Principle 12
Physical Security

The voting system prevents or detects attempts to tamper with voting system hardware.

12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.1-A – Unauthorized Physical Access

Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.

[icon] Requirement source Applies to: Voting Device

Discussion

Manufacturer may provide for and recommend a combination of procedures and physical measures that allow election officials to differentiate authorized from unauthorized access during all modes of operation such as a system that relies on tamper evident tape, seals, or tags coded with consecutive serial numbers. Other systems may incorporate seals incorporating radio frequency identification devices with physically unclonable functions or other technology in the future.

This requirement extends [VVSG2005] I.7.3.1 by requiring that any tampering with a device leave physical evidence. [VVSG2005] I.7.3.1 states that any tampering should be detectable, using manufacturer-specified procedures a, using manufacturer-specified procedures and measures.

Status:	Updated
Updated:	Dec. 08, 2017
VVSG 1.1:	<#.#.#.a, #.#.#.b>
Gap notes:	<text>

12.1-B – Unauthorized Physical Access Capability

Voting devices SHALL produce an alarm and leave physical evidence if access to a restricted voting device component is gained during the Activated state.

Comment [FJM(1]: Don't we want an alarm to sound if this occurs in more than just the activated state?

[icon] Requirement source Applies to: Voting Device

Discussion

Status: Updated
Updated: Dec. 08, 2017
VVSG 1.1: <#.#.#.a, #.#.#.b>
Gap notes: <text>

12.1-C – Physical Component Alarm

The voting device SHALL produce an alarm and leave physical evidence if a connected component is disconnected during the Activated state.

[icon] Requirement source Applies to: Voting Device

Discussion

Status: Updated
Updated: Dec. 08, 2017
VVSG 1.1: <#.#.#.a, #.#.#.b>
Gap notes: <text>

12.1-D – Physical Component Event Log

The voting system SHALL log if a voting device or connected component is disconnected during the Activated state.

[icon] Requirement source Applies to: Voting Device

Discussion
A log entry is a type of record.

Status: Updated
Updated: Dec. 08, 2017
VVSG 1.1: <#.#.#.a, #.#.#.b>
Gap notes: <text>

12.1-E – Door Cover and Panel Security

Access points such as covers and panels SHALL be secured by locks or other mechanisms in such a way as to leave physical evidence in case of tampering or unauthorized access.

[icon] Requirement source Applies to: Voting Device

Discussion
The Manufacturer may provide for and recommend a combination of procedures and physical measures that allow election officials to differentiate authorized from unauthorized access during all modes of operation, such as a system that relies on tamper evident tape, seals, or tags coded with consecutive serial numbers. Other systems may incorporate seals incorporating radio frequency identification devices with physically unclonable functions or other technology in the future.

Status:	Updated
Updated:	Dec. 08, 2017
VVSG 1.1:	<#.#.#.a, #.#.#.b>
Gap notes:	<text>

12.1-F – Door Cover and Panel Logging

The voting system SHALL log the status (e.g., open, closed) of physical access points such as covers and panels upon boot.

[icon] Requirement source Applies to: Voting Device

Discussion
This ensures system owners can monitor access to voting device components through these points.

Status:	New
Updated:	Dec. 08, 2017
VVSG 1.1:	<#.#.#.a, #.#.#.b>
Gap notes:	<text>

12.1-G – Secure Ballot Box

Comment [FJM(2]: Seems identical to 12.1-G.1. Suggest deleting one.

Unauthorized physical access to ballot boxes SHALL result in physical evidence that an unauthorized event has taken place.

[icon] Requirement source Applies to: Voting Device

Discussion
The goal is to ensure that poll workers or observers would easily notice if someone has tampered with the ballot box. This requirement can be achieved through locks or seals as a part of tamper evidence and tamper resistance countermeasures described by the use procedures and supplied by the manufacturer.

