Physical Security Requirements – DRAFT – 20180423

**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 must leave physical evidence that an unauthorized event has taken place.

**Applies to:** Voting Device

**Discussion**

Access points such as covers and panels need to be secured by locks or other mechanisms in such a way as to leave physical evidence in case of tampering or unauthorized access. 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 use 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
**Source:** 2005 VVSG 7.3.1

**Gap notes:**

12.1-B – Unauthorized Physical Access Alarm

Voting devices must produce an alarm if access to a restricted voting device component is detected during the Activated state.

**Applies to:** Voting Device
**Discussion**
This alarm is meant to call attention to election workers in the polling place.

<table>
<thead>
<tr>
<th>Status:</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated:</td>
<td>Dec. 08, 2017</td>
</tr>
<tr>
<td>Source:</td>
<td></td>
</tr>
<tr>
<td>Gap notes:</td>
<td></td>
</tr>
</tbody>
</table>

**12.1-C – Disconnecting a Physical Device**

The voting device must produce an alarm if a connected component is physically disconnected during the Activated state.

** Applies to: Voting Device **

**Discussion**
Examples of connected components include printers, removable storage devices, and mechanisms used for networking. If a token is necessary for normal operation, such as a memory card or other device granting a voter access to the voting system, it is not necessary to trigger the alarm.

<table>
<thead>
<tr>
<th>Status:</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated:</td>
<td>Dec. 08, 2017</td>
</tr>
<tr>
<td>Source:</td>
<td></td>
</tr>
<tr>
<td>Gap notes:</td>
<td></td>
</tr>
</tbody>
</table>

**12.1-D – Logging of Physical Connections & Disconnections**

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

** Applies to: Voting Device **

**Discussion**
Logging of the devices is vital for determining cause and providing incident information if a physical security event occurs.

<table>
<thead>
<tr>
<th>Status:</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated:</td>
<td>Dec. 08, 2017</td>
</tr>
<tr>
<td>Source:</td>
<td></td>
</tr>
<tr>
<td>Gap notes:</td>
<td></td>
</tr>
</tbody>
</table>

**12.1-F – Door Cover and Panel Logging**

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

** Applies to: Voting Device **
Discussion
This ensures system owners can monitor access to voting device components throughout the entire usage of the voting device on election day. The status of the open physical access points may be externally monitored and communicated to the voting device itself.

Status: New
Updated: Dec. 08, 2017
Source: Gap notes:

12.1-G – Secure Container
Unauthorized physical access to a container holding voting system records must result in physical evidence that an unauthorized event has taken place.

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
Source: Gap notes:

12.1-H – Secure Physical Lock Strength
Locks installed in voting devices for security purposes must have been evaluated and meet or exceed requirements of UL 437 for door locks and locking cylinders.

Applies to: Voting Device

Discussion
See [UL03] for UL listing requirements.

Status: Updated
Updated: Dec. 08, 2017
Source: Gap notes:
12.1-H.1 – Secure Physical Lock Access
Voting devices incorporating locks installed for security purposes must 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.

Applies to: Voting Device

Discussion

<table>
<thead>
<tr>
<th>Status</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Updated</td>
</tr>
<tr>
<td></td>
<td>Dec. 08, 2017</td>
</tr>
</tbody>
</table>

12.1-H.2 – Secure Locking System Key
The voting system must support 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.

Applies to: Voting Device

Discussion

The use of a single key used to unlock thousands of precinct-based voting devices makes for a challenging security situation, as copies of this single key design must be distributed to a large number of individuals. This does create a situation in which the key may be easily lost or stolen, and subsequently copied. This situation does make key management significantly easier for election officials. To alleviate this situation, election officials may want keying schemes that are more or less restrictive in accordance with their election management practices and needs. 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.

<table>
<thead>
<tr>
<th>Status</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Updated</td>
</tr>
<tr>
<td></td>
<td>Dec. 08, 2017</td>
</tr>
</tbody>
</table>

12.1-I – Backup Power for Power-Reliant Countermeasures
Any physical security countermeasure that requires power must have a backup power supply.
Applies to: Voting Device, EMS

Discussion
This ensures that the countermeasure isn’t disabled or intentionally circumvented by a power failure.

Status: Updated
Updated: Dec. 08, 2017
Source: VVSG 2007 5.8.9-A
Gap notes:

12.1-I.1 – Power Outage Alarm
A physical security countermeasure that switches from its primary power supply to its backup power supply must produce an alarm.

Applies to: Voting Device, EMS

Discussion
An alarm alerts an election worker to the issue so that any problem can be further diagnosed and eventually resolved.

Status: Updated
Updated: Dec. 08, 2017
Source: VVSG 2007 5.8.9-B
Gap notes:

12.1-I.2 – Power Outage Logging
An event log entry must be generated when a physical security countermeasure switches from its primary power supply to its backup power supply.

Applies to: Voting Device, EMS

Discussion
This information is security relevant, especially once a security incident has occurred, and would be useful when determining cause.

Status: New
Updated: Dec. 08, 2017
Source:
Gap notes:
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 must only have physical ports and access points that are essential to voting operations, testing and auditing.

Applies to: Voting Device

**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
- Source: VVSG 2007 5.6.3-C

12.2 – B - Physical Port Auto-Disable
If a physical connection between voting device components is broken during Activated or Suspended State, the affected voting machine port must be automatically disabled.

Applies to: Voting Device

**Discussion**
Automatically disabling will require an election worker’s attention to re-enable and re-attach any network or power cabling. Under ideal circumstances, the specific election worker performing maintenance is uniquely identified within the logs, but this is not required.

- Status: Updated
- Updated: Dec. 08, 2017
- Source: 
- Gap notes:

12.2-C - Physical Port Restriction
Voting systems must restrict physical access to voting machine ports that accommodate removable media, with the exception of ports used to activate a voting session.

Applies to: Voting Device

**Discussion**
Although voting systems may have ports dedicated to voting operations outside of election day activities, those ports need not be exposed while balloting is in progress. 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 essential that any removable drives, whether or not they are used by the system, are not accessed without detection.

Status: Updated
Updated: Dec. 08, 2017
Source: Gap notes: Aligns with 14.2

12.2-E – Capability to Disable Ports
Voting machines must be designed such that physical ports can be put into a disabled state by an authorized administrator.

Applies to: Voting Device, EMS

Discussion
Logically disabling ports prevents unused ports from being used as a staging point for an attack on the voting system.

Status: Updated
Updated: Dec. 08, 2017
Source: Gap notes: System integrity – Attack Surface Reduction

12.2-E.1 – Logging of Disabled Ports
An event log entry that identifies the name of the affected device must be generated when physical ports are enabled or disabled.

Applies to: Voting Device, EMS

Discussion
If a port is disabled or not is security relevant, especially once a security incident has occurred, and this information would be useful when determining cause. 12.2-D discusses physical restrictions, whereas 12.2-E.1 discusses logical disabling of ports.

Status: New
Updated: Dec. 08, 2017
Source: Gap notes: Aligns with 9.3, Access Control