AC.L2-3.1.19

Access Control

Encrypt CUI on Mobile

"Encrypt CUI on mobile devices and mobile computing platforms."

Objectives

[a]

Mobile devices and mobile computing platforms that process, store, or transmit CUI are identified.

[b]

Encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.

Key Discussion Points

FIPS-Validated Module: v2.13 references SC.L2-3.13.11 — BitLocker in standard mode is not sufficient. FIPS mode must be enabled, and the module's CMVP certificate number must be documented in the SSP.

Verify, Don't Assume: Encryption being 'on by default' or 'set up at imaging' does not satisfy [b] — compliance must be actively verified through MDM reporting on a defined schedule.

Full-Disk vs. Container: v2.13 explicitly permits both full-device encryption and container-based encryption — container encryption is more granular but must protect all CUI data paths on the device.

Data at Rest Scope: This control covers CUI at rest on the device — 3.1.13 covers CUI in transit during remote sessions. Both must be met for CUI to be protected through its full lifecycle on mobile platforms.

Assessment Methods

EXAMINE

Access control policy; procedures addressing access control for mobile devices; system design documentation; system configuration settings; encryption mechanisms and associated configuration documentation; system security plan; system audit logs and records.

INTERVIEW

Personnel with access control responsibilities for mobile devices; system or network administrators; personnel with information security responsibilities.

TEST

Encryption mechanisms protecting confidentiality of information on mobile devices.

AC.L2-3.1.19

ACCESS CONTROL — Encrypt CUI on Mobile

Plain English

What this control is really saying:

A laptop containing CUI that gets left on a plane is not a breach — if it is encrypted. This control is what turns a lost or stolen device from a reportable incident into a non-event. v2.13 requires FIPS-validated encryption, so BitLocker in FIPS mode for Windows laptops and MDM-enforced encryption verification for mobile devices. Encryption being 'on by default' is not enough — it must be actively verified.

How it is used:

- BitLocker full-disk encryption is enabled on all company laptops via Group Policy with FIPS mode enforced — the CMVP certificate number for the BitLocker module is documented in the SSP.
- Intune MDM enforces an encryption compliance policy on all enrolled mobile devices — devices that do not report encryption as enabled are automatically blocked from corporate resources.
- Encryption status is verified monthly through MDM compliance reports — non-compliant devices are flagged and remediated within 48 hours.
- The lost or stolen device procedure requires immediate remote wipe — the procedure is tested quarterly and documented in the SSP.

Real World Example

The Scenario

Acme Defense issued laptops to all engineers running Windows 11. BitLocker was not configured during imaging because IT was unaware of the CMMC requirement. Engineers also have company iPhones enrolled in Intune, but the MDM compliance policy does not enforce encryption verification.

What the assessor finds

None of the five company laptops have BitLocker enabled — the drives are completely unencrypted. One laptop was reported lost at a conference six months ago and contained CUI engineering drawings. No remote wipe was performed. The iPhone MDM policy does not require or verify device encryption.

SPRS Score Impact

3.1.1 carries a point value of 1. An acceptable use policy without monitoring is unenforceable — and monitoring without a defined authorized use baseline cannot reliably distinguish authorized from unauthorized activity.

What Good Looks Like

Mobile devices accessing CUI identified and inventoried, BitLocker in FIPS mode on all company laptops verified via MDM, MDM policy enforces encryption on all mobile devices, compliance verified monthly, lost or stolen device protocol includes immediate remote wipe, CMVP certificate documented in SSP.

Common Gaps

What assessors actually find in the field:

✗ **No BitLocker on laptops**

Company laptops have no disk encryption configured — a lost or stolen laptop immediately exposes all local CUI to whoever finds it.

✗ **BitLocker not in FIPS mode**

BitLocker is enabled but not configured for FIPS mode — the encryption is present but does not meet the SC.L2-3.13.11 FIPS-validated module requirement.

✗ **Encryption not verified**

IT believes encryption is enabled because it was set up during imaging, but compliance has never been verified — devices may have had encryption disabled without detection.

✗ **Personal devices not encrypted**

Employees access CUI on personal phones and tablets with no MDM policy enforcing encryption — the encryption status of these devices is unknown.

✗ **Lost device not wiped**

A laptop reported lost at a conference six months ago contained CUI files — no remote wipe was performed and the device had no encryption.