Status:	Updated
Updated:	Dec. 08, 2017
VVSG 1.1:	<#.#.#.a, #.#.#.b>
Gap notes:	<text>

12.1-G.1 – Secure Container

Unauthorized physical access to a container holding voting system records SHALL result in physical evidence that an unauthorized event has taken place.

[icon] Requirement source Applies to: Voting Device

Discussion

The goal here is to ensure that poll workers or observers would easily notice if someone has tampered with the container. This requirement can be achieved through locks or seals as a part of tamper evidence and tamper resistance countermeasures described by the use procedures and supplied by the manufacturer.

Additionally, to support the auditable principle, containers which hold voting system records, whether paper or electronic, needed for audits need to be secure against physical access.

Status:	New
Updated:	Dec. 08, 2017
VVSG 1.1:	<#.#.#.a, #.#.#.b>
Gap notes:	<text>

12.1-H – Secure Physical Lock Strength

Locks installed in voting devices for security purposes SHALL have been evaluated and meet or exceed requirements of UL 437 for door locks and locking cylinders.

[icon] Requirement source Applies to: Voting Device

Discussion

See [UL03] for UL listing requirements.

Status:	Updated
Updated:	Dec. 08, 2017
VVSG 1.1:	<#.#.#.a, #.#.#.b>
Gap notes:	<text>

12.1-H.1 – Secure Physical Lock Access

Voting devices incorporating locks installed for security purposes SHALL be designed with countermeasures that give a physical indication that unauthorized attempts have been made to defeat the lock and gain access to the voting device.

[icon] Requirement source Applies to: Voting Device

Discussion

Status: Updated
Updated: Dec. 08, 2017
VVSG 1.1: <#.#.#.a, #.#.#.b>
Gap notes: <text>

12.1-H.2 – Secure Locking System Key

Manufacturers SHALL provide locking systems for securing voting devices that are flexible enough to support different keying schemes, including a scheme that can make use of keys that are unique to each owner.

[icon] Requirement source Applies to: Voting Device

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. This system may make use of replicable locks or cylinders, mechanisms which allow for rekeying of locks, or other technologies. 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.

Status: Updated
Updated: Dec. 08, 2017
VVSG 1.1: <#.#.#.a, #.#.#.b>
Gap notes: <text>

12.1-I – Backup Power for Physical Security

Any physical security countermeasure that requires power SHALL have a backup power supply.

[icon] Requirement source Applies to: Voting Device

Discussion

Status: Updated
Updated: Dec. 08, 2017
VVSG 1.1: <#.#.#.a, #.#.#.b>

Gap notes: <text>

12.1-I.1 – Power Outage Alarm

A physical security countermeasure that switches from its primary power supply to its backup power supply SHALL produce an alarm and leave physical evidence.

[icon] Requirement source Applies to: Voting Device

Discussion

Status: Updated
Updated: Dec. 08, 2017
VVSG 1.1: <#.#.#.a, #.#.#.b>
Gap notes: <text>

12.1-I.2 – Power Outage Logging

An event log entry SHALL be generated when a physical security countermeasure switches from its primary power supply to its backup power supply.

[icon] Requirement source Applies to: Voting Device

Discussion

Status: New
Updated: Dec. 08, 2017
VVSG 1.1: <#.#.#.a, #.#.#.b>
Gap notes: <text>

12.1-I.3 – Power Outage Indicator

A physical security countermeasure that switches from its primary power supply to its backup power supply SHALL leave physical evidence of the switch.

[icon] Requirement source Applies to: Voting Device

Discussion

If a physical security countermeasure requires power, and switches to the backup power supply, and then back to the primary supply, a physical indicator should be left since no authorized users of the system are present to hear or see the alarm. There are a variety of technologies that can be used to implement this requirement, such as by heating thermally sensitive tamper evident seals, or having

electromagnets break a tamper evident seal, however they are unlikely to be deployed in current system.

Status: New
Updated: Dec. 08, 2017
VVSG 1.1: <#.#.#.a, #.#.#.b>
Gap notes: <text>

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.

