MP.L2-3.8.1

Media Protection

Media Protection

"Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital."

Objectives

[a]
Paper media containing CUI is physically controlled.

[b]
Digital media containing CUI is physically controlled.

[c]
Paper media containing CUI is securely stored.

[d]
Digital media containing CUI is securely stored.

Key Discussion Points

Both Types Required:
Paper AND digital — both must be physically controlled and securely stored. Organizations often address digital but neglect paper CUI.

Secure Storage:
Locked drawer, locked cabinet, or controlled media library — unsecured CUI media left on a desk or in an unlocked drawer is a direct finding.

Inventory Required:
Physical control includes maintaining accountability — an inventory of CUI media with known custodians is part of this control.

Checkout Process:
Procedures for checking media in and out create an accountability trail — who has it, when they took it, and when it was returned.

Assessment Methods

EXAMINE

System media protection policy; procedures addressing media storage; procedures addressing media access restrictions; access control policy and procedures; physical and environmental protection policy; system security plan; media storage facilities; access control records.

INTERVIEW

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

TEST

Organizational processes for restricting information media; mechanisms supporting or implementing media access restrictions.

MP.L2-3.8.1

MEDIA PROTECTION — Media Protection

Plain English

What this control is really saying:

A USB drive with CUI designs sitting on an unattended desk is a breach waiting to happen. This control requires that both paper and digital media containing CUI are physically controlled — locked away, inventoried, with a checkout process — and that only authorized people can access them.

How it is used:

- USB drives and external hard drives containing CUI are stored in a locked cabinet — only the project lead and designated team members have the key.
- Paper CUI documents are stored in a locked drawer when not in use — a checkout log tracks who accessed which document and when.
- A media inventory is maintained listing all removable media containing CUI — each item is logged with a unique identifier and last-known custodian.
- Digital media is labeled to identify CUI content and classified separately from non-CUI media — unlabeled media is not permitted in the CUI environment.

Real World Example

The Scenario

Acme Defense stores CUI design files on USB drives. The drives are kept in an unlocked drawer in the engineering office. No inventory exists. Engineers take drives home when working remotely without logging the checkout.

What the assessor finds

Three USB drives are unaccounted for — nobody knows if they contain CUI or where they are. One engineer took a drive home six weeks ago and has not returned it. There is no inventory, no checkout log, and no locked storage for any removable media.

SPRS Score Impact

3.8.1 carries a point value of 1. Physical media loss is one of the most commonly reported CUI spill vectors — a single untracked USB drive with CUI designs can constitute a reportable breach under DFARS 252.204-7012.

What Good Looks Like

All CUI media inventoried with unique IDs, stored in locked secure location, checkout log maintained, only authorized personnel have access, paper CUI secured when not in use, media labeled to identify CUI content.

Common Gaps

What assessors actually find in the field:

✗ **USB drives left uncontrolled**

CUI-containing USB drives are kept in an unlocked desk drawer accessible to anyone in the office.

✗ **No media inventory**

Nobody knows how many removable media items contain CUI or where they are — no inventory has ever been conducted.

✗ **Paper CUI unsecured**

Printed CUI documents are left on desks overnight — no clean-desk policy or locked storage requirement exists.

✗ **No checkout process**

Media can be taken out of the office without logging — there is no record of who took what or when it was returned.

✗ **Media accessible to all staff**

CUI media is stored in an unlocked cabinet in a common area — all employees and visitors can access it without restriction.