Final Mapping of VVSG 2007 Auditability Requirements to VVSG Cybersecurity Working Group Principles and Guidelines

After discussion of the Auditability gap analysis (http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/GapsInAuditRequirements.pdf), the Working Group decided to make the following changes to the principles and guidelines:

- Add the word "hardware" to the software independence guideline, now reading as follows:

  *An undetected error or fault in the **voting system's software or hardware** is not capable of causing an undetectable change in election results*

  This ensures that neither a hardware or software failure will affect the election outcome.

Other areas for future changes to the requirements include:

- The Human Factors and Interoperability Principles and Guidelines were not used in the initial mapping. That has been rectified. For instance, there was discussion on adding a new guideline on voter verification, but that is included within the Human Factors Principle titled *Marked as Intended*.
- Observational testing – the current thought is to remove these requirements.
- Ballot counter – Although these were discussed for removal, the current thought is to leave these requirements inside the VVSG.
- The group decided that the VVPAT requirements should be "up-leveled" so they are not technology specific, essentially removing the VVPAT requirements.
- Reconciliation audits need a more descriptive name that everyone understands.
- Reconciliation audits need to include Ballot on Demand and other ballots created throughout other voting channels / methods (e.g., postal voting for UOCAVA voters).

This information is based on the requirements found at:
http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/2007-VVSG.pdf

4.1 Overview of Auditing Requirements

This chapter contains requirements pertaining to independent voter-verifiable record (IVVR) voting systems to ensure that they can be audited independently of their software. As part of this material, this chapter also includes basic requirements for voter-verifiable paper audit trail voting systems (VVPATs) that have been updated from [VVSG2005].

The requirements in this chapter are necessary to ensure that IVVR systems fully meet the definition of software independence. IVVR systems in general meet the SI definition because they produce two records that can be compared against each other: (1) the electronic version of the CVR, and (2) the IVVR

summary of the electronic CVR that the voter has the opportunity to compare against the voting system's display of the electronic CVR.

However, additional requirements are still needed for IVVR systems to ensure that the audits can be independently verifiable. IVVR records must be constructed carefully for this purpose; IVVR systems must produce other supporting records for the purposes of verifying that the number of electronic CVRs is correct and for the purposes of being able to verify that the records are indeed authentic and have been produced by the appropriate authorized voting systems. Accordingly, this chapter contains the following sections:

- Section 4.2: high-level requirements to ensure that IVVR voting systems produce records that can be used in certain general types of independent audits;
- Section 4.3: requirements for electronic records created and exported by IVVR voting systems; and
- Section 4.4: requirements for IVVR and for VVPAT and PCOS voting systems that use voter-verifiable paper records (VVPR), i.e., paper IVVR.

4.2 Requirements for Supporting Auditing

This section presents requirements on voting system devices to provide the capability for certain general types of audits described herein. The audits work together to ensure independent agreement between what is presented to the voters by the IVVR vote-capture devices, what is counted by tabulators, and what is reported by the EMS as a final ballot count and vote totals.

Note: This section does not include requirements on election officials to perform the audits described herein. Audits are considered part of election procedures and cannot be mandated by the VVSG. The requirements in this section focus on ensuring that IVVR voting systems produce records that are capable of being used in independent audits so that the voting systems will meet. It is left to election procedures to mandate whether the audits are to be performed.

Auditing procedures for IVVR systems imposes requirements on the voting system in several ways, including:

A. Some auditing procedures need to reconcile that the number of electronic CVRs captured by the voting system is indeed accurate, that this number agrees with the number of voters who have cast a ballots.

B. Some auditing procedures need specific information or behavior from voting systems in order to be possible or practical. For example, hand auditing the correspondence between IVVR and electronic CVRs is only possible if the voting system produces IVVR and electronic CVRs that include the same information.

C. Some auditing procedures require certain assurances about the operation of the voting devices in order to be meaningful. For example, the hand audit of the paper and electronic records from VVPATs is meaningful only because voters had the opportunity to both view and verify the paper records.

Accordingly, there are three general types of audits anticipated for IVVR voting systems to ensure that the electronic CVRs and IVVRs fully agree. These are as follows:

1. Reconciliation Audit: Verifying that the number of voters for each reporting context and ballot style agrees with the totals reported by the tabulator. This guards against a tabulator reporting more votes than it had voters, or reassigning some voters to the wrong precinct or ballot style. This type of audit is referred to here as the pollbook audit.

2. Hand Count of IVVRs: Verifying by hand that the IVVR agree with the reported totals from the tabulator. This guards against a voting device silently misrecording votes.

3. Ballot Count and Vote Total Audit: Comparing IVVR vote-capture device records against final ballot and vote totals to verify that the electronic records from the tabulators agree with the final reported totals. This guards against a compromised EMS misreporting the final results.

Additional audit types that may be supported include:

- Risk Limiting Audits: A procedure for checking a sample of ballots (or IVVRs) that is guaranteed to have a large, pre-specified chance of correcting the reported outcome if the reported outcome is wrong (i.e., if a full hand count would reveal an outcome different from the reported outcome).
- Image Interpretation Audits: Automatically and procedurally verifying Cast Vote Records against images of IVVRs, in an attempt to identify any issues voters had marking ballots, and machines had when creating ballot images

4.2.1 Reconciliation Audit

The purpose of the reconciliation audit is to verify that:

- The total number of ballots recorded by the voting system in some location is the same as the total number of voters who have cast ballots.
- The total number of ballots recorded for each ballot configuration, and for each reporting context, is the same as the number of such voters authorized to vote with that ballot configuration, in those reporting contexts.

This mitigates the threat that a tampered tabulator (such as a PCOS scanner) might have inserted or deleted votes, and also the threat that it may have assigned some voters the wrong reporting context or ballot configuration to prevent them voting in certain elections or to dilute the effect of their votes.

