Ballot Secrecy Requirements Gap Analysis

An overarching goal of the next VVSG is to have each requirement mapped to a principle and its associated guidelines. During the mapping activity for the ballot secrecy requirements, some requirements did not map to the current list of principles and guidelines. Others mapped directly to a principle and not any of the sub-guidelines. New guidelines may be necessary to completely map to all the requirements below.

Possible modifications for the Ballot Secrecy requirements and/or guidelines include:

- As mentioned in the System Event Log Gap Analysis, 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 notifications/warnings do not violate ballot secrecy.

  Requirement(s): 3.2.3.1-A.3, 5.7.1-C, 7.5.1.2-A,

- Add an additional guideline to the Physical Security principle reading as follows:

  The voting system records and other election artifacts should be stored in a secure manner.

  Requirement(s): 4.4.2.6-A, 7.5.1.2-A

- There are some requirements in this section that had no clear mapping:

  Requirement(s): 7.5.1.2-A.2, 7.5.1.2-A.3

Below is a list of ballot secrecy requirements that did not map directly to a principle and/or guideline. If a guideline is listed, NIST found that it did not fully map to the requirement, although partial applicability is noted. It is possible that requirements without an associated guideline may be superfluous and should be deleted. For more information about each requirement, please reference VVSG 2007 at:
http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/2007-VVSG.pdf

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.
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.

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.
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: This mapped to the principle of Physical security. Another guideline may be necessary.**

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.
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.

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 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.
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. *Security: Physical Security* The voting system prevents or detects attempts to tamper with voting system hardware. **Justification:** The locks used are meant to prevent tampering.

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.
Principle(s)/ Guideline(s):	Unknown

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.
Principle(s)/ Guideline(s):	Unknown