MP.L2-3.8.6

Media Protection

Portable Storage Encryption

"Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards."

Objectives

[a]

The confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.

Key Discussion Points

Encrypt or Safeguard:
Cryptographic protection is the default — alternative physical safeguards only apply when encryption is technically not feasible.

Portable Media Types:
USB drives, external hard drives, backup tapes, CDs, and DVDs — all portable digital media carrying CUI must be covered.

Must Be FIPS-Validated:
The cryptography used must meet SC.L2-3.13.11 — FIPS 140-2 validated modules are required for CUI confidentiality protection.

Extends 3.8.5:
3.8.5 handles access control and accountability; 3.8.6 adds encryption — encryption protects against scenarios where access control fails.

Assessment Methods

EXAMINE

System media protection policy; procedures addressing media transport; system design documentation; system security plan; system configuration settings; system media transport records; system audit logs.

INTERVIEW

Personnel with system media transport responsibilities; personnel with information security responsibilities.

TEST

Cryptographic mechanisms protecting information on digital media during transportation outside controlled areas.

MP.L2-3.8.6

MEDIA PROTECTION — Portable Storage Encryption

Plain English

What this control is really saying:

3.8.5 requires accountability when CUI media is transported. 3.8.6 says: encrypt it too. If the drive is lost, stolen, or intercepted, encryption makes the data unreadable without the key. This applies to USB drives, backup tapes, external hard drives, CDs — any portable digital media carrying CUI.

How it is used:

- All USB drives used to transport CUI use hardware encryption — drives without encryption are not permitted to carry CUI outside the facility.
- Backup tapes sent offsite are encrypted using the backup software's built-in encryption feature — unencrypted tapes are not sent to the offsite vendor.
- The SSP documents the encryption standard used (FIPS 140-2 validated), the key management process, and the media types covered.
- When encryption is not technically feasible, alternative physical safeguards (e.g., locked tamper-evident container with courier receipt) are used and documented.

Real World Example

The Scenario

Acme Defense sends monthly backup tapes to an offsite storage vendor for disaster recovery. The backup software has an encryption option that was never enabled. A tape containing a full backup of the CUI project file server is lost by the courier.

What the assessor finds

The lost tape contains unencrypted CUI — full project design files, contract documentation, and personnel data. The tape can be read by anyone with a compatible tape drive. There is no encryption, no policy requiring encryption, and no alternative physical safeguard procedure.

SPRS Score Impact

3.8.6 carries a point value of 3. Unencrypted portable media is one of the simplest CUI exposure events — encryption is the primary technical safeguard that renders a lost or stolen drive harmless.

What Good Looks Like

All CUI portable media encrypted with FIPS 140-2 validated cryptography, backup tapes encrypted before offsite transport, alternative physical safeguards documented when encryption not feasible, encryption standard and key management in SSP.

Common Gaps

What assessors actually find in the field:

✗ **USB drives not encrypted**

Standard USB drives are used to transport CUI — if one is lost, the data is immediately readable by anyone who finds it.

✗ **Backup tapes unencrypted**

Backup tapes sent to an offsite vendor are not encrypted — the vendor and any third party handling the tapes can read CUI.

✗ **Non-FIPS cryptography used**

Media is encrypted but with a non-FIPS 140-2 validated algorithm — SC.L2-3.13.11 requires FIPS-validated cryptography for CUI.

✗ **Physical safeguards not defined**

Encryption is unavailable for some legacy media types but no alternative physical safeguard procedure is documented.

✗ **Encryption not enforced**

Policy requires encryption but nothing technically prevents employees from copying CUI to a standard unencrypted USB drive.