SC.L2-3.13.8

System & Communications Protection

Data in Transit

"Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards."

Objectives

[a]
Cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified.

[b]
Alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified.

[c]