4.2.1-A Voting system, support for the reconciliation audit

Requirement:	The voting system SHALL support a secure reconciliation audit that can detect differences in ballot counts between the pollbooks, vote-capture devices, activation devices, and tabulators.
Applies to:	Voting system
Test Reference:	Part 3:4.3 “Verification of Design Requirements”, 5.2 “Functional Testing”, 5.3 “Benchmarks”
Discussion:	The reconciliation audit is critical for blocking various threats on voting systems, such as simply inserting additional votes into the voting system. This requirement and its subrequirement are high-level “goal” requirements whose aim is to ensure that the voting system produces records that are adequate and usable by election officials for conducting reconciliation audits. This requirement is supported by various other requirements for general reporting and in Part 1:4.3 “Electronic Records”. It can be tested as part of the volume tests discussed in Part 1:7.8 “Reporting” and Part 3:5.3 “Benchmarks”; this type of testing may be useful for assessing the usability of the audit records for typical election environments.

Source:	[VVSG2005] I.2.1.5.1
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** Both the requirement and this guideline discuss analyzing the outcome and identifying any variances. *Security: Data Protection* Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. **Justification:** The Discussion section mentions the importance of the reconciliation audit and how it protects against the threat of adding, deleting, and modifying ballots.

4.2.1-A.1 Records and reports for reconciliation audit

Requirement:	The Vote-capture devices, activation devices, and tabulators SHALL support production and retention of records and reports that support the reconciliation audit.
Applies to:	Vote-capture device, Tabulator, Activation device
Test Reference:	Part 3:5.2 “Functional Testing”, 5.3 “Benchmarks”
Discussion:	The reconciliation audit is only practical when the number of ballots, and of each distinct type of ballot, is available from both the pollbooks and the tabulators.
Source:	[VVSG2005] I.5.4.4
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This guideline supports the requirements mention of the “production and retention of records and reports that support the reconciliation audit”.

4.2.2 Hand Count Verifies Machine Audit

The hand audit of verifies that the IVVRs and reported totals from a tabulator are in agreement. The hand audit addresses the threats that the voting device might record and report results electronically that disagree with the choices indicated by the voter.

4.2.2-A IVVR, support for hand audit

Requirement:	The voting system SHALL support a hand audit of IVVRs that can detect differences between the IVVR and the electronic CVR.
Applies to:	Voting system
Test Reference:	Part 3:5.2 “Functional Testing”, 5.3 “Benchmarks”
Discussion:	Hand auditing verifies the reported electronic records; IVVR offer voters an opportunity to discover attempts to misrecord their votes on the IVVR, and the

	hand audit ensures that devices that misrecord votes on the electronic record but not the IVVR are very likely to be caught. Hand auditing draws on the results from the pollbook audit and the ballot count and vote total. For example, the hand audit cannot detect insertion of identical invalid votes in both paper and electronic records in a VVPAT, but the pollbook audit can detect this since it reconciles the electronic CVR count with the number of voters who cast ballots. Similarly, the hand audit cannot detect that the summary of reported ballots from the tabulator or polling place agrees with the final election result, but this can be checked by the ballot count and vote total audit. This requirement and its subrequirement are high-level "goal" requirements whose aim is to ensure that the voting system produces records that are adequate and usable by election officials for conducting audits of IVVR records by hand. It can be tested as part of the volume tests discussed in Part 1:7.8 "Reporting" and Part 3:5.3 "Benchmarks"; this type of testing may be useful for assessing the usability of the audit records for manual audits in typical election volumes.
Source:	[VVSG2005] I.2.1.5.1
Principle(s)/ Guideline(s):	*Security: Auditability* An undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results. ***Justification:*** The requirement of a hand audit is to verify the electronic records. This aligns with software independence. The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** Both the requirement and this guideline discuss analyzing the outcome and identifying any variances. *Security: Data Protection* Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. **Justification:** The requirement mentions detecting differences between record data sources.

4.2.2-A.1 IVVR, information to support hand auditing

Requirement:	IVVR vote-capture devices and tabulators SHALL provide information to support hand auditing of IVVR.
Applies to:	IVVR vote-capture device, Tabulator
Test Reference:	Part 3:4.3 "Verification of Design Requirements", 5.2 "Functional Testing", 5.3 "Benchmarks"
Discussion:	The electronic summary information from the DRE or scanner and the IVVRs, must contain sufficient information to carry out the hand audit. Because the hand audit may be carried out at different reporting contexts (for example, a specific tabulator or a whole precinct or polling place may be selected for audit), the voting system must be able to provide reports that support hand auditing at each of the different reporting contexts.

Source:	[VVSG2005] I.5.4.4
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This guideline aligns directly with the requirement. Both the requirement and this guideline discuss analyzing the outcome and identifying any variances. *Security: Data Protection* Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. **Justification:** The requirement mentions detecting differences between record data sources.

4.2.3 VVPAT Match Paper Ballots Audit

The purpose of this process is to verify that the ballot counts and vote totals reported by EMSs are correct. This guards against the threat that the EMS used to produce the final results might be compromised. Please see Part 1:7.8 “Reporting”, Reporting, for information on ballot count and vote total reports.

4.2.3-A EMS, support for reconciling voting device totals

Requirement:	The EMS SHALL support the reconciliation of the tabulator totals and the final ballot count and vote totals according to the following: a. A tabulator whose reported totals are not correctly included in the ballot count and vote total reports, and which is audited, SHALL be detectable; b. A difference between the final ballot count and vote totals and the audit records for a tabulator that is audited SHALL be detectable; c. The disagreements in records SHALL be detectable even when the election management software is acting in a malicious way; and d. The EMS SHALL be able to provide reports that support ballot count and vote total auditing for different reporting contexts.
Applies to:	EMS
Test Reference:	Part 3:4.3 “Verification of Design Requirements”, 5.2 “Functional Testing”, 5.3 “Benchmarks”
Discussion:	This auditing process, part of the canvassing procedure, is a defense against problematic behavior by the voting device computing the final election ballot count and vote totals. Section 4.3 includes requirements to make this procedure easier to carry out and to add cryptographic protection to the records produced by the voting devices. One complication in making a full voting system support this procedure is the likely mixing of old and new voting devices in a full voting system. When the specific reporting context used is the same as for the hand audit, the ballot count and vote totals audit and hand audit together verify that the votes that appear on the IVVR correspond to the votes that are reported in the final election result.

