Dual Verification Systems

A primary objective for using electronic voting systems is the production of voting records that are highly precise, highly reliable, and easily counted - in essence, an accurate representation of ballot choices whose handling requirements are reasonable. To meet this objective, there are many factors to consider in an electronic voting system's design, including:

- the environment provided for voting, including the voting site and various environmental factors,
- the ease with which voters can use the voting system, i.e., its usability,
- the robustness and reliability of the voting equipment, and
- the capability of the records to be used in audits.

Independent Dual Verification (IDV) systems have as their primary objective the production of ballot records that are capable of being used in audits in which their correctness can be audited to very high levels of precision. The primary security issues addressed by IDV systems are:

- whether electronic voting systems are accurately recording ballot choices, and
- whether the ballot record contents can be audited precisely post-election.

The threats addressed by IDV systems are those that could cause a voting system to inaccurately record the voter's intent or cause a voting system's records to become damaged, i.e., inserted, deleted, or changed. These threats could occur via any number of means including accidental damage or various forms of fraud. The threats are addressed mainly by providing, in the voting system design, the capability for ballot record audits to detect precisely whether specific records are correct as recorded or damaged, missing, or fraudulent.

1.1 Independent Dual Verification Systems: Improved Accuracy in Audits

Independent Verification is the top-level categorization for electronic voting systems that produce multiple records of ballot choices whose contents are capable of being audited to

high levels of precision. For this to happen, the records must be produced and made verifiable by the voter, and then subsequently handled according to the following protocol:

- At least two records of the voter's choices are produced and one of the records is then stored such that it cannot be modified by the voting system, e.g. the voting system creates a record of the voter's choices and then copies it to some write-once media.

- The voter must be able to verify that both records are correct, e.g., verify his or her choices on the voting system's display and also verify the second record of choices stored on the write-once media.

- The verification processes for the two verifications must be independent of each other and (a) at least one of the records must be verified directly by the voter, or (b) it is acceptable for the voter to indirectly verify both records if they are stored on different systems produced by different vendors.

- The content of the two records can be checked later for consistency through the use of identifiers that allow the records to be linked.

An assumption is made that at least one set of records is usable in an efficient counting process such as by using an electronic voting system, and the other set of records is usable in an efficient process of verifying its agreement with the other set of records used in the counting process. The sets of records would preferentially be different in form and thus have more resistance to accidental or deliberate damage.

Given these conditions above, the multiple records are said to be distinct and independently verifiable, that is, both records are not under the control of the same processes. As a result of this independence, one record can be used to audit or check up on the accuracy of the other record. Because the storage of the records is separate, an attacker who can compromise one of the records still will face a difficult task in compromising the other.

1.2 Issues in Handling Multiple Records Produced by Independent Dual Verification Systems

There are several fundamental questions that need to be addressed when designing the structure and selecting the physical characteristics of IDV systems records, including:

- how to tell if the records are authentic and not forged,

- how to tell if the integrity of the records has remained intact from the time they were recorded,

- the suitability of the records for various types of auditing, and

- how best to address problems if there are errors in the records.

Whenever an electronic voting system produces multiple records of votes, there is some possibility that one or more of the records may not match. Records can be lost, or deliberately or accidentally damaged, or stolen, or fabricated. Keeping the two records in correspondence with each other can be made more or less difficult depending on the technologies used for the records and the procedures used to handle the records.

As a consequence, it is important to structure the records so that errors and other anomalies can be readily detected during audits. There are a number of techniques that can be used, such as the following:

- associating unique identifiers with corresponding records, e.g., an individual paper record sharing a unique identifier with its corresponding electronic record,

- including an identification of the specific voting system that produced the records, such as a serial number identifier or by having the voting system digitally sign the records using public key cryptography,

- including other information about the election and the precinct or location where the records were created,

- creating checksums of the electronic records and having the voting system digitally sign the entire sets of records so that missing or inserted records can be detected, and

- structuring the records in open, publicly documented formats that can be readily analyzed on different computing platforms.

The ease or relative difficulty with which some types of records must be handled is also a determining factor in the practical capability to conduct precise audits, given that some types of records are better suited to different types of auditing and different voting environments than others. The factors that make certain types of records more suitable than others could vary greatly depending upon many other criteria, both objective and subjective. For example, paper records may require manual handling by voters or poll workers and thus be more susceptible to damage or loss. At the same time, the extent to which the paper records must be handled will vary depending on the type of voting system in use. Electronic records may by their nature be more suitable for automated audits; however electronic records are still subject to accidental or deliberate damage, loss, and theft.

2. Core characteristics for Independent Verification Systems

This section contains a preliminary set of characteristics for IDV systems. These characteristics are fundamental in nature and apply to all categories of IDV systems. They will form the basis for future requirements for independent verification systems.

2.1 An independent dual verification voting system produces two distinct sets of records of ballot choices via interactions with the voter such that one set of records can be compared against the other to check their equality of content.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: This is the fundamental core definition for IDV systems. The records can be checked against one another to determine whether or not the voter's choices were correctly recorded.

2.1.1 The voter verifies the content of each 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.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: Direct Verification involves using human senses, e.g., directly verifying a paper record via one's eyesight. Indirect Verification involves using an intermediary to perform the verification, e.g., verifying an electronic ballot image at the voting system.

2.1.2 The creation, storage, and handling of the records are sufficiently separate such that the failure or compromise of one record does not cause the failure or compromise of another.
Voting System Vendor
Pre-Voting Voting Post-Voting

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.

2.1.2.1 At least one record is highly resistant to damage or alteration and should be capable of long-term storage.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: At least one of the records should be difficult to alter or damage so that it could be used in case the counted records are damaged or lost.

