Mapping of VVSG 2007 Ballot Secrecy Requirements to VVSG Cybersecurity Working Group Principles and Guidelines

After discussion of the Ballot Secrecy gap analysis (http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/BallotSecrecy-GapAnalysis-06062017-1.pdf), the Working Group decided to make the following changes to the principles and guidelines:

- The second Ballot Secrecy guideline should be amended to include "other election artifacts". Another amendment is to include "notifications" and reads as follows:

  *Records, **notifications**, and **other election artifacts** produced by the voting system do not reveal how a voter voted.*

  This ensures that all logs and notifications/warnings do not violate ballot secrecy.

- The second Ballot Secrecy guideline should be amended to include "any identifiable" and reads as follows:

  *Records, notifications, and other election artifacts produced by the voting system do not reveal **the intent, choices, or selections of any identifiable** voter.*

  This modifies the guideline to bring it in line with modern terminology.

- Add a new Ballot Secrecy guideline, which reads as follows:

  The voting system does not have access to both a voter's identity and the content of voted ballot selections.

  This new guideline ensures there is no connection between voter registration information and voted ballots. Both 7.5.1.2-A.2 and 7.5.1.2-A.3 are associated with this guideline.

Other areas for future changes and development to the VVSG auditability requirements include:

- Remove "without the voter's cooperation" from 3.2.3's introduction.
- Develop definitions for ballot secrecy and voter privacy.
- Categorize these requirements into ballot secrecy and voter privacy.
- Rewrite the Requirement and Discussion section for 3.2.3.1.
- Develop and/or enhance requirements that ensure voter information is not included on the cast vote records (e.g. IP address or precinct number). For instance, it is importance to make sure that information about the remote ballot marking session does not violate voter privacy or ballot secrecy.

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

3.2.3 Privacy

The voting process must preclude anyone else from determining the content of a voter's ballot without the voter's cooperation. Privacy ensures that the voter can cast votes based solely on his or her own preferences without intimidation or inhibition.

3.2.3.1 Privacy at the polls

Requirement:	The voting system SHALL prevent others from determining the contents of a ballot.
Applies to:	Voting system
Test Reference:	Part 3:3.2 “Functional Testing”
Discussion:	The voting system itself provides no means by which others can "determine" how one has voted. Of course voters could simply tell someone else for whom they voted, but the system provides no evidence for such statements, and therefore voters cannot be coerced into providing such evidence. It is assumed that the system is deployed according to the installation instructions provided by the manufacturer. Whether the configuration of the voting system protects privacy may well depend on proper setup.
Source:	VVSG2007
Principle(s)/ Guideline(s):	*Human Factors: Cast As Marked* 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 directly aligns with these ballot secrecy guidelines.

3.2.3.1-A.1 Visual privacy

Requirement:	The ballot, any other visible record containing ballot information, and any input controls SHALL be visible only to the voter during the voting session and ballot submission.
Applies to:	Voting system
Test Reference:	Part 3:3.2 “Functional Testing”
Discussion:	This requirement may involve different approaches for electronic and paper interfaces. In both cases, appropriate shielding of the voting station is important. When a paper record with ballot information needs to be transported by the voter, devices such as privacy sleeves may be necessary. This requirement applies to all records with information on votes (such as a vote verification record) even if that record is not itself a ballot.
Source:	VVSG2007
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* Ballot secrecy is maintained throughout the voting process. Records produced by the voting system do not reveal how a voter voted. **Justification:** This requirement aligns with these ballot secrecy guidelines.

3.2.3.1-A.3 Privacy of warnings

Requirement:	The voting system SHALL issue all warnings in a way that preserves the privacy of the voter and the confidentiality of the ballot.
Applies to:	Voting system
Test Reference:	Part 3:3.2 “Functional Testing”
Discussion:	HAVA 301 (a)(1)(C) mandates that the voting system must notify the voter of an attempted overvote in a way that preserves the privacy of the voter and the confidentiality of the ballot. This requirement generalizes that mandate.
Source:	VVSG2007
Principle(s)/ Guideline(s):	*Security: Ballot Secrecy* Records, **notifications**, and **other election artifacts** produced by the voting system do not reveal how a voter voted. **Justification:** This requirement aligns with these ballot secrecy guidelines.