	This requirement and its subrequirement can be tested as part of the volume tests discussed in Part 1 Section 7.8 and Part 3 Section 5.3.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* An undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results. **Justification:** The requirement states that any incorrect tabulation reports should be detectable. The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This guideline supports the requirements to produce reports and detect incorrect data or differences between the collected data.

4.2.3-B Records for ballot count/vote total audit

Requirement:	Vote-capture devices, tabulators, and activation devices SHALL produce records that support the ballot count and vote total audit.
Applies to:	Vote-capture device, Tabulator, Activation device
Test Reference:	Part 3:5.2 "Functional Testing", 5.3 "Benchmarks"
Discussion:	This auditing step requires that electronic summary records from voting devices can be reconciled with the final election ballot count and vote total reports. The ballot count and vote total records must thus be capable of breaking down totals by voting device as well as by precinct and polling place. Sections 4.3 and 4.4 specify content of the IVVR and electronic records, respectively, needed to support this requirement.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** The requirement specifies the production of records to support the ballot count and vote total audit.

4.2.4 Ensure System is Unaware of Testing Audit

Another issue in the operational behavior of accessible IVVR voting systems needs to be considered to ensure that they are software independent and independently auditable.

Accessible IVVR systems that provide an audio readback of the IVVR (e.g., a VVPAT's VVPR) may use the same software base to do the following:

- Permit the voter to make ballot choices;
- Create the IVVR of the voter's ballot choices; and
- Read back to the voter the IVVR.

To ensure that the accessible IVVR vote-capture device is interacting with the voter properly and recording voting choices accurately, the accessible IVVR voting system must allow for all voters to

A. Cast their votes using assistive technology such as the audio-tactile interface even if the voters do not require this technology to be able to vote, and
B. Verify the IVVR record with the audio readback.

Election procedures must actually ensure that sufficient numbers of voters use the accessible IVVR voting system in this way to ensure that the audio readback matches the IVVR record. These voters are able to confirm that both the IVVR and audio ballots contain the same information. This guards against the voting device selectively misrecording votes of voters with disabilities. For the purposes of discussion in this section, this type of voter behavior is referred to as Observational Testing.

4.2.4-A IVVR vote-capture device, observational testing

Requirement:	IVVR vote-capture devices that support assistive technology SHALL support observational testing.
Applies to:	IVVR vote-capture device ^ Acc-VS
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Blind, partial vision, and non-written languages voters may not be able to directly verify the IVVR produced by the voting system. This may be because they are using the audio-tactile interface, magnified screen images, or other assistive technology. This raises the possibility that a malicious IVVR vote-capture device could modify these voters’ votes by simply recording the wrong votes on both electronic records and IVVRs. Observational testing provides a defense by using volunteer voters. When observational testing is in use, a malicious IVVR vote-capture device cannot safely assume that a voter using the audio-tactile interface will be unable to check the IVVR record.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	

4.2.4-B IVVR vote-capture device, authentication for observational testing

Requirement:	The mechanism for authenticating the voter to the accessible IVVR vote-capture device SHALL NOT allow the IVVR vote-capture device to distinguish whether a voter is performing observational testing. The pollworker issuing the ballot activation for voters performing observational testing SHALL NOT be capable of signaling to the IVVR vote-capture device that it is being tested.
Applies to:	IVVR vote-capture device ^ Acc-VS, Activation device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Observational testing would not detect attacks if the IVVR vote-capture device were somehow alerted that the voter was carrying out observational testing. Thus, the authentication mechanism must not permit the device to discover this fact.
Source:	VVSG 2007 Requirement

Principle(s)/ Guideline(s):	

4.3 Overall Electronic Records Discussion

In order to support independent auditing, an IVVR voting system must be able to produce electronic records that contain the needed information in a secure and usable manner. Typically, this includes records such as:

- Vote counts;
- Counts of ballots recorded;
- Information that identifies the electronic record;
- Event logs and other records of important events or details of how the election was run on this device; or
- Election archive information.

By ensuring that certain records are produced, secured, and exported, many threats to security can be reduced, including tampering with electronic records in transit from the polling place to the tabulation center, tampering with the operation of the tabulation center, or altering election records after the totals are determined.

There are three types of requirements on electronic records in this section:

1. Requirements for how electronic records must be protected cryptographically;
2. Requirements for which electronic records must be produced by tabulators; and
3. Requirements for printed reports to support auditing steps.

4.3.1 Records from Voter Facing Machines

The following requirements apply to records produced by the voting system for any exchange of information between devices, support of auditing procedures, or reporting of final results. This includes the electronic version of all reports specified in Part 1:5.1 “Cryptography”.

4.3.1-A All records capable of being exported

Requirement:	The voting system SHALL provide the capability to export its electronic records to files.
Applies to:	Voting system
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	The exported format for the records must meet the requirements for data export in Part 1:6.6 “Integratability and Data Export/Interchange”.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root

	cause of any irregularities. **Justification:** To fulfill this requirement, records must be produced to have electronic records to export.

