SC.L2-3.13.11

System & Communications Protection

CUI Encryption

"Employ FIPS-validated cryptography when used to protect the confidentiality of CUI."

Objectives

[a]
FIPS-validated cryptography is employed to protect the confidentiality of CUI.

Assessment Methods

EXAMINE

System and communications protection policy; procedures addressing cryptographic protection; system security plan; system design documentation; system configuration settings; cryptographic module validation certificates; list of FIPS-validated cryptographic modules; system audit logs.

INTERVIEW

System or network administrators; personnel with information security responsibilities; system developers; personnel with responsibilities for cryptographic protection.

TEST

Mechanisms supporting or implementing cryptographic protection.

Key Discussion Points

Module, Not Algorithm:
FIPS-validated means the module (software or hardware) is validated by NIST CMVP — using an approved algorithm in an unvalidated module is not sufficient.

CMVP Certificate:
The NIST Cryptographic Module Validation Program database is the authoritative source — assessors will search for the specific module and version being used.

Where It Applies:
FIPS-validated crypto is required when CUI is transmitted or stored OUTSIDE the protected environment — internal use within a secured enclave has more flexibility.

Ties to Other Controls:
SC.L2-3.13.11 is referenced by AC.L2-3.1.19, MP.L2-3.8.6, SC.L2-3.13.8, and SC.L2-3.13.16 — it is the cryptographic standard that underlies all CUI encryption requirements.

SC.L2-3.13.11

SYSTEM & COMMS PROTECTION — CUI Encryption

Plain English

What this control is really saying:

Using encryption is not enough — the encryption must meet a specific standard. AES-256 is a strong algorithm, but if the software implementing it has not been tested and validated by NIST under the FIPS 140 program, it does not meet this requirement. The NIST Cryptographic Module Validation Program (CMVP) validates the specific module, not just the algorithm.

How it is used:

- Full-disk encryption uses BitLocker in FIPS mode or a CMVP-validated third-party product — the NIST CMVP certificate number is documented in the SSP.
- VPN connections use a FIPS-validated cryptographic module — the module validation certificate number and version are verified annually via the NIST CMVP website.
- The SSP documents each cryptographic use case, the product/module used, and its CMVP validation certificate number — this is the primary evidence for [a].
- The Windows 'FIPS-compliant algorithms' group policy setting is enabled — this forces FIPS-validated mode for OS-level encryption operations.

Real World Example

The Scenario

Acme Defense uses 7-Zip with AES-256 to encrypt CUI files before emailing them. The IT admin believes AES-256 is FIPS-compliant. He has not checked whether the specific version of 7-Zip he is using has a CMVP validation certificate.

What the assessor finds

The assessor searches the NIST CMVP database — the version of 7-Zip in use does not appear in the validated modules list. AES-256 is being used but with an unvalidated module. The SPRS score claimed SC.L2-3.13.11 as fully implemented.

SPRS Score Impact

3.13.11 carries a point value of 5. Using unvalidated cryptography while claiming FIPS compliance on the SPRS score is a potential False Claims Act exposure — the distinction between 'AES-256' and 'FIPS-validated AES-256' is legally significant.

What Good Looks Like

FIPS-validated modules used for all CUI encryption, CMVP certificate numbers documented in SSP for each cryptographic use case, validation status verified annually, Windows FIPS policy enabled where applicable, non-FIPS tools prohibited for CUI protection.

Common Gaps

What assessors actually find in the field:

✗ Non-FIPS module in use

BitLocker is enabled but not in FIPS mode — or a third-party tool is used that has not been CMVP-validated.

✗ Algorithm known, module unknown

The organization knows AES-256 is in use but cannot identify the specific module or locate a CMVP validation certificate.

✗ Open-source crypto, unvalidated

An open-source library implements encryption — the algorithm is strong but the library has not been submitted for FIPS 140 validation.

✗ FIPS validation expired

The cryptographic module was validated but the certificate has since expired — ongoing FIPS compliance requires current validation status.

✗ Not documented in SSP

FIPS-validated encryption is in use but the module, certificate number, and use case are not documented in the SSP — assessors cannot verify [a].