3.2.3.1-A.4 No receipts

Requirement:	The voting system SHALL NOT issue a receipt to the voter that would provide proof to another of how the voter voted.
Applies to:	Voting system
Test Reference:	Part 3:3.2 “Functional Testing”
Discussion:	
Source:	VVSG2007
Principle(s)/ Guideline(s):	*Security: Ballot Secrecy* Records produced by the voting system do not reveal how a voter voted. **Justification:** This requirement aligns with these ballot secrecy guidelines.

3.2.3.2 No recording of alternative format usage

When voters use non-typical ballot interfaces, such as large print or alternative languages, their anonymity may be vulnerable. To the extent possible, only the logical contents of their ballots should be recorded, not the special formats in which they were rendered. In the case of paper ballots, where the interface is the record, some format information is unavoidably preserved.

3.2.3.2-A No recording of alternative languages

Requirement:	No information SHALL be kept within an electronic CVR that identifies any alternative language feature(s) used by a voter.

Applies to:	Voting system
Test Reference:	Part 3:3.2 “Functional Testing”
Discussion:	
Source:	VVSG2007
Principle(s)/ Guideline(s):	*Human Factors: Cast As Marked* 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 aligns with these ballot secrecy guidelines.

3.2.3.2-B No Recording of Accessibility Features

Requirement:	No information SHALL be kept within an electronic CVR that identifies any accessibility feature(s) used by a voter.
Applies to:	Voting system
Test Reference:	Part 3:3.2 “Functional Testing”
Discussion:	
Source:	VVSG2007
Principle(s)/ Guideline(s):	*Human Factors: Cast As Marked* 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 aligns with these ballot secrecy guidelines.

3.3.3-C.1 Standard connector

Requirement:	The ATI SHALL provide its audio signal through an industry standard connector for private listening using a 3.5mm stereo headphone jack to allow voters to use their own audio assistive devices.
Applies to:	VEBD-A
Test Reference:	Part 3:3.2 “Functional Testing”
Discussion:	
Source:	VVSG2007
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* Ballot secrecy is maintained throughout the voting process. **Justification:** This requirement aligns with these ballot secrecy guidelines.

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:	VVSG2007
Principle(s)/ Guideline(s):	*Human Factors: Cast As Marked* 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 aligns with these ballot secrecy guidelines.

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:	
Source:	VVSG2007
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* Ballot secrecy is maintained throughout the voting process. Records produced by the voting system do not reveal how a voter voted. **Justification:** This requirement aligns with these ballot secrecy guidelines.

4.4.2.2-C VVPAT, error handling specific requirements

Requirement:	If a printer error or malfunction is detected, the VVPAT SHALL: a. Present a clear indication to the voter and election officials of the malfunction. This must indicate clearly whether the current voter’s vote has been cast, discarded, or is waiting to be completed; b. Suspend voting operations until the problem is resolved; c. Allow canceling of the current voter’s electronic CVR by election officials in the case of an unrecoverable error; and d. d. Protect the privacy of the voter while the error is being resolved.
Applies to:	VVPAT
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	A printer error must not cause the voting device to end up in a state where the

	election officials cannot determine whether the ballot was cast or not. This requirement restates and extends [VVSG2005] I.7.9.4-h by requiring that in the event of a printer error, privacy must be maintained to the greatest extent possible, and that voting officials need to be able to cancel the voting session.
Source:	[VVSG2005] I.7.9.4-h
Principle(s)/ Guideline(s):	*Human Factors: Cast As Marked* The voting system ensures that ballot selections, interface options, voter identity and information about voters are kept private. *Security: Ballot Secrecy* Ballot secrecy is maintained throughout the voting process. Records produced by the voting system do not reveal how a voter voted. **Justification:** This requirement aligns with these ballot secrecy guidelines. *Security: Detection and Monitoring* The voting system generates, stores, and reports to the user or election official, all error messages as they occur. **Justification:** A printer error or malfunction is an error message that must be produced for the voter and elections officials by the voting system.

4.4.2.6 Paper-roll VVPAT privacy and audit-support

Paper roll VVPATs may introduce a privacy risk when records are sequentially. However, this risk can be mitigated using a combination of technology and strong election procedures. The following requirements address this threat.