2.1.3 The processes of verification for the multiple records do not all depend for their integrity on the same device, software module, or system, and are sufficiently separate such that each record provides evidence of the voter's choices independently of its other corresponding record.
Voting System Vendor

Pre-Voting Voting Post-Voting

Discussion: For example, the verification of an electronic record on a DRE is not sufficiently separate from the verification of an electronic record located on a token but performed by the same DRE as the verification for the first record. Verification of the paper record by one's senses is sufficiently separate in this case.

2.1.4 The records can be used in checks of one another, such that if one set of records can be used in an efficient counting process, the other set of records can be used for checking its agreement with the first set of records.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: For example, an electronic record can be used in an efficient counting process. A second paper record can be used to verify the accuracy of the electronic record; however its suitability for efficient counting is less clear. If a paper record can be used in an automated scan process, it may be more suitable.
2.1.5 The records within a set are linked to their corresponding records in the other set by including a unique identifier within each record that can be used to identify the record's corresponding record in the other set.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: The identifier should serve the purpose of uniquely identify the record so as to identify duplicates and/or for cross-checking two record types.

2.1.6 Each record includes an identification of the voting site/precinct.
Voting System Vendor
Pre-Voting Voting Post-Voting

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

2.1.7 The records include information identifying whether the balloting is provisional, early, or on Election Day, and information that identifies the ballot style in use.
Voting System Vendor
Pre-Voting Voting Post-Voting

2.1.8 The records include a voting session identifier that is generated when the voting station is placed in voting mode and that can be used to identify the records as being created during that voting session.
Voting System Vendor
Pre-Voting Voting Post-Voting

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

2.1.9 The records include an identifier of the voting system that is unique to that style of voting systems.
Voting System Vendor
Pre-Voting Voting Post-Voting

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

2.1.10 The cryptographic software in independent verification voting systems is approved by the U.S. Government's Cryptographic Module Validation Program (CMVP) as applicable.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: The 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. 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 web site is http://csrc.nist.gov/cryptval.

2. Requirements for Voter Verified Paper Audit Trails (Normative)
This section contains requirements for Voter Verified Paper Audit Trail (VVPAT) voting systems. VVPAT is not mandatory. These requirements apply only to voting systems that include a VVPAT component and are consistent with the definition of Independent Dual Verification (IDV) systems from Section 6.0.1. Requirements for usability, accessibility, and privacy from Volume I, Section 2.2.7 apply to VVPAT. The requirements in this section apply only to VVPAT systems; the requirements do not apply to other types of voting systems and are not intended to in any way restrict use or operation of other types of voting systems.

1. Display and Print a Paper Record
1.1 The voting station shall print and display a paper record of the voter’s ballot choices prior to the voter making the ballot choices final.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: This is the basic requirement for VVPAT capability. It requires that the paper record be created as a distinct representation of the voter's ballot choices. It requires that the paper record contain the same information as contained in the electronic

record and be suitable for use in verifications and recounts of the election and of the voting station's electronic records. Thus, either the paper or electronic record could be used as the ballot of record for the election.

1.1.1 The paper record shall constitute a complete record of ballot choices that can be used to assess the accuracy of the voting station's electronic record, to verify the election results, and in full recounts.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: This requirement exists to make clear that it is possible to use the paper record for checks of the voting station's accuracy in recording voter's ballot choices, as well as usable for election audits (such as mandatory 1% recounts). The paper record shall also be suitable for use in full manual recounts of the election.
1.1.2 The paper record shall contain all information stored in the electronic record.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: The electronic record cannot hide any information related to ballot choices; all information relating to ballot choices 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.

2. VVPAT Voting Station Usability
2.1 All usability requirements from Volume I, Section 2.2.7 shall apply to voting stations with VVPAT.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: The requirements in this section are in addition to those requirements from Section 2.2.7. They require that the paper record be formatted and displayed so that the voter is able to verify his or her votes with maximum reasonable ease and satisfaction, and that instructions be provided to the voter to handle all relevant aspects of the voter verification.

2.1.1 The voting station 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, (a) 3.0-4.0 mm and (b) 6.3-9.0 mm, under control of the voter or poll worker.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: In keeping with requirements in Section 2.2.7, the paper record should use the same font sizes as displayed by the voting station, but at least be capable of 3.0 mm.

While larger font sizes may assist most voters with poor vision, certain disabilities such as tunnel vision are best addressed by smaller font sizes.

2.1.2 The paper and electronic records shall be presented so as to allow for easy, simultaneous comparison.
Voting System Vendor
Pre-Voting Voting Post-Voting

2.1.2.1 The paper and electronic records shall be positioned so that the voter can, at the same posture, easily read and compare the two records.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: The voter should not have to shift positions when comparing the records.

2.1.2.2 If the paper record cannot be displayed in its entirety, a means shall be provided to allow the voter to view the entire ballot.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: Possible solutions include scrolling the paper or printing a new sheet of paper.

2.1.2.3 If the paper record cannot be displayed in its entirety on a single page, each page of the record shall be numbered and the last page shall be clearly distinguished.
Voting System Vendor
Pre-Voting Voting Post-Voting

2.1.3 The instructions for performing the verification process shall be made available to the voter in a location on the voting station.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: All instructions need to meet the accessibility requirements contained in Section 2.2.7.

3. VVPAT Voting Station Accessibility
3.1 All accessibility requirements from Section 2.2.7 shall apply to voting stations with VVPAT.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: Requirements in this section are in addition to the accessibility and alternative language requirements from Section 2.2.7. They make explicit that an accessible vote verification procedure for voters be provided at voting sites, including voters with disabilities, limited English proficiency (LEP), and voters with Native American and Alaska Native languages that are not written.