4.3.1-B All records capable of being printed

Requirement:	The voting system SHALL provide the ability to produce printed forms of its electronic records. a. The printed forms SHALL retain all required information as specified for each record type other than digital signatures; b. The printing MAY be done from a different device than the voting device that produces the electronic record; and **c.** It shall be possible to print records produced by the central tabulator or EMS on a different device.
Applies to:	Voting system
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Printed versions of all records in this chapter are either necessary or extremely helpful to support required auditing steps. Ensuring that the printing can be done from a machine other than the tabulator used to compute the final totals for the election supports the vote total audit, and is a logical consequence of the requirement for a fully open record format.
Source:	[VVSG2005] I.2.1.5.1-a
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This guideline follows the required electronic records in the requirement.

4.3.1-C Cryptographic protection of records from voting devices

Requirement:	Electronic records SHALL be digitally signed with the Election Signature Key.
Applies to:	Voting system
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	The digital signatures address the threat that the records might be tampered with in transit or in storage. When combined with the Election Public Key Certificate, the signature also addresses the threat that a legitimate electronic record might be misinterpreted as coming from the wrong voting device or scanner. The use of per-election keys to sign these records addresses the threat that a compromise of a voting device before or after election day might permit production of a false set of records for the election, which could then be reported to the EMS. This requirement mandates a similar optional recommendation in [VVSG2005] 7.9.3-d which applies only to VVPATs. There is no requirement that states that all electronic records must be signed in the [VVSG2005].
Source:	[VVSG2005] I.7.9.3-d
Principle(s)/ Guideline(s):	*Security: Data Protection* Voting systems prevent unauthorized to or manipulation of configuration data,

	cast vote records, transmitted data and audit records. **Justification:** As mentioned in the discussion, this requirement addresses "the threat that records might be tampered with in transit or in storage". The digital signatures with the Election Signature Key ensure the integrity of the data within the electronic records have not be modified. The source and integrity of electronic tabulation reports are verifiable. **Justification:** The digitally signed electronic records allow for verification.

4.3.2 Records from Counting Machines

The following requirements apply to records produced by tabulators, such as DREs and optical scanners, for exchange of information between devices, transmission of results to the EMS, support of auditing procedures, or reporting of intermediate election results.

4.3.2-A Tabulator, summary count record

Requirement:	Each tabulator SHALL produce a Tabulator Summary Count record including the following: a. Device unique identifier from the X.509 certificate; b. Time and date of summary record; c. The following, both in total and broken down by ballot configuration and precinct: 1. Number of read ballots; 2. Number of counted ballots; 3. Number of rejected electronic CVRs; and 4. For each N-of-M (including 1-of-M) or cumulative voting contest appearing in any ballot configuration handled by the tabulator: I. Number of counted ballots that included that contest, per the definition of K(j,r,t) in Part 1:Table 8-2; II. Vote totals for each non-write-in contest choice per the definition of T(c,j,r,t) in Part 1:Table 8-2; III. Number of write-in votes; IV. Number of overvotes per the definition of O(j,r,t) in Part 1:Table 8-2; and V. Number of undervotes per the definition of U(j,r,t) in Part 1:Table 8-2. In producing this summary count record, the tabulator SHALL assume that no provisional or challenged ballots are accepted.
Applies to:	Tabulator
Test Reference:	Part 3:4.5 "Source Code Review", 5.2 "Functional Testing"
Discussion:	The Tabulator Summary Count Record is essentially an estimated summary report from the viewpoint of the individual tabulator, for auditing purposes. Since the eventual disposition of provisional ballots, challenged ballots, and write-in votes is unknown at the close of polls, arbitrary assumptions are made in

	order to make a summary possible. All provisional and challenged ballots are assumed rejected, and all write-in votes are effectively aliased to a single contest choice that is not one of the choices "on the ballot." The quantities provided for each contest should balance in the sense that N × K = sum of non-write-in vote totals (T) + write-ins + overvotes (O) + undervotes (U). In addition to the reporting context corresponding to the tabulator itself, reporting contexts corresponding to the different ballot configurations handled by that tabulator are synthesized. These contexts are quite narrow in scope as they include only the ballots of a specific configuration that were counted by a specific tabulator. The tabulator is not required to handle the complexities of reporting contexts that are outside of its scope. This record is sufficient to support random audits of paper records. The record will not contain the results of election official review of review-required ballots, so auditors can use this record to verify that the number of these ballots is correct, but will need to do further steps to verify that these ballots were handled correctly. This record can be used to verify a correct result from a system under parallel testing. This record can be used to randomly check electronic totals, when the final results are given broken out by voting system or scanner. When used in the Ballot Count and Vote Total Audit, this record blocks the class of attacks that involves tampering with the EMS computer used to compute the final totals. The tabulator summary could in principle be published for each voting system, along with corrected final totals for each precinct and for absentee ballots, to show how the final election outcomes were computed, though care would have to be taken to avoid violations of voter privacy. For auditing, this record must be output in a human-readable format, such as a printed report. This requirement clarifies [VVSG2005] I.2.4.3, which describes the vote data summary reports that all voting systems are required to produce. While [VVSG2005] I.2.4.3 applies to voting systems as a whole, this requirement specifically requires that all vote tabulators produce such a report.
Source:	[VVSG2005] I.2.4.3
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement calls for records to be produced for auditing purposes.

4.3.2-B Tabulator, summary count record handling

Requirement:	The tabulator SHALL handle the summary count record according to the following:

	a. The record SHALL be transmitted to the EMS with the other electronic records; b. It SHALL be stored in the election archive, if available; and **c.** It SHALL be stored in the voting systems event log.
Applies to:	Tabulator
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification**: This requirement calls for records to be produced for auditing purposes. *Security: Detection/Monitoring* Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing. **Justification:** It is required that the records be stored in the event log.