4.4.2.6-A VVPAT, paper-roll, VVPRs secured immediately after vote cast

Requirement:	Paper-roll VVPATs SHALL store the part of the paper roll containing VVPRs in a secure, opaque container, immediately after they are verified.
Applies to:	VVPAT
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Paper rolls containing VVPRs for voters in the order in which they used the voting systems represent a privacy risk. VVPATs that comply with this requirement decrease this risk.
Source:	[VVSG2005] I.7.9.5-d, I.7.9.5-g, I.7.9.4-d
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* Ballot secrecy is maintained throughout the voting process. Records produced by the voting system do not reveal how a voter voted. **Justification:** This requirement aligns with these ballot secrecy guidelines.

	Security: Physical Security The voting system prevents or detects attempts to tamper with voting system hardware. **Justification:** The security principle itself maps to this requirements.

4.4.2.6-B VVPAT, paper-roll, privacy during printer errors

Requirement:	Procedures for recovery from printer errors on paper-roll VVPATs SHALL NOT expose the contents of previously cast VVPRs.
Applies to:	VVPAT
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	Printer errors must not result in the loss of ballot secrecy. This is related to the requirement for immediately storing the VVPRs inside a secure, opaque container.
Source:	VVSG2007
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* Ballot secrecy is maintained throughout the voting process. Records produced by the voting system do not reveal how a voter voted. **Justification:** This requirement aligns with these ballot secrecy guidelines.

4.4.2.6-C VVPAT, paper-roll, support tamper-seals and locks

Requirement:	Paper-roll VVPATs SHALL be designed so that when the rolls are removed from the voting device according to the following: a. All paper containing VVPRs are contained inside the secure, opaque container; b. The container supports being tamper-sealed and locked; and **c.** The container supports being labeled with the device serial number, precinct, and other identifying information to support audits and recounts.
Applies to:	VVPAT
Test Reference:	Part 3:5.2 “Functional Testing”
Discussion:	aper-roll VVPAT must support good procedures to protect the voters’ privacy. The supported procedure in this case is immediately locking and tamper sealing each VVPAT container upon removing it from the voting device. This is consistent with the goal of having the paper rolls with VVPRs on them treated like paper ballots, stored in a locked and sealed box. If the paper roll cartridge is locked and sealed before the start of voting, and some mechanism in the cartridge prevents extraction of the used paper roll collected inside the cartridge, locking and sealing the cartridge a second time at

	poll closing would be necessary only for preventing further VVPRs being printed on the paper roll.
Source:	[VVSG2005] I.7.9.5-g
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* Ballot secrecy is maintained throughout the voting process. Records produced by the voting system do not reveal how a voter voted. **Justification:** This requirement aligns with these ballot secrecy guidelines. Security: *Physical Security* Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence. Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing. **Justification:**

5.4.3-D Secure storage of authentication data

Requirement:	When private or secret authentication data is stored in the voting device, the data SHALL be protected to ensure that the confidentiality and integrity of the data is not violated.
Applies to:	Voting device
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	Ensuring the privacy and secrecy of stored data may involve the use of encryption. This requirement extends [VVSG2005] I.7.2.1.2-g by requiring securely stored private or secret authentication data.
Source:	[VVSG2005] I.7.2.1.2-1
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* Ballot secrecy is maintained throughout the voting process. Records produced by the voting system do not reveal how a voter voted. **Justification:** This requirement aligns with these ballot secrecy guidelines. *Security: Data Protection* The voting system protects sensitive data from unauthorized access,

	modification, or deletion. **Justification:**

5.7.1-C Voter privacy and ballot secrecy requirement

Requirement:	The voting device logs SHALL NOT contain information that, if published, would violate ballot secrecy or voter privacy or that would compromise voting system security in any way.
Applies to:	Programmed device
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”
Discussion:	The device must be constructed so that the security of the system does not rely upon the secrecy of the event logs. It should be considered routine for event logs to be made available to election officials and possibly even to the public, if election officials so desire. The system must be designed to permit the election officials to do so without fear of negative consequences to the security and integrity of the election. For example, cryptographic secret keys or passwords must not be logged in event log records.
Source:	[VVSG2005] I.5.4
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* Ballot secrecy is maintained throughout the voting process. Records, **notifications**, and **other election artifacts** produced by the voting system do not reveal how a voter voted. **Justification:** This requirement aligns with these ballot secrecy guidelines.