3.1.1 The voting station shall display, print, and store a paper record in any of the alternative languages chosen for making ballot selections.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: For the purposes of voter privacy, it must not be possible to identify voters based on their use of alternative languages. Requirement 6.0.2.5.1.3 addresses this issue.

3.1.1.1 For the purposes of verification, candidate names on the records shall be in English.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: This requirement is included to assist manual auditing of the paper records.
3.1.1.2 Other markings not related to ballot selection on the paper record shall be in English.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: Other markings may include designations of the precinct and the election.

3.1.2 If the normal procedure includes VVPAT, the accessible voting station should provide features that enable voters who are blind to perform this verification.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: This requirement is repeated from Section 2.2.7 and included here for emphasis. This requirement will be mandatory in future versions.

4. Approve or Spoil the Paper Record
4.1 The voting station shall allow the voter to approve or spoil the paper record.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: The voting station cannot create an electronic record without its corresponding paper record. It requires that the voting station mark the electronic record

as accepted or spoiled in the voter's presence, and if spoiled, the corresponding electronic record be marked as spoiled and be preserved. It requires that the voting station display a warning message when a spoil limit is reached.

4.1.1 The voting station shall, in the presence of the voter, mark the paper record as being accepted by the voter or spoiled.

Voting System Vendor

Pre-Voting Voting Post-Voting

Discussion: If a paper record is marked as spoiled, then the corresponding electronic record is presented to the voter for update.

4.1.2 The voting station should mark and preserve electronic and paper records that have been spoiled.

Voting System Vendor

Pre-Voting Voting Post-Voting

Discussion: For the purposes of reconciliation of records, electronic and paper spoiled records should be retained and analyzed.

4.1.3 Following the close of polls, a means shall be provided to reconcile the number of spoiled paper records with the number of occurrences of spoiled electronic records, and procedures shall be in place to address any discrepancies.

Voting System Vendor

Pre-Voting Voting Post-Voting

[Best practice for voting officials] Appropriate procedures are needed for reconciling the number of spoiled paper records with the number of spoiled electronic records and for addressing any discrepancies after the close of polls.

4.1.4 Prior to the maximum number of spoiled ballots occurring, the voting station shall display a warning message to the voter indicating that the voter may spoil only one more ballot.

Voting System Vendor

Pre-Voting Voting Post-Voting

Discussion: The maximum number of spoiled ballots varies from state to state.

4.1.5 If the maximum number of spoiled ballots occurs, the voting station should provide a way to permit the voter to cast a ballot, as required.

Voting System Vendor

Pre-Voting Voting Post-Voting

Discussion: Possible solutions include using other equipment, using a paper ballot, or accepting the last ballot cast. This capability defined by state and local jurisdiction.

[Best practice for voting officials] Appropriate procedures are needed to permit the voter to cast a ballot if the maximum number of spoiled ballots occurs.

[Best practice for voting officials] Appropriate procedures are needed to address situations in which a voter is unable to review the paper record.

[Best practice for voting officials] Appropriate procedures are needed to address situations in which a voter indicates that the electronic and paper records do not match. If the records do not match, a potentially serious error has likely occurred, and voting officials may need to take appropriate actions such as removing the voting station from service and quarantining its records for later analysis.

4.1.6 The voting station should not record the electronic record as being approved by the voter until the paper record has been stored.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: In general it is better not to record any record as being approved until the record that is independent of the voting system is approved by the voter.

4.1.7 Vendor documentation shall include procedures for returning a voting station 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.
Voting System Vendor
Pre-Voting Voting Post-Voting

5. Preserve Voter Privacy and Anonymity
5.1 The voter's privacy and anonymity shall be preserved during the process of recording, verifying, and auditing ballot choices.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: Privacy requirements from Section 2.2.7 apply to voting stations with VVPAT; requirements in this section are in addition to those requirements from Section 2.2.7. They require that the voter's privacy be maintained during the verification step, including requirements that the paper record contain no human or machine-readable

markings that could identify the voter and that the paper and electronic records be stored in ways that preserve the privacy and anonymity of the voter.

5.1.1 The privacy and anonymity of the voter's verification of his or her ballot choices on the electronic and paper records shall be maintained.
Voting System Vendor
Pre-Voting Voting Post-Voting

5.1.1.1 When the voter is responsible for depositing a paper record in the ballot box, the accessible voting station shall maintain the privacy and anonymity of voters unable to manually handle paper.
Voting System Vendor
Pre-Voting Voting Post-Voting

5.1.2 The electronic and paper records shall be created and stored in ways that preserve the privacy and anonymity of the voter.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: This can be accomplished in various ways including shuffling the order of the records or other methods to separate the order of stored records.
5.1.3 The privacy and anonymity of voters whose paper records contain any of the alternative languages chosen for making ballot selections shall be maintained.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: One method for accomplishing this is to ensure that no less than, e.g., five voters use any of the alternative languages for their ballot selections.

[Best practice for voting officials] Appropriate procedures are needed to ensure the privacy and anonymity of voters whose paper records contain any of the alternative languages chosen for making ballot selections.

5.1.4 The voter shall not be able to leave the voting area with the paper record if the information on the paper record can directly reveal the voter’s choices.
Voting System Vendor
Pre-Voting Voting Post-Voting

[Best practice for voting officials] Appropriate procedures are needed to prevent voters from leaving the voting area with a paper record that can directly reveal the voter's choices.

5.1.5 Unique identifiers shall not be displayed in a way that is easily memorable by the voter.
Voting System Vendor
Pre-Voting Voting Post-Voting

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.

