MP.L2-3.8.5

Media Protection

Media Accountability

"Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas."

Objectives

[a]

Access to media containing CUI is controlled.

[b]

Accountability for media containing CUI is maintained during transport outside of controlled areas.

Key Discussion Points

Two Parts:
Access control ([a]) applies inside the facility. Accountability ([b]) applies during transport — both must be addressed.

Encryption for Transit:
Encrypting CUI before transport ensures that a lost or stolen drive cannot be read — this is a primary mechanism for transport accountability.

Track Movement:
Maintaining accountability means knowing where the media is at all times — tracking numbers, chain of custody, and delivery confirmation.

Authorized Transport:
Only authorized personnel should transport CUI media — a courier or shipping service must be vetted and the transfer documented.

Assessment Methods

EXAMINE

System media protection policy; procedures addressing media storage; physical and environmental protection policy; access control policy and procedures; system security plan; system media; designated controlled areas.

INTERVIEW

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

TEST

Organizational processes for storing media; mechanisms supporting or implementing media storage and media protection.

MP.L2-3.8.5

MEDIA PROTECTION — Media Accountability

Plain English

What this control is really saying:

This control has two parts: controlling who can access CUI media inside your facility, and tracking it when it leaves. A USB drive in a briefcase on a plane needs accountability — tamper-evident packaging, tracking numbers, encryption, and a record of who authorized the transport.

How it is used:

- Physical access to CUI media storage is restricted to authorized personnel — the storage location is locked and access is logged.
- When CUI media must be shipped, it is placed in tamper-evident packaging with a tracking number and shipped via a carrier with delivery confirmation.
- CUI on portable media is encrypted before transport — if the drive is lost in transit, the data cannot be accessed without the decryption key.
- A transport authorization form is completed before CUI media leaves the facility — identifying the media, destination, carrier, and authorizing official.

Real World Example

The Scenario

An Acme Defense engineer carries a USB drive with CUI design files to a customer meeting. He puts the drive in his laptop bag. The bag is stolen from his rental car at the airport. The drive is unencrypted and has no transport authorization.

What the assessor finds

The drive contains unencrypted CUI design drawings. There is no transport authorization form, no tracking record, and no encryption. The breach is discovered only when the engineer reports the stolen bag the next day. A DFARS cyber incident report is required.

SPRS Score Impact

3.8.5 carries a point value of 1. CUI media in transit without encryption or tracking is among the most commonly reported breach vectors — physical loss of unprotected media is a reportable incident under DFARS 252.204-7012.

What Good Looks Like

Access to CUI media controlled and logged, transport authorization required before media leaves facility, CUI encrypted before transport, tamper-evident packaging and tracking for shipped media, transport records retained, delivery confirmation obtained.

Common Gaps

What assessors actually find in the field:

✗ **No transport procedure**

CUI media is shipped without documentation — no authorization form, no tracking, no confirmation of delivery.

✗ **Unencrypted media in transit**

USB drives with CUI are transported in briefcases or checked luggage without encryption — a single lost bag exposes CUI.

✗ **No access control on storage**

CUI media storage is accessible to all employees — no restriction on who can retrieve or handle it.

✗ **Third-party couriers unvetted**

Media is handed to couriers without verifying authorization — the transport chain is uncontrolled after it leaves the building.

✗ **No tracking records**

Media that leaves the facility is not tracked — there is no record of what was sent, when, or whether it arrived.