12.2-A – Physical Port and Access Least Functionality

The voting device SHALL only have physical ports and access points that are essential to voting operations, testing and auditing.

[icon] Requirement source Applies to:

Discussion

Examples of ports are USB and RJ45 physical network interfaces. Examples of access points are doors, panels and vents. Voting operations include voting machine upgrades and maintenance.

Status: Updated
Updated: Dec. 08, 2017
VVSG 1.1: <#.#.#.a, #.#.#.b>
Gap notes: <text>

12.2-B - Physical Port Shutdown

If a physical connection between voting device components is broken during Activated or Suspended State, the affected voting machine port SHALL be automatically disabled.

[icon] Requirement source Applies to:

Discussion

Status: Updated
Updated: Dec. 08, 2017
VVSG 1.1: <#.#.#.a, #.#.#.b>
Gap notes: <text>

12.2-C - Physical Port Restriction

Voting systems SHALL restrict physical access to voting machine ports that accommodate removable media, with the exception of ports used to activate a voting session.

[icon] Requirement source Applies to:

Discussion

Removable media (e.g. Floppy, CD or DVD drives, thumb drives, and memory cards) might be essential to voting operations during Pre-voting and Post-voting phases of the voting cycle such as machine upgrade, maintenance and testing. Therefore, all removable media should be accessible only to authorized personnel. They should not be accessible to voters during Activated and Suspended phases of the voting cycle. It is paramount that any removeable drives, whether or not they are used by the system, are not accessed without detection.

The Manufacturer may provide for and recommend a combination of procedures and physical measures that allow election officials to differentiate authorized from unauthorized access during all modes of operation, such as a system that relies on tamper evident tape, seals, or tags coded with consecutive serial numbers. Other systems may incorporate seals incorporating radio frequency identification devices with physically unclonable functions or other technology in the future.

Status:	Updated
Updated:	Dec. 08, 2017
VVSG 1.1:	<#.#.#.a, #.#.#.b>
Gap notes:	<text>
Additional note:	Aligns with 14.2

12.2-D - Physical Port Tamper Evidence

Voting systems SHALL give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.

[icon] Requirement source Applies to:

Discussion

Manufacturer may provide for and recommend a combination of procedures and physical measures that allow election officials to monitor and control access points in such a way as to leave physical evidence in case of tampering or unauthorized access. Such a system might relies on tamper evident tape, seals, or tags coded with consecutive serial numbers. Other systems may incorporate seals incorporating radio frequency identification devices with physically unclonable functions or other technology in the future.

Comment [HGE(3]: Does this belong in 12.1?

Comment [HGE(4]: Reworded. Here is the original:

Voting devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.

Comment [FJM(5R4]: I think your re-wroding is stellar, but I think the whole requirement is duplicative with 12.1-A and 12.1-D.

This requirement extends [VVSG2005] I.7.3.1 by requiring that tampering with device ports or access points leave physical evidence. [VVSG2005] I.7.3.1 states that any tampering should be detectable using manufacturer-specified procedures and measures.

Status:	Updated
Updated:	Dec. 08, 2017
VVSG 1.1:	<#.#.#.a, #.#.#.b>
Gap notes:	<text>

12.2-E - Physical Port Disabling Capability

Voting machines SHALL be designed such that physical ports can be put into a disabled state by an authorized administrator.

[icon] Requirement source Applies to:

Discussion

Status:	Updated
Updated:	Dec. 08, 2017
VVSG 1.1:	<#.#.#.a, #.#.#.b>
Gap notes:	<text>

12.2-F - Physical Port Disabled – Logging Capability

An event log entry that identifies the name of the affected device SHALL be generated when physical ports are enabled or disabled.

[icon] Requirement source Applies to:

Discussion

Status:	New
Updated:	Dec. 08, 2017
VVSG 1.1:	<#.#.#.a, #.#.#.b>
Gap notes:	<text>
Additional note:	Aligns with 9.3