6. Electronic and Paper Record Structure
6.1 The voting station's ballot records shall be structured and contain information so as to support highly precise audits of their accuracy.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: It requires that electronic records and paper records contain election precinct information, information to link the paper record to its corresponding electronic record, and information identifying the voting station. It requires that the electronic records be maintained in a format that can be exported to a different computer, e.g., a personal computer, and that the format be well-documented to support analysis of the records.

6.1.1 All cryptographic software in the voting station should be approved by the U.S. Government's Cryptographic Module Validation Program (CMVP) as applicable.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: The voting station 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. 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 web site is http://csrc.nist.gov/cryptval.

6.1.2 The electronic and paper records shall include information about the election.
Voting System Vendor
Pre-Voting Voting Post-Voting

6.1.2.1 The voting station shall be able to include an identification of the particular election, the voting site/precinct, and the voting station.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: If the voting site and precinct are different, both should be included. Some of this information may have to be excluded in certain cases to protect voter privacy.

6.1.2.2 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.

Voting System Vendor

Pre-Voting Voting Post-Voting

6.1.2.3 The records shall include a voting session identifier that is generated when the voting station is placed in voting mode and that can be used to identify the records as being created during that voting session.

Voting System Vendor

Pre-Voting Voting Post-Voting

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

6.1.3 The electronic 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.

Voting System Vendor

Pre-Voting Voting Post-Voting

Discussion: The identifier serves the purpose of uniquely identifying the record so as to identify duplicates and/or for crosschecking two record types.

6.1.4 The voting station should generate and store a digital signature for each electronic record.

Voting System Vendor

Pre-Voting Voting Post-Voting

6.1.5 The electronic records shall be able to be exported for auditing or analysis on standards based and/or COTS information technology computing platforms.

Voting System Vendor

Pre-Voting Voting Post-Voting

6.1.5.1 The exported electronic records shall be in a publicly available, non-proprietary format.

Voting System Vendor

Pre-Voting Voting Post-Voting

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

6.1.5.2 The voting station should export the records accompanied by a digital signature of the collection of records, which shall be calculated on the entire set of electronic records and their associated digital signatures.
Voting System Vendor
Pre-Voting Voting Post-Voting

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

6.1.5.3 The voting system vendor shall provide documentation as to the structure of the exported records and how they shall be read and processed by software.
Voting System Vendor
Pre-Voting Voting Post-Voting

6.1.5.4 The voting system vendor shall provide a software program that will display the exported records and that may include other capabilities such as providing vote tallies and indications of undervotes.
Voting System Vendor
Pre-Voting Voting Post-Voting

6.1.6 The paper record should be created in a format that may be made available across different manufacturers of electronic voting systems.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: Future standards may require some commonality in the format of paper records.

6.1.7 The paper record shall be created such that its contents are machine-readable.
Voting System Vendor
Pre-Voting Voting Post-Voting

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

6.1.7.1 The paper record should contain error correcting codes for the purposes of detecting read errors and for preventing other markings on the paper record to be misinterpreted when machine reading the paper record.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: This requirement is not mandatory if, for example, a state prohibits non-human-readable information on the paper record. This requirement serves the purpose of

detecting scanning errors and preventing stray or deliberate markings on the paper from being interpreted as valid data.

6.1.8 Any automatic accumulation of electronic or paper records shall be capable of detecting and discarding duplicate copies of the records.
Voting System Vendor
Pre-Voting Voting Post-Voting

6.1.9 The voting station should be able to print a barcode with each paper record that contain the human readable contents of the paper record and digital signature information.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: This requirement is not mandatory if, for example, a state prohibits non-human-readable information on the paper record.

6.1.9.1 The barcode shall use an industry-standard format and shall be able to be read using readily available commercial technology.
Voting System Vendor
Pre-Voting Voting Post-Voting

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

6.1.9.2 If the paper record's corresponding electronic record contains a digital signature, the digital signature shall be included in the barcode.
Voting System Vendor
Pre-Voting Voting Post-Voting

6.1.9.3 The barcode shall not contain any information other than the paper record's human readable content and digital signature information.
Voting System Vendor
Pre-Voting Voting Post-Voting

6.1.10 The voting system vendor shall provide full documentation of procedures for exporting its electronic records and reconciling its electronic records with its paper records.
Voting System Vendor
Pre-Voting Voting Post-Voting

7. Equipment Security and Reliability

7.1 The voting station equipment shall be secure, reliable, and easily maintained.

Voting System Vendor

Pre-Voting Voting Post-Voting

7.1.1 The voting station shall be physically secure from tampering, including intentional damage.

Voting System Vendor

Pre-Voting Voting Post-Voting

[Best practice for voting officials] Appropriate procedures are needed to ensure that voting systems are physically secured from tampering and intentional damage.

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

Voting System Vendor

Pre-Voting Voting Post-Voting

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

7.1.1.2 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.

Voting System Vendor

Pre-Voting Voting Post-Voting

7.1.1.3 The printer shall not be permitted to communicate with any other system or machine other than the single voting machine to which it is connected.

Voting System Vendor

Pre-Voting Voting Post-Voting

7.1.1.4 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.

Voting System Vendor

Pre-Voting Voting Post-Voting

7.1.1.5 Printer access to replace consumables such as ink or paper shall only be possible if it does not compromise the sealed printer paper path.