4.3.2-C Tabulator, collection of ballot images record

Requirement:	Tabulators SHOULD produce a record of ballot images that includes: a. Time and date of creation of complete ballot image record; and b. Ballot images recorded in randomized order by the DRE for the election. For each voted ballot, this includes: 1. Ballot configuration and counting context; 2. Whether the ballot is accepted or rejected; 3. For each contest: I. The choice recorded, including undervotes and write-ins; and II. Any information collected by the vote-capture device electronically about each write-in; Information specifying whether the ballot is provisional, and providing unique identifier for the ballot, as well as provisional category information required to support Requirement Part 1:7.7.2-A.6.
Applies to:	Tabulator
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This record is not required for auditing, however it is useful.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** Although this requirement is not necessarily for auditing purposes, the records produced from this requirement may prove helpful when auditing.

4.3.2-C.1 DRE, collection of ballot images record

Requirement:	DREs SHALL produce a record of ballot images that includes: a. Time and date at poll closing; and b. Ballot images recorded in randomized order by the DRE for the election. For each voted ballot, this includes: 1. Ballot configuration and counting context; 2. Whether the ballot is accepted or rejected; 3. For each contest: I. The choice recorded, including undervotes and write-ins; and II. Any information collected by the vote-capture device electronically about each write-in; **4.** Information specifying whether the ballot is provisional, and providing unique identifier for the ballot, as well as provisional category information required to support Requirement Part 1:7.7.2-A.6.
Applies to:	DRE
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	DREs already contain the information to create the ballot image records. This requirement extends [VVSG2005] I.7.9.3-b by requiring an audit record containing electronic ballot images, and specifies other information that must be contained in this record. This requirement extends [VVSG2005] I.7.9.3-e by requiring that VVPATs produce an audit record containing electronic ballot images. [VVSG2005] I.7.9.3-e only requires that electronic ballot images be exportable for auditing purposes.
Source:	[VVSG2005] I.7.9.3-b, I.7.9.3-e
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** Although this requirement is not necessarily for auditing purposes, the records produced from this requirement may prove helpful when auditing.

4.3.2-C.2 Tabulator. Collection of cast votes handling

Requirement:	Tabulators that produce the collection of ballot images record SHALL handle the record according to the following: a. The record SHALL be transmitted to the EMS with the other electronic records; b. It SHALL be stored in the election archive, if available; and **c.** It SHALL be stored in the voting systems event log.
Applies to:	Tabulator
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	
Source:	VVSG 2007 Requirement

Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement calls for records to be produced for auditing purposes. *Security: Detection/Monitoring* Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing. **Justification:** It is required that the records be stored in the event log.

4.3.2-D Tabulator, electronic records event log record handling

Requirement:	The tabulator SHALL digitally sign the event log, transmit the signed event log to an EMS, and retain a record of the transmission.
Applies to:	Tabulator
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	The EMS can verify that the event log record is received and that the digital signature and per election key and certificate are valid.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. **Justification:** The digital signing of the event log will provide verification that the log was not modified.

4.3.3 Records from the Backend

The following requirements apply to the records produced by an EMS. EMSs include both DREs used as accumulators in the polling place, called a Precinct EMS, as well as EMSs used as jurisdiction-wide accumulators. All of the requirements for tabulators apply to EMSs. This section addresses additional requirements based on an EMSs role as an accumulator of ballot counts and vote totals.

4.3.3-A EMS tabulator summary count record

Requirement:	The EMS Tabulator Summary Count Record SHALL include: a. Unique identifiers for each tabulator contained in the summary; b. For tabulators with public keys: 1. The public key for each tabulator in the summary; 2. The Election Signature Key certification and closeout record; and 3. Signed tabulator summary count record. c. Summary ballot counts and vote totals by tabulator, precinct, and polling place. 1. Precinct totals include subtotals from each tabulator used in the precinct.
Applies to:	EMS
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”

Discussion:	Requirements in Part 1 Section 7.8 ensure that the EMS is capable of producing a report containing this information. This report is required to allow checking of the final ballot counts and vote totals, based on their agreement with local totals, without relying on the correct operation of equipment and execution of procedures at the tabulation center. The goal is to provide cryptographic support for a process that is currently done in a manual, procedural way, which may be subject to undetected error or tampering. This record can be used to detect most problems at the tabulation center. Item c.1 is needed for cases when a tabulator, such as a DRE, contains votes from multiple precincts. Note: The requirement supports older voting systems to allow for transitioned upgrades of fielded equipment. This requirement extends [VVSG2005] I.2.4.3; this requirement specifically requires that each tabulation center EMS produce this report.
Source:	[VVSG2005] I.2.4.3
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement calls for records to be produced for auditing purposes.

4.3.3-A.1 Tabulator, report combination for privacy

Requirement:	The EMS shall be capable of combining tabulator reports to protect voter privacy in cases when there are tabulators with few votes.
Applies to:	EMS
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	
Source:	
Principle(s)/ Guideline(s):	*Human Factors: Cast as marked* The voting process preserves the secrecy of the ballot. The voting system ensures that ballot selections, interface options, voter identity and information about voters are kept private. *Security: Ballot Secrecy* Records produced by the voting system do not reveal how a voter voted. **Justification:** This requirement protects voter privacy.

4.3.3-B EMS, precinct summary count records

Requirement:	The EMS SHALL produce a report for each precinct including: a. Each tabulator included in the precinct with its unique identifier; b. Number of read ballots; c. Number of counted ballots; d. Number of rejected electronic CVRs; and e. For each N-of-M (including 1-of-M) or cumulative voting contest appearing in any ballot configuration handled by the tabulator:

	1. Number of counted ballots that included that contest, per the definition of K(j,r,t) in Part 1:Table 8-2; 2. Vote totals for each non-write-in contest choice per the definition of T(c,j,r,t) in Part 1:Table 8-2; and 3. Number of write-in votes
Applies to:	EMS
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	This report supports hand auditing of paper records against the final totals, the ballot count and vote totals audit, and the pollbook audit. This requirement extends [VVSG2005] I.2.4.3; this requirement specifically requires that each tabulation center EMS produce the report.
Source:	[VVSG2005] I.2.4.3
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement calls for records to be produced for auditing purposes.

