Physical Security 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 physical security requirements, it was found that some requirements did not map well to the principles and guidelines.

Possible modifications for the physical security requirements and/or guidelines include:

- An amendment to the first Physical Security guideline to include "***and provides an audible alert***". This would read as follows:

  *Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence **and provides an audible alert**.*

  An alarm may not provide "physical" evidence. This amendment allows the guideline to also cover audible alerts.

  Requirement(s): 5.8.1-B, 5.8.3-B, 5.8.9-B

- There are some requirements which may need discussion from the working group to enhance clarity:

  Requirement(s): 5.8.4-C, 5.8.5-A, 5.8.7-C

- This requirement is unclear and may be a candidate for deletion:

  Requirement(s): 5.8.8-A

For more information about each requirement, please reference VVSG 2007 at: http://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/2007-VVSG.pdf

5.8.1-B Unauthorized physical access capability requirement

Requirement:	Voting devices SHALL produce an audible and visual alarm if access to a restricted voting device component is gained during the Activated state.
Applies to:	Voting device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	
Source:	
Principle(s)/ Guideline(s):	*Security: Physical Security* Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence. **Justification:** This requirement directly aligns with this guideline.

5.8.3-B Physical component alarm requirement

Requirement:	The voting device SHALL produce an audible and visual alarm if a connected component is disconnected during the Activated state.
Applies to:	Voting device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	
Source:	[VVSG2005]
Principle(s)/ Guideline(s):	*Security: Physical Security* Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence. **Justification:** This requirement directly aligns with this guideline.

5.8.4-C Physical port disabling capability requirement

Requirement:	Voting machines SHALL be designed such that physical ports can be manually disabled by an authorized administrator.
Applies to:	Voting device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	
Source:	[VVSG2005]
Principle(s)/ Guideline(s):	*Security: Access Control* The voting system authenticates administrators, users, devices and services before granting access to sensitive functions. ***Justification:*** *Security: Physical Security* Voting systems only expose physical ports and access points that are essential to voting operations, testing, or auditing. **Justification:** This requirement directly aligns with these guidelines.

5.8.5-A Door cover and panel security requirement

Requirement:	Access points such as covers and panels SHALL be secured by locks or tamper evidence or tamper resistance countermeasures SHALL be implemented so that system owners can monitor access to voting device components through these points.
Applies to:	Voting device
Test Reference:	Part 3:4.3 "Verification of Design Requirements"
Discussion:	
Source:	
Principle(s)/ Guideline(s):	*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:** This requirement directly aligns with these guidelines.

5.8.7-C Secure locking system key requirement

Requirement:	Manufacturers SHALL provide locking systems for securing voting devices that can make use of keys that are unique to each owner.
Applies to:	Voting device
Test Reference:	Part 3:Chapter 4: "Documentation and Design Reviews (Inspections)"
Discussion:	Voting device owners are the individuals accountable for purchasing, maintaining and/or operating the voting devices. They may work at the State level or at a local level. Election officials may want keying schemes that are more or less restrictive in accordance with their election management practices. The requirement does not mandate a unique key for each piece of voting equipment, but requires manufacturers to be able to provide unique keys for the voting equipment per the requests of election officials. System owners must establish procedures for issues such as key reproduction, use and storage.
Source:	
Principle(s)/ Guideline(s):	*Security: Physical Security* The voting system prevents or detects attempts to tamper with voting system hardware. **Justification:** This requirement directly aligns with the principle itself.

5.8.8-A Physical encasing lock access requirement

Requirement:	Locks installed for purposes other than security SHALL NOT, if bypassed, compromise the security of a voting device.
Applies to:	Voting device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	Locks on voting devices may be used to secure access points such as doors and panels or they may be used simply to fasten a segment of the voting device's encasement. In the former case, testing labs must verify that the lock does indeed provide a measure of security. In the latter case, the testing lab must verify that bypassing the lock does not put the security of the system in jeopardy.
Source:	
Principle(s)/ Guideline(s):	*Security: Physical Security* The voting system prevents or detects attempts to tamper with voting system hardware. **Justification:** This requirement directly aligns with the principle itself.

5.8.9-B Power outage alarm

Requirement:	A physical security countermeasure that switches from its primary power supply to its back-up power supply SHALL give an audible and visual alarm.
Applies to:	Voting device
Test Reference:	Part 3:5.2 "Functional Testing"
Discussion:	
Source:	
Principle(s)/ Guideline(s):	*General: High Quality Construction*

	Handle errors actively and appropriately, recovering from failure gracefully – processing or avoiding well-known errors and/or software bugs; and avoiding single points of failure that could cause complete loss of voting capabilities. **Justification:** *Security: Physical Security* Any unauthorized physical access to the voting system, ballot box, ballots, or other hardware, leaves physical evidence. **Justification:** This requirement directly aligns with these guidelines.