Voting System Vendor

Pre-Voting Voting Post-Voting

7.1.1.6 The ballot box storing the paper records shall be sealed and secured and no access shall be provided to poll workers.
Voting System Vendor
Pre-Voting Voting Post-Voting

7.1.1.7 Tamper-evident seals or physical security measures shall protect the connection between the printer and the voting station, so that the connection cannot be broken or interfered with without leaving extensive and obvious evidence.
Voting System Vendor
Pre-Voting Voting Post-Voting

7.1.2 The voting station's printer shall be highly reliable and easily maintained.
Voting System Vendor
Pre-Voting Voting Post-Voting

7.1.2.1 The voting station should 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.
Voting System Vendor
Pre-Voting Voting Post-Voting

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

7.1.2.2 If errors or malfunctions occur, the voting station shall suspend voting operations and should present a clear indication to the voter and election officials of the malfunctions.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: The voting station does not record votes if errors or malfunctions occur.

7.1.2.3 Printing devices should either (a) contain paper and ink of sufficient capacity so as not to require reloading or opening equipment covers or enclosures and circumvention of security features, or (b) be able to reload paper and ink with minimal disruption to voting and without circumvention of security features such as seals.
Voting System Vendor
Pre-Voting Voting Post-Voting

7.1.2.4 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.
Voting System Vendor
Pre-Voting Voting Post-Voting

7.1.2.5 Vendor documentation shall include printer reliability information including mean time between failure information and shall include recommendations for appropriate numbers of backup printer and printer supplies.
Voting System Vendor
Pre-Voting Voting Post-Voting

7.1.3 Protective coverings intended to be transparent on voting station devices shall be maintainable via a predefined cleaning process. If the coverings become damaged such that they obscure the paper record, they shall be replaceable.
Voting System Vendor
Pre-Voting Voting Post-Voting

7.1.4 The paper record shall be sturdy, clean, and of sufficient durability to be used for verifications, reconciliations, and recounts conducted manually and via machine reading equipment.
Voting System Vendor
Pre-Voting Voting Post-Voting

3. Wireless Requirements (Normative)

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

Wireless is defined as any means of communication that occurs without wires. This normally covers the entire electromagnetic spectrum. For the purposes of this section wireless includes radio frequency (RF), infrared, (IR), and microwave.

Since the wireless communications path on which the signals travel is via the air and not via 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 use of wireless technology

introduces severe risk and should be approached with extreme caution. The requirements in this section (i.e., controlling and identifying usage, protecting the transmitted data and path, and protecting the system) mitigate these risks.

The requirements that are applicable to all types of wireless communications are presented, followed by requirements that are applicable to a specific part of the electromagnetic spectrum (e.g., audible, radio frequency, and infrared). These latter requirements only apply to systems using those parts of the spectrum.

There are other concerns when evaluating wireless usage, specifically radio frequency. 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 RF wireless of 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.

1. Relationship to Volume I, Section 5: "Telecommunications."

1.1 At a minimum wireless communications shall meet the requirements listed in Volume I, Section 5, "Telecommunications."

Voting System Vendor

Pre-Voting Voting Post-Voting

2. Controlling Usage

2.1 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.

Voting System Vendor

Pre-Voting Voting Post-Voting

2.1.1 This documentation shall include:

- 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,
- 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,

- 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, and
- 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.

Voting System Vendor
Pre-Voting Voting Post-Voting
Discussion: In general, convenience is not a sufficiently compelling reason, on its own, to justify the inclusion of wireless communications in a voting system. If convenience is cited as an advantage of wireless, it shall be balanced against the difficulty of working with cryptographic keys.

[Best Practice for Voting Officials] When using encryption to ensure that the wireless communication is secure, appropriate procedures are needed for cryptographic key management.

2.1.2 The details of all cryptographic protocols used for wireless communications, including the specific features and data, shall be documented.
Voting System Vendor
Pre-Voting Voting Post-Voting

2.1.3 The wireless documentation shall be closely reviewed for accuracy, completeness, and correctness.
Testing Authority
Pre-Voting Voting Post-Voting

2.1.3.1 This review shall be done either through an open and public review or by a subject area recognized expert.
Testing Authority
Pre-Voting Voting Post-Voting

2.1.4 There shall be no undocumented use of the wireless capability, nor shall there be any use of the wireless capability that is not entirely controlled by the voting official.
Testing Authority

Pre-Voting Voting Post-Voting

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.

2.2 If a voting system includes wireless capabilities, then the voting system should be able to accomplish the same function if wireless capabilities are not available due to an error or no service.
Voting System Vendor
Pre-Voting Voting Post-Voting

2.2.1 The vendor shall provide documentation how to accomplish these functions when wireless is not available.
Voting System Vendor
Pre-Voting Voting Post-Voting

2.3 The system shall be designed and configured such that it is not vulnerable to a single point of failure using wireless communications that causes a total loss of any of voting capabilities.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: Rewritten from Volume 1, Section 5.2.6 Integrity item c)

2.4 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.
Voting System Vendor
Pre-Voting Voting Post-Voting

2.5 If a voting system includes wireless capabilities, then the system shall not activate the wireless capabilities without confirmation from a voting official.
Voting System Vendor
Pre-Voting Voting Post-Voting

3. 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.

3.1 If a voting system provides wireless communications capabilities, then there shall be a method for determining the existence of the wireless communications capabilities.
Voting System Vendor
Pre-Voting Voting Post-Voting

3.2 If a voting system provides wireless communications capabilities, then there shall be an indication that allows one to determine when the wireless communications (e.g., radio frequencies) capability is active.
Voting System Vendor
Pre-Voting Voting Post-Voting

3.2.1 The indication should be visual.
Voting System Vendor
Pre-Voting Voting Post-Voting

3.3 If a voting system provides wireless communications capabilities, then the type of wireless communications used (e.g., radio frequencies) shall be identified either via a label or via the voting systems documentation.
Voting System Vendor
Pre-Voting Voting Post-Voting

4. Protecting the 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, ballot instructions (audio), voting device counts, precinct counts, opening of poll signal, and closing of poll signal.