4.3.3-C EMS, precinct adjustment record

Requirement:	The EMS SHALL produce a report showing the changes made to each contest based on the resolution of provisional ballots, challenged ballots, write-in choices, and the date and time of the report.
Applies to:	EMS
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This report may be produced more than once during the course of an election as the resolution of provisional ballots, challenged ballots, and write-in choices are processed. This report can be used to support pollbook audit showing that number of ballots processed do not exceed the total recorded by the tabulator as well as to support the ballot total and vote count audit. Many jurisdictions resolve provisional and challenged ballots in groups to protect voter privacy.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement calls for records to be produced for auditing purposes.

4.3.4 Validating Voting Record Digital Signatures

4.3.4-A Tabulator, verify signed records

Requirement:	For each tabulator producing electronic records, the EMS SHALL verify: a. The Election Public Key Certificate associated with the record is

	valid for the current election, using the public key of the tabulator to verify the certificate as specified in Part 1:5.1 “Cryptography”; b. The election ID and timestamp of the record agrees with the current election and the values in the Election Public Key Certificate; and c. The digital signature on the record is correct, using the Election Public Key to verify it.
Applies to:	EMS
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	The digital signature applied to the electronic records from the voting devices is only useful if it is verified before the EMS accepts electronic records. A DRE that accumulates results at a precinct or polling place is serving as a precinct level EMS.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement calls for records to be produced for auditing purposes. *Security: Data protection* Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. **Justification:** The tools used for verification within this requirement follow this guideline. Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit record. **Justification:** The tools used for verification within this requirement follow this guideline. The source and integrity of electronic tabulation reports are verifiable. **Justification:** The tools used for verification within this requirement follow this guideline.

4.3.5 Tabulator Requirements

4.3.5-A Ballot counter

Requirement:	Tabulators and vote-capture devices SHALL maintain a count of the number of ballots read at all times during a particular test cycle or election.
Applies to:	Tabulator, Vote-capture device
Test Reference:	Part 3:3.2 “Functional Testing”
Discussion:	For auditability, the ballot count must be maintained (incremented each time a ballot is read) rather than calculated on demand (by counting the ballots currently in storage). This requirement restates [VVSG2005] I.2.1.8.
Source:	Implied by design requirements in [VSS2002] I.2.2.9, [VVSG2005] I.2.1.8

Principle(s)/ Guideline(s):	*Security: Auditability* Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. **Justification:** This guideline somewhat reflects this requirement.

4.3.5-B Ballot counter, availability

Requirement:	Tabulators SHALL enable election judges to determine the number of ballots read at all times during a particular test cycle or election without disrupting any operations in progress.
Applies to:	Tabulator, Vote-capture device
Test Reference:	Part 3:3.2 “Functional Testing”
Discussion:	[VSS2002] I.2.4 refers to separate “election counter” and “life-cycle counter;” the latter was an error (intended to delete). This requirement clarifies [VVSG2005] I.2.1.8 by stating that reading the ballot counter must not disrupt voting system operations.
Source:	Implied by design requirements in [VSS2002] I.2.2.9, I.2.1.8
Principle(s)/ Guideline(s):	

4.4 Independent Voter-Verifiable Records

This chapter contains requirements for voting systems that produce and use independent voter-verifiable records (IVVR). IVVR are generally understood to mean voter-verifiable paper records (VVPR); however non-paper IVVR, once developed, could be used to still satisfy these requirements. There are two broad categories of paper-based IVVR, i.e., VVPR:

- VVPATs couple an electronic voting device with a printer. The voter makes selections on the voting device, but is given the opportunity to review and verify choices on a paper record. The paper record may be a continuous roll or cut sheets.
- Optical scan voting systems use paper ballots that are humanreadable and may be marked by either hand or device, along with an electronic scanner that checks the ballot for problems such as under- and over-votes, and also records the votes.

For all IVVR systems, the records are available to the voter to review and verify, and these records are retained for later auditing or recounts as needed. This chapter addresses the use of the records for auditing and security. The chapter first presents the requirements for IVVR systems and then presents specific requirements for VVPR systems.

4.4.1 Ballot Requirements

Voter-verifiable records exist to provide an independent record of the voter’s choices that can be used to verify the correctness of the electronic record produced by the voting device.

4.4.1-A IVVR vote-capture device, IVVR creation

Requirement:	The IVVR vote-capture device shall create an independent voter verifiable

	record.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement is further defined by its subrequirements. Its purpose is to ensure that a single IVVR meets all requirements and all properties as outlined in the following subrequirements.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement states that the vote-capture device must create a record. An undetected error or fault in the voting system’s software is not capable of causing an undetectable change in election results. **Justification:** The record produced from the vote-capture device will ensure the software has not made any changes to the election results.

4.4.1-A.1 IVVR vote-capture device, IVVR direct verification by voters

Requirement:	IVVR vote-capture devices SHALL create an IVVR that voters can verify (a) without software, or (b) without programmable devices excepting assistive technology.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	The exclusion of software or programmable devices from the voter verification process is necessary for the system to be software independent. It suffices to meet this requirement that most voters can review the record directly. Voters who use some assistive technologies may not be able to directly review the record. This requirement allows for observational testing to be able to determine whether the assistive technology is operating without error or fraud.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Interoperability: Transparent* The processes and transactions associated with the voting system are easy for the public to understand and verify. *Human Factors: Marked As Intended* Understandable – Voters can understand all information as it is presented. *Security: Auditability* An undetected error or fault in the voting system’s software is not capable of causing an undetectable change in election results **Justification:** Voters will use the IVVR created, to verify there are no changes to their votes.

