SC.L2-3.13.16

System & Communications Protection

Data at Rest

"Protect the confidentiality of CUI at rest."

Objectives

[a]
The confidentiality of CUI at rest is protected.

Key Discussion Points

Encryption Not Mandatory: The guide explicitly states encryption is one approach but not required — physical controls, access restrictions, and secure offline storage also satisfy this control.

All Storage Locations: CUI at rest includes workstations, laptops, servers, USB drives, mobile devices, and cloud storage — any storage location containing CUI must be addressed.

FIPS Required If Crypto: If cryptography is used for CUI at rest protection, it must be FIPS-validated per SC.L2-3.13.11 — unvalidated encryption does not satisfy the cryptographic path.

Inventory First: Protection cannot be verified without knowing where CUI lives — a CUI data inventory identifying all at-rest storage locations is a prerequisite for this control.

Assessment Methods

EXAMINE

System and communications protection policy; procedures addressing protection of information at rest; system security plan; system design documentation; list of information at rest requiring confidentiality protections; system configuration settings; cryptographic mechanisms and configuration documentation.

INTERVIEW

System or network administrators; personnel with information security responsibilities; system developer.

TEST

Mechanisms supporting or implementing confidentiality protections for information at rest.

SC.L2-3.13.16

SYSTEM & COMMS PROTECTION — Data at Rest

Plain English

What this control is really saying:

CUI stored on a workstation, a file server, a laptop, or a USB drive is at risk if the device is lost, stolen, or accessed by an unauthorized person. This control requires that stored CUI be protected — most commonly through full-disk encryption, but also through physical controls, access restrictions, and secure offline storage when encryption is not feasible.

How it is used:

- Full-disk encryption using BitLocker (FIPS mode) is deployed on all CUI workstations and laptops — any device that might leave the facility or be accessed by unauthorized personnel is covered.
- The CUI file server uses access controls to restrict who can read files, and the OS volume is encrypted — access logs record who accessed which files.
- Devices that cannot support encryption are subject to physical controls — locked cabinet, sign-out log, and end-of-day return audit.
- The SSP documents the encryption method used, the CMVP certificate number, and any devices protected by alternative physical controls instead of encryption.

Real World Example

The Scenario

Acme Defense deploys BitLocker on company laptops but uses it in standard mode, not FIPS mode. The recovery keys are saved to a shared folder on the file server accessible to all employees. Three engineers have CUI files on personal laptops used for remote work — no encryption.

What the assessor finds

An assessor verifies BitLocker is not in FIPS mode and notes the recovery keys are accessible to all users. A review of the three unencrypted personal laptops reveals CUI design files in local Downloads folders. No physical controls govern those devices.

SPRS Score Impact

3.13.16 carries a point value of 5. CUI at rest is the largest storage risk for most DIB contractors — a single stolen or lost unencrypted device can constitute a reportable breach under DFARS 252.204-7012.

What Good Looks Like

CUI at rest inventoried across all storage locations, FIPS-validated full-disk encryption on all laptops and workstations, recovery keys protected, alternative physical controls documented for devices that cannot be encrypted, encryption methods documented in SSP with CMVP references.

Common Gaps

What assessors actually find in the field:

✗ Laptops not encrypted

CUI workstations and laptops have no disk encryption — a lost or stolen laptop immediately exposes all CUI stored on it.

✗ Encryption not FIPS-validated

Full-disk encryption is in use but with a non-FIPS-validated module — SC.L2-3.13.11 requires FIPS-validated cryptography for CUI protection.

✗ File server CUI unprotected

CUI on the file server relies on access controls alone — no encryption exists, so a compromised admin account exposes all CUI files.

✗ Recovery keys exposed

BitLocker is deployed but recovery keys are stored in an unprotected spreadsheet accessible to all staff — the encryption is only as strong as key protection.

✗ Not inventoried

The organization cannot identify all locations where CUI is stored at rest — CUI may exist on workstations, personal devices, and cloud storage without controls.