AC.L2-3.1.13

Access Control

Remote Access Confidentiality

"Employ cryptographic mechanisms to protect the confidentiality of remote access sessions."

Objectives

[a]

Cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.

[b]

Cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.

Key Discussion Points

FIPS-Validated Required: v2.13 explicitly requires FIPS-validated cryptography by reference to SC.L2-3.13.11 — a VPN using strong algorithms with unvalidated modules does not satisfy this control.

All Remote Methods: VPN, RDP, SSH, and HTTPS must all use FIPS-approved cryptography — one unencrypted or weakly encrypted access method fails [b] regardless of other protections.

Identify the Mechanism: [a] requires identifying the specific cryptographic mechanisms — product name, algorithm, and CMVP certificate number documented in the SSP are evidence for [a].

Telnet and HTTP Are Never Acceptable: Telnet and unencrypted HTTP transmit session data in plaintext — both must be disabled on all systems that store, process, or provide access to CUI.

Assessment Methods

EXAMINE

Access control policy; procedures addressing remote access to the system; system security plan; system design documentation; system configuration settings; cryptographic mechanisms and associated configuration documentation; system audit logs and records.

INTERVIEW

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

TEST

Cryptographic mechanisms protecting remote access sessions.

AC.L2-3.1.13

ACCESS CONTROL — Remote Access Confidentiality

Plain English

What this control is really saying:

Any remote access session carrying CUI must be encrypted. This is not just about having a VPN — it is about what encryption that VPN uses. v2.13 explicitly ties this control to SC.L2-3.13.11, which requires FIPS-validated cryptography for CUI protection. A VPN using weak or unvalidated algorithms does not satisfy this control.

How it is used:

- Cisco AnyConnect VPN is configured with AES-256-GCM encryption using a FIPS 140-2 validated module — the CMVP certificate number is documented in the SSP.
- RDP connections are encrypted using TLS with the RDP Security Layer disabled — only Network Level Authentication with TLS is permitted.
- Web portals serving CUI require HTTPS with TLS 1.2 or higher — TLS 1.0 and 1.1 are disabled, HTTP is redirected to HTTPS.
- SSH is used for all server management in place of Telnet — SSH version 2 with FIPS-approved cipher suites only.

Real World Example

The Scenario

Acme Defense uses Cisco AnyConnect for VPN and a web portal for contractor collaboration. Several legacy network switches and a CNC machine controller are managed remotely by the IT admin.

What the assessor finds

The web portal serves both HTTP and HTTPS with no redirect — CUI documents are accessible over unencrypted HTTP. Legacy network switches are managed via Telnet. The CNC machine uses a proprietary protocol with no encryption. VPN cipher suites have not been reviewed since 2018. No CMVP certificate number is documented anywhere.

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

Cryptographic mechanisms identified in SSP with CMVP certificate numbers, VPN using FIPS-validated module with AES-256, HTTPS-only for all web portals with TLS 1.2 minimum, Telnet disabled and replaced with SSH v2, weak cipher suites disabled across all remote access methods.

Common Gaps

What assessors actually find in the field:

✗ **VPN using weak cipher suites**

VPN is configured but using DES, 3DES, or RC4 — these are not FIPS-approved algorithms and do not satisfy the FIPS-validated cryptography requirement.

✗ **HTTP access to CUI portals**

Web portals serving CUI accept HTTP connections — session data and CUI transit in plaintext readable by anyone on the network path.

✗ **Telnet still in use**

Legacy network devices and servers are managed via Telnet — all commands, credentials, and CUI data transmitted during sessions are in cleartext.

✗ **TLS 1.0 and 1.1 enabled**

Web servers and VPN concentrators accept TLS 1.0 and 1.1 — both have known vulnerabilities allowing session decryption attacks.

✗ **Cryptography not documented**

Encryption is in use but the specific modules, certificate numbers, and algorithm configurations are not documented in the SSP — [a] is not met.