Examples of non--specific election 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 materials. However to a lesser extent, infrared signals can still be received by other devices that are in the line of sight. Similarly, wireless signals can also be easily transmitted by others in order to create unwanted signals. Thus to protect the privacy and confidentiality of the

information, encryption is required. The following requirements are rewritten from Volume I, Section 6.5.3.

4.1 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.
Voting System Vendor
Pre-Voting Voting Post-Voting

4.1.1 The encryption shall be as defined in Federal Information Processing Standards (FIPS) 197, "Advanced Encryption Standard (AES)."
Voting System Vendor
Pre-Voting Voting Post-Voting

4.1.1.1 The cryptographic modules used shall comply with FIPS 140-2, Security Requirements for Cryptographic Modules.
Voting System Vendor Testing Authority
Pre-Voting Voting Post-Voting

4.1.2 The capability to transmit non-encrypted and non-authenticated information via wireless communications shall not exist.
Voting System Vendor
Pre-Voting Voting Post-Voting

4.1.2.1 If wireless communication (audible) is used, and if the receiver of the wireless transmission is the human ear, then the information shall not be encrypted (i.e., this specifically covers the case of the wireless T-Coil coupling for assistive devices used by people who are hard of hearing - see Volume I, Section 2.2.7.2 DRE standards item c)
Voting System Vendor
Pre-Voting Voting Post-Voting

5. Protecting the Wireless Path
With the exception of wireless communications using audible and infrared, it is technically infeasible to use physical means to prevent denial of service (DoS) attacks. If wireless communications are used, then the following capabilities shall exist in order to mitigate the effects of a denial of service (DoS) attack:

5.1 The voting system shall be able to function properly throughout a DoS attack, since the DoS attack may continue throughout the voting process.
Voting System Vendor
Pre-Voting Voting Post-Voting

5.2 The voting system shall function properly as if the wireless capability were never available for use.
Voting System Vendor
Pre-Voting Voting Post-Voting

5.3 Alternative procedures or capabilities shall exist to accomplish the same functions that the wireless communications capability would have done.
Voting System Vendor
Pre-Voting Voting Post-Voting

5.4 The wireless (audible) path shall be protected or shielded.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: Protecting the audible path is a tradeoff between the high volume level necessary for an individual to hear with the low volume level necessary to keep others from hearing, as well as protecting from interference (i.e., noise) from the polling place, voting station, or voting environment. The same is true for the audible path if a voter's speech is to be captured by the voting device. This wireless communication's path protection is necessary to protect privacy. Some audio headsets may already satisfy this requirement for the hearing part, while a soundproof voting booth may be necessary in some other cases (e.g., voice recordings).

5.5 Infrared
Since infrared has the line-of-sight (LoS) property, securing the wireless path can be accomplished by shielding the path between the wireless communicating devices with an opaque enclosure. However this is only practical for short distances. Additionally, this type of shielding can help to prevent accidental damage to the eyes by the infrared signal.

5.5.1 The shielding shall be strong enough to prevent escape of the voting system's signal, as well as strong enough to prevent infrared saturation jamming.
Voting System Vendor
Pre-Voting Voting Post-Voting

6. Protecting the Voting System from a Wireless-based Attack

The security of the wireless voting systems is as important as the information transmitted. If a voting system becomes compromised, there is no way to determine the harm to the system until the compromise is discovered and an investigation is conducted to determine the extent of the damage.

Physical security measures (Volume I, Section 6.3) to prohibit access to a voting system are not possible when using a wireless communications interface. This is similar to when access is through a telecommunications interface, but it is worsened by the fact that there is no wire (physical communication path) to physically secure and by the various physical properties of the electromagnetic spectrum used.

This section covers and reaffirms the applicable overall system capabilities defined in Volume I, Section 2 as well as authentication requirements.

6.1 The security requirements listed in Volume I, Section 2.2.1 shall be applicable to systems with wireless communications.
Voting System Vendor
Pre-Voting Voting Post-Voting

6.2 The accuracy requirements listed in Volume I, Section 2.2.2 shall be applicable to systems with wireless communications.
Voting System Vendor
Pre-Voting Voting Post-Voting
6.2.1 The use of wireless communications that may cause impact to the system's accuracy through electromagnetic stresses is prohibited.
Voting System Vendor
Pre-Voting Voting Post-Voting

6.3 The error recovery requirements listed in Volume I, Section 2.2.3, shall be applicable to systems with wireless communications.
Voting System Vendor
Pre-Voting Voting Post-Voting

6.4 All wireless communications actions shall be logged.
Voting System Vendor
Pre-Voting Voting Post-Voting

Discussion: A log of important information is maintained to monitor the wireless communications. This is to ensure that the wireless communications are only used by authorized users with authorized access to authorized devices or services, or to determine if these requirements were not followed. This relates to the system audit requirements

(Volume I, Section 2.2.5) and integrity (Volume I, Section 2.2.4), if wireless communications are used.

6.4.1 The log shall contain at least the following entries: times wireless 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.

Voting System Vendor

Pre-Voting Voting Post-Voting

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.

[Best Practice for Voting Officials] Appropriate procedures are needed to ensure that wireless communication actions are logged and capture at least the following information: times wireless 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.

6.5 Authentication

Authentication is an important part in the protection and security of the wireless communications. It provides a mechanism to verify the identity and legitimacy of a person, device, services, or system. Authenticating users, devices and services helps to secure the wireless communications and prevent unauthorized access to the system, services and/or information.