7.5.1.2 Secrecy of the ballot

7.5.1.2-A Activation device, ballot secrecy

Requirement:	Voting devices SHALL only make use of locks installed for security purposes that have been evaluated to the listing requirements of UL 437 for door locks and locking cylinders or higher.
Applies to:	Activation device, DRE, EBP
Test Reference:	Part 3:4.5 “Source Code Review”, 5.2 “Functional Testing”, 5.4 “Open-Ended Vulnerability Testing”
Discussion:	Secrecy of the ballot must be preserved during all operations associated with activation of the ballot, including during the creation of the ballot activation credential and information, during the process of activating the ballot, and in all keeping of associated records, reports, and logs. It must not be possible to identify a voter’s ballot or in some way violate secrecy of the ballot by aggregating records from different devices.

	For example, an epollbook cannot retain and associate any information written to a ballot activation token with the voter’s identification information, and a vote-capture device cannot retain information from the token and associate it with the CVR – or else it would be possible to link the sets of records and identify the voter. Note that Requirement Part 1:7.5.1.2-A.3 modifies this requirement if the activation device is used with provisional voting on a DRE.
Source:	VVSG2007
Principle(s)/ Guideline(s):	*Security: Ballot Secrecy* Records, **notifications**, and **other election artifacts** produced by the voting system do not reveal how a voter voted. **Justification:** This requirement aligns with these ballot secrecy guidelines. *Security: Physical Security* The voting system prevents or detects attempts to tamper with voting system hardware. **Justification:** This physical security principle maps to this requirement.

7.5.1.2-A.1 DRE and EBP, open primaries, party selection should be private

Requirement:	In an open primary on a DRE or EBP, the voter SHOULD be allowed to choose a party affiliation in private at the start of the voting session and vote the appropriate ballot configuration (i.e., the choice of affiliation SHOULD be private as well as the selection of votes on the ballot).
Applies to:	DRE ∧ Open primaries device, EBP ∧ Open primaries device
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* Ballot secrecy is maintained throughout the voting process. Records produced by the voting system do not reveal how a voter voted. **Justification:** This requirement aligns with these ballot secrecy guidelines.

7.5.1.2-A.2 Activation device, records preserve secrecy of the ballot

Requirement:	Activation devices SHALL NOT create or retain information that can be used to identify a voter’s ballot, including the order and time at which a voter uses the voting system.
Applies to:	Activation device, DRE, EBP

Test Reference:	Part 3:5.2 “Functional Testing”, 5.4 “Open-Ended Vulnerability Testing
Discussion:	The activation device must not create or retain any information that could be used for the purposes of identifying a voter’s ballot, or the time at which the voter arrived at the polls, or the specific vote-capture device used by the voter.
Source:	VVSG2007
Principle(s)/ Guideline(s):	*Security: Ballot Secrecy* The voting system does not have access to both a voter’s identity and the content of voted ballot selections.

7.5.1.2-A.3 Activation device, ballot activation provisional voting

Requirement:	Credential issuance, only when used during provisional voting, MAY permit the voter’s name to be associated with the voter’s ballot for the purposes of deciding whether to count the ballot. The mechanism used for this association SHALL itself not identify the voter.
Applies to:	Activation device, DRE, EBP
Test Reference:	Part 3:5.2 “Functional Testing”, 5.4 “Open-Ended Vulnerability Testing”
Discussion:	For provisional voting, the voter’s identity is associated with the voter’s ballot so as to permit a subsequent decision whether to count the ballot. As an example, the activation device may create an identifier and associate it with the provisional voter’s identity, and then include this identifier with other information necessary to activate the ballot. The vote-capture device may store this identifier with the ballot so as to trace the ballot back to the voter’s identity for the purposes of deciding whether the count the ballot. The identifier must not itself identify the voter. For example, it must not include the voter’s identity or other information associated with the voter such as an SSN or other identifying information.
Source:	VVSG2007
Principle(s)/ Guideline(s):	*Security: Ballot Secrecy* The voting system does not have access to both a voter’s identity and the content of voted ballot selections.