4.4.1-A.2 IVVR vote-capture device, IVVR direct review by election officials

Requirement:	IVVR vote-capture devices SHALL create an IVVR that election officials and auditors can review without software or programmable devices.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	The exclusion of programmable devices from the voter verification process is necessary for the system to be software independent.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Interoperability: Transparent* The processes and transactions associated with the voting system are easy for the public to understand and verify. *Security: Auditability* An undetected error or fault in the voting system’s software is not capable of causing an undetectable change in election results **Justification:** Election officials and auditors will use the IVVR created, to verify there are no changes to the elections results.

4.4.1-A.3 IVVR vote-capture device, support for hand auditing

Requirement:	IVVR vote-capture devices SHALL create an IVVR that election officials can use without software or programmable devices to verify that the reported electronic totals are correct.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	The records must support a hand audit that uses no programmable devices to read or interpret the records. The hand audit may provide a statistical basis for other larger audits or recounts performed using technology (such as OCR).
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement calls for records to be produced for auditing purposes. An undetected error or fault in the voting system’s software is not capable of causing an undetectable change in election results **Justification:** Election officials and auditors will use the IVVR created, to verify there are no changes to the elections results.

4.4.1-A.4 IVVR vote-capture device, IVVR use in recounts

Requirement:	IVVR vote-capture devices SHALL create an IVVR that election officials can use to reconstruct the full set of totals from the election.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 “Functional Testing”

Discussion:	This requirement addresses the completeness of the records, rather than their technology independence.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement calls for records to be produced for auditing purposes. An undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results **Justification:** Election officials and auditors will use the IVVR created, to verify there are no changes to the elections results.

4.4.1-A.5 IVVR vote-capture device, IVVR durability

Requirement:	IVVR vote-capture devices SHALL create an IVVR that will remain unchanged for minimally 22 months unaffected by power failure, software failure, or other technology failure.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement calls for records to be produced for auditing purposes. An undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results. **Justification:** Election officials and auditors will use the IVVR created, to verify that no changes are made to the elections results. *Security: Data Protection* Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. **Justification:** It is required that the IVVR created remains unchanged.

4.4.1-A.6 VVR vote-capture device, IVVR tamper evidence

Requirement:	IVVR vote-capture devices SHALL create an IVVR that show evidence of tampering or change by the voting system.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	

Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* An undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results **Justification:** Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. **Justification:**

4.4.1-A.7 IVVR vote-capture device, IVVR support for privacy

Requirement:	IVVR vote-capture devices SHALL create an IVVR for which procedures or technology can be used to protect voter privacy.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Privacy protection includes a method to separate the order of voters from the order of records or procedural means to ensure that information relating to the order of voters, including time a record is created, can be protected. Privacy also includes other methods to make records hard to identify, normally by having them be indistinguishable from each other.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement calls for records to be produced for auditing purposes. *Security: Ballot Secrecy* Records produced by the voting system do not reveal how a voter voted **Justification:** This requirement protects the voter's privacy, which may include the privacy of how a voter voted.

4.4.1-A.8 IVVR vote-capture device, IVVR public format

Requirement:	IVVR vote-capture devices shall create an IVVR in a non-restrictive, publicly available format, readable without confidential, proprietary, or trade secret information.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Interoperability: Transparent* Data reported by the voting system is in a publicly documented format. *Security: Auditability*

	An undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results. **Justification:** With the IVVR created in a human readable format, voters, election officials, and auditors can verify that no changes are made to the ballots.

4.4.1-A.9 IVVR vote-capture device, IVVR unambiguous interpretation of cast vote

Requirement:	Each IVVR SHALL contain a human-readable summary of the electronic CVR. In addition, all IVVR SHALL contain audit-related information including: a. Polling place; b. Reporting context; c. Ballot configuration; d. Date of election; and **e.** Complete summary of voter's choices.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	All IVVR contain some human-readable content. In addition, some IVVR may use machine-readable content to make counting or recounting more efficient. For example, PCOS systems place a human-readable representation of the votes beside a machine-readable set of ovals to be marked by a human or a machine. The human-readable content of the IVVR must contain all information needed to interpret the cast vote. This is necessary to ensure that hand audits and recounts can be done using only the human-readable parts of the paper records. This requirement generalizes [VVSG2005] I.7.9.1-b, I.7.9.1-c and I.7.9.3-h by extending its provisions to include all IVVR.
Source:	[VVSG2005] I.7.9.1-b, I.7.9.1-c, I.7.9.3-h
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement calls for records to be produced for auditing purposes. An undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results **Justification:** Election officials and auditors will use the IVVR created, to verify there are no changes to the elections results.

4.4.1-A.10 IVVR vote-capture device, no codebook required to interpret

Requirement:	The human-readable ballot contest and choice information on the IVVR SHALL NOT require additional information, such as a codebook, lookup table, or other information, to unambiguously determine the voter's ballot choices.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	The hand audit of records requires the ability for auditors to verify that the

	electronic CVR as seen and verified by voters is the same as the electronic CVR that was counted. This requires that the auditor have all information necessary on the IVVR to interpret completely how the contests were voted. If an external codebook or lookup table were needed to interpret the IVVR, there would be no way for the auditor to be certain that the codebook had not changed since the voter used it.
Source:	
Principle(s)/ Guideline(s):	*Interoperability: Transparent* The processes and transactions associated with the voting system are easy for the public to understand and verify. *Human Factors: Marked As Intended* Understandable – Voters can understand all information as it is presented. **Justification:** A human-readable ballot must be understandable for the verification purposes.