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

Voting System Vendor

Pre-Voting Voting Post-Voting

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

Voting System Vendor

Pre-Voting Voting Post-Voting

4. Distribution of Voting System Software and Setup Validation (Normative)

This section specifies 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 qualification 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 qualified 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 other systems including polling place systems, central counting/aggregation systems, and election management systems. These other systems may reside on different computer based 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, etc.

1. Software Distribution Methodology Requirements

1.1 The vendor shall document all software including voting system software, third party software (such as operating systems, drivers, etc.) to be installed on voting equipment of the qualified voting system, and installation programs.

Voting System Vendor

Pre-Voting Voting Post-Voting

1.1.1 The documentation shall have a unique identifier (such as a serial number) for the following set of information: documentation, software vendor name, product name, version, qualification number of the voting system, file names and paths or other location information (such as storage addresses) of the software.

Voting System Vendor

Pre-Voting Voting Post-Voting

1.1.2 The documentation shall designate all software files as static, semi-static, or dynamic.

Voting System Vendor

Pre-Voting Voting Post-Voting

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 a priori making it impossible to create reference information to verify the software.

1.2 The EAC accredited testing authority shall witness the final build of the executable version of the qualified voting system software performed by the vendor.
Testing Authority
Pre-Voting Voting Post-Voting

1.2.1 The testing authority shall create a complete record of the build that includes: a unique identifier (such as a serial number) for the complete record, list of unique identifiers of write-once media associated with the record, time, date, location, name and signatures of all people present, source code and resulting executable file names, version of voting system software, qualification 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.
Testing Authority
Pre-Voting Voting Post-Voting
1.2.2 The record of the source code and executable files shall be made on write-once media. Each piece of write-once media shall have a unique identifier.
Testing Authority
Pre-Voting Voting Post-Voting

Discussion: Write-once media includes technology such as a CD-R, ROM, or PROM (but not EEPROM or CD-RW). The unique identifiers appear on indelibly printed labels and in a digitally signed file on the write-once media.

1.2.3 The testing authority shall retain this record until the voting system ceases to be qualified.
Testing Authority
Pre-Voting Voting Post-Voting

1.2.4 The EAC accredited testing authority 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, list of unique identifiers of write-once media associated with the subset, vendor, product name, version of voting system software, qualification number of the voting system, all the files that resulted from the build and binary images of all installation programs.
Testing Authority
Pre-Voting Voting Post-Voting

1.2.5 The record of the software shall be made on write-once media. Each piece of write-once media shall have a unique identifier.
Testing Authority
Pre-Voting Voting Post-Voting

1.2.6 The testing authority shall retain a copy, send a copy to the vendor, and send a copy to the NIST National Software Reference Library (NSRL) and/or to any other repository named by the Election Assistance Commission.
Testing Authority
Pre-Voting Voting Post-Voting

Discussion: The NSRL was established to meet the needs of the law enforcement community for court admissible digital evidence by providing an authoritative source of commercial software reference information. Information is available at www.nsrl.nist.gov.

1.2.7 The testing authority shall retain this record until the voting system ceases to be qualified.
Testing Authority
Pre-Voting Voting Post-Voting

1.3 The vendor shall provide the NSRL or other EAC designated repository with a copy of all third party software.
Voting System Vendor
Pre-Voting Voting Post-Voting

1.4 All voting system software, installation programs, third party software (such as operating systems, drivers, etc.) used to install or to be installed on voting system equipment shall be distributed on a write-once media.
Voting System Vendor
Pre-Voting Voting Post-Voting

[Best Practice for Voting Officials] Voting software used to install the qualified voting systems can be obtained on write-once media from the voting system vendor or an EAC accredited testing authority.

1.4.1 The vendor shall document that the process used to verify the software distributed on write-once media is the qualified software by using the reference information provided by the NSRL or other EAC designated repository.
Voting System Vendor
Pre-Voting Voting Post-Voting

[Best Practice for Voting Officials] The reference information produced by the NSRL or other EAC designated repository can be used to verify that the correct software has been received.

1.4.2 The voting system equipment shall be designed to allow the voting system administrator to verify that the software is the qualified software by comparing it to reference information produced by the NSRL or other EAC designated repository before installing the software.
Voting System Vendor
Pre-Voting Voting Post-Voting

1.4.3 The vendors and testing authority shall document to whom they provide voting system software write-once media.
Voting System Vendor Testing Authority
Pre-Voting Voting Post-Voting

2. Generation and Distribution Requirements for Reference Information
2.1 The NSRL or other EAC designed repository shall generate reference information using the binary images of the (a) qualified voting system software received on write-once media from testing authorities and (b) election specific software received on write-once media from jurisdictions.
Repository
Pre-Voting Voting Post-Voting

2.1.1 The NSRL or other EAC 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.
Repository
Pre-Voting Voting Post-Voting

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.

2.1.1.1 The NSRL or other EAC 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, file names of software and associated unique identifier(s) of the write-once media from which reference information is generated, time, date, name of people who generated reference information, the type of reference information created,

qualification number of voting system (if issued), voting system software version, product name, and vendor.
Repository
Pre-Voting Voting Post-Voting

2.1.1.2 The NSRL or other EAC designated repository shall retain the write-once media used to generate the reference information until the voting system ceases to be qualified.
Repository
Pre-Voting Voting Post-Voting

2.1.1.3 The NSRL or other EAC designated repository that generates hash value and/or digital signature reference information shall use FIPS approved algorithms for hashing and signing.
Repository
Pre-Voting Voting Post-Voting

2.1.1.4 The NSRL or other EAC 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.
Repository
Pre-Voting Voting Post-Voting

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

2.1.1.5 The NSRL or other EAC 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.
Repository
Pre-Voting Voting Post-Voting

2.1.1.6 If the NSRL or other EAC designated repository uses public key technology, the following requirements shall be met:
- public and private key pairs used by the repository to generate digital signatures shall be 2048-bits or greater in length, and
- the repository's private keys used to generate digital signature reference information shall be used for no more than three years.

