MP.L2-3.8.7

Media Protection

Removable Media

"Control the use of removable media on system components."

Objectives

[a]
The use of removable media on system components is controlled.

Key Discussion Points

Policy + Technical:
Technical controls — disabling USB ports, device whitelists — are more reliable than policy alone. Policy without enforcement is incomplete.

Limit to Minimum:
The guide says to limit removable media to the smallest number needed — reduce the attack surface by restricting types and quantity.

Scan Before Use:
All removable media should be scanned for malware before use on CUI systems — infected drives are a primary malware introduction vector.

Differs from 3.8.1:
3.8.1 restricts who can access media. 3.8.7 restricts what media can be used on systems — different control, different requirement.

Assessment Methods

EXAMINE

System media protection policy; system use policy; procedures addressing media usage restrictions; system security plan; rules of behavior; system design documentation; system configuration settings; system audit logs.

INTERVIEW

Personnel with system media use responsibilities; personnel with information security responsibilities; system or network administrators.

TEST

Organizational processes for media use; mechanisms restricting or prohibiting use of system media on systems or system components.

MP.L2-3.8.7

MEDIA PROTECTION — Removable Media

Plain English

What this control is really saying:

An employee plugs in a personal USB drive, copies CUI files, and takes them home. That is an uncontrolled CUI exfiltration event. This control requires a policy on removable media use — what is permitted, by whom, and under what conditions — and technical controls to enforce it.

How it is used:

- Group Policy disables USB storage ports on all CUI workstations — only IT-issued, organization-approved drives can be used via a device whitelist.
- Removable media policy defines: only organization-issued drives permitted, for work purposes only, scanned before each use on a dedicated AV workstation.
- CD/DVD drives are disabled on all CUI systems via BIOS configuration — no exceptions without written IT approval and a documented business justification.
- The removable media policy is included in the acceptable use policy and reviewed with all employees annually.

Real World Example

The Scenario

Acme Defense has no removable media policy. An engineer uses his personal USB drive to take work files home. The drive is also used on his home computer, which has malware. The next morning he plugs the drive into his CUI workstation.

What the assessor finds

The malware spreads from the personal USB drive to the CUI workstation and begins harvesting files. USB ports are not blocked, personal drives are not prohibited, and no scan was performed. There is no removable media policy and no technical control to detect or prevent the incident.

SPRS Score Impact

3.8.7 carries a point value of 1. Uncontrolled removable media is the most common vector for both CUI exfiltration and malware introduction in DIB environments — a single personal USB drive can do both.

What Good Looks Like

Written removable media policy, only organization-issued drives permitted on CUI systems, USB ports technically restricted via Group Policy or device whitelist, all media scanned before use, removable media controls documented in SSP.

Common Gaps

What assessors actually find in the field:

✗ **No removable media policy**

Any employee can plug in any USB drive — there is no policy or technical control governing removable media use.

✗ **Personal drives permitted**

Employees use personal USB drives on CUI systems — personally owned media is an uncontrolled exfiltration and infection vector.

✗ **Policy but no enforcement**

A policy prohibits personal USB drives but USB ports are not disabled — users ignore the policy with no technical consequence.

✗ **No scanning requirement**

Removable media is used on CUI systems without being scanned for malware — infected drives can introduce malicious code.

✗ **All media types unrestricted**

CD/DVD, USB, and external hard drives are all permitted without restriction — no limit to smallest number needed.