4.4.1-A.11 IVVR vote-capture device, multiple physical media

Requirement:	When a single IVVR spans multiple physical media, each physical piece of media SHALL include polling place, reporting context, ballot configuration, date of election, and number of the media and total number of the media (e.g. page 1 of 4).
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	This requirement generalizes [VVSG2005] I.7.9.6-f by describing the information that must be included on each piece of physical media for an IVVR spread across multiple pieces of media and extends its provisions to include all IVVR.
Source:	[VVSG2005] I.7.9.6-f
Principle(s)/ Guideline(s):	*Interoperability: Transparent* Data used in critical device operations such as for cast vote records, tabulations, and event logs includes all elements necessary for verification of the data, and analysis and auditability of the operations. *Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** The requirement specifies what shall be included on the produced records.

4.4.1-A.12 IVVR vote-capture device, IVVR accepted or rejected

Requirement:	The IVVR SHALL be marked as accepted or rejected in the presence of the voter.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Unambiguous verification or rejection markings address the threat that the voting device might attempt to accept or reject ballot summaries without the

	voter's approval. This requirement extends [VVSG2005] I.7.9.2-b to all IVVR voting systems.
Source:	[VVSG2005] I.7.9.2-b
Principle(s)/ Guideline(s):	*Interoperability: Transparent* The processes and transactions associated with the voting system are easy for the public to understand and verify. *Human Factors: Marked As Intended* Understandable – Voters can understand all information as it is presented. **Justification:** The voter must be able to understand the process to accept or reject.

4.4.1-A.13 IVVR vote-capture device, IVVR accepted or rejected for multiple physical media

Requirement:	Each piece of IVVR physical media or SHALL be individually accepted or rejected by the voter.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	It must be unambiguous that all choices were rejected or accepted. This can be done at the end of physical media (e.g., a cut sheet VVPAT) or per contest.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Interoperability: Transparent* The processes and transactions associated with the voting system are easy for the public to understand and verify. *Human Factors: Marked As Intended* Understandable – Voters can understand all information as it is presented. **Justification:** The voter must be able to understand the process to accept or reject.

4.4.1-A.14 IVVR vote-capture device, IVVR non-human-readable contents permitted

Requirement:	The IVVR MAY include machine-readable encodings of the electronic CVR and other information that is not human-readable.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	This requirement extends [VVSG2005] I.7.9.3-g to include all IVVR.
Source:	[VVSG2005] I.7.9.3-g
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system supports efficient audits. **Justification:** Machine-readable encodings may allow for an efficient audit method.

4.4.1-A.15 IVVR vote-capture device, IVVR machine-readable part contains same information as human-readable part

Requirement:	If a non-human-readable encoding is used on the IVVR, it SHALL contain the entirety of the human-readable information on the record.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	The machine-readable part of the IVVR must permit the reconstruction of the human-readable part of the record.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* The voting system produces records that provide the ability to check whether the election outcome is correct, and to the extent possible, identify the root cause of any irregularities. **Justification:** This requirement calls for records to be produced for auditing purposes.

4.4.1-A.16 IVVR vote-capture device, IVVR machine-readable contents may include error correction/detection information

Requirement:	If a non-human-readable encoding is used on the IVVR, the encoding MAY also contain information intended to ensure the correct decoding of the information stored within, including: a. Checksums; b. Error correcting codes; c. Digital signatures; and d. Message Authentication Codes.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Error correction/detection information is used to protect digital data from error or tampering. This information would not be meaningful to a human, so there is no reason to demand that it also appear in the human-readable part of the record. This requirement extends [VVSG2005] 7.9.3-g to include all IVVR.
Source:	[VVSG2005] I.7.9.3-g
Principle(s)/ Guideline(s):	*Security: Auditability* Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. **Justification:** The encoding may ensure the integrity of the information on the IVVR. *Security: Data Protection* Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. **Justification:** The encoding may ensure the integrity of the information on the IVVR.

4.4.1-A.17 IVVR vote-capture device, public format for IVVR non-human-readable data

Requirement:	Any non-human-readable information on the IVVR SHALL be presented in a fully disclosed public format.
Applies to:	IVVR vote-capture device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Meaningful automated auditing requires full disclosure of any non-human-readable encodings on the IVVR. However, hand auditing does not require disclosure of this kind. This requirement extends [VVSG2005] I.7.9.3-e to include all IVVR.
Source:	[VVSG2005] I.7.9.3-f
Principle(s)/ Guideline(s):	*Interoperability: Transparent* Data reported by the voting system is in a publicly documented format. **Justification:** This requirement aligns with this guideline.

4.4.3 Precinct Count Optical Scan Requirements

A PCOS voting system involves paper ballots marked in a way that is both human and machine-readable. The following requirements apply to optical scan ballots, as required for supporting audit and recount.

4.4.3-A Optical scanner, optional marking

Requirement:	Optical scanners MAY add markings to each paper ballot, such as: a. Unique record identifiers to allow individual matching of paper and electronic CVRs; b. Digital signatures; and **c.** Batch information.
Applies to:	Optical scanner
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Auditability* Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. **Justification:** The encoding may ensure the integrity of the information on the IVVR. *Security: Data Protection* Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. **Justification:** The encoding may ensure the integrity of the information on the IVVR.

4.4.3-A.1 Optical scanner, optional marking restrictions

Requirement:	Optical scanners that add markings to paper ballots scanned SHALL NOT be capable of altering the contents of the human-readable CVR on the ballot. Specifically, optical scanners capable of adding markings to the scanned ballots SHALL NOT permit:

	a. Marking in the regions of the ballot that indicate voter choices; b. Marking in the regions of the ballot that contain the human-readable description of the marked choice; and **c.** Marking in regions reserved for timing marks.
Applies to:	Optical scanner
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	If the scanner could alter the human-readable contents of the ballot, or mark the ballot, after scanning, then the paper records stored by the scanner could no longer be considered voter-verifiable, and the optical scan system would no longer be software independent.
Source:	VVSG 2007 Requirement
Principle(s)/ Guideline(s):	*Security: Data Protection* Voting systems prevent unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. **Justification:** This requirement ensures the optical scanners that add markings to not manipulate the data on the CVR.