Repository
Pre-Voting Voting Post-Voting

2.1.1.7 Public keys used to verify digital signature reference information shall be placed on a write-once media if not contained in a signed non-proprietary format for distribution.
Repository
Pre-Voting Voting Post-Voting

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

2.1.1.8 All copies of public key write-once 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 write-once media, time, date, location, name(s) of the repository owning the associated private keys, documentation about its creation, and an indication that the contents are public keys.
Repository
Pre-Voting Voting Post-Voting

2.1.1.9 The NSRL or other EAC designated repository shall document to whom they provide write-once media containing their public keys used to verify digital signature reference information including at a minimum: the uniquely identified public keys, time and date provided, name and contact information (phone, address, email address, etc.) of the recipient.
Repository
Pre-Voting Voting Post-Voting

2.1.1.10 When a private key used to generate digital signature reference information becomes compromised, the NSRL or EAC designated repository shall provide notification to recipients of the associated public key that the private key has been compromised and the date of compromise.
Repository
Pre-Voting Voting Post-Voting

2.2 The NSRL or other EAC designated repository shall make both the reference information available on write-once 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 write-once media, time, date, location, name of the creating repository, and an indication that the contents are reference information.
Repository
Pre-Voting Voting Post-Voting

[Best Practice for Voting Officials] To ensure that the write-once media contains the correct information, a digital signature can be used. The digital signature can replace secure storage of reference information since the digital signature can be used to verify that the reference information media has not been modified or corrupted.

3. Setup Validation Methodology Requirements

3.1 Setup validation methods shall verify that no unauthorized software is present on the voting equipment.

Voting System Vendor

Pre-Voting Voting Post-Voting

3.1.1 The vendor shall have a process to verify that the correct software is loaded, that there is no unauthorized software, and that static and semi-static voting system software on voting equipment has not been modified using the reference information from the NSRL or other EAC designated repository.

Voting System Vendor

Pre-Voting Voting Post-Voting

3.1.1.1 The process used to verify software should be possible to perform without using software installed on the voting system.

Voting System Vendor

Pre-Voting Voting Post-Voting

3.1.1.2 The vendor shall document the process used to verify software on voting equipment.

Voting System Vendor

Pre-Voting Voting Post-Voting

3.1.1.3 The process shall not modify the voting system software on the voting system during the verification process.

Voting System Vendor

Pre-Voting Voting Post-Voting

3.1.2 The vendor shall provide a method to comprehensively list all software files that are installed on voting systems.

Voting System Vendor

Pre-Voting Voting Post-Voting

3.1.2.1 The verification process shall be able to be performed using COTS software and hardware available from sources other than the voting system vendor.
Voting System Vendor
Pre-Voting Voting Post-Voting

3.1.2.2 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.
Voting System Vendor
Pre-Voting Voting Post-Voting

3.1.2.3 The verification process shall either (a) use reference information on "write-once" media received from the repository or (b) verify the digital signature of the reference information on any other media.
Voting System Vendor
Pre-Voting Voting Post-Voting

3.1.2.4 Voting system equipment shall provide a read-only external interface to access the software on the system.
- The external interface shall be protected using tamper evident techniques.
- The external interface shall have a physical indicator showing when the interface is enabled and disabled.
- The external interface shall be disabled during voting.
- The external interface should provide a direct read-only access to the location of the voting system software without the use of installed software.

Voting System Vendor
Pre-Voting Voting Post-Voting

3.2 Setup validation methods shall verify that registers and variables of the voting system equipment contain the proper static and initial values.
Voting System Vendor
Pre-Voting Voting Post-Voting

3.2.1 The vendor should provide a method to query the voting systems 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.
Voting System Vendor
Pre-Voting Voting Post-Voting

3.2.2 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.
Voting System Vendor
Pre-Voting Voting Post-Voting

[Best Practice for Voting Officials] The vendor's documented values can be used to verify that all voting systems' static and initial register and variable values are correct prior to an election.

[Best Practice for Voting Officials] The reference information can be used to verify that voting system software is the correct version of the software prior to an election.

[Best Practice for Voting Officials] If differences between the reference information and voting system software are found, then appropriate procedures are needed to handle and resolve these anomalies.

Page 1: [2] Deleted **Author**

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.

Page 1: [3] Deleted **Author**

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.

Page 1: [4] Deleted **Author**

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.

Page 1: [5] Deleted **Author**

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.

Page 1: [6] Deleted **Author**

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.

Page 1: [7] Deleted **Author**

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.

Page 1: [8] Deleted **Author**

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

Page 1: [9] Deleted **Author**

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.

Page 1: [10] Deleted **Author**

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.

Page 1: [11] Deleted **Author**

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.

Page 1: [12] Deleted **Author**

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.

Page 1: [13] Deleted **Author**

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.

Page 1: [14] Deleted **Author**

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.

Page 1: [15] Deleted **Author**

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

Page 1: [16] Deleted **Author**

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.

Page 1: [17] Deleted **Author**

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.

Page 1: [18] Deleted **Author**

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.

Page 1: [19] Deleted **Author**

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.

Page 1: [20] Deleted **Author**

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.

Page 1: [21] Deleted **Author**

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.

Page 1: [22] Deleted **Author**

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.

Page 1: [23] Deleted **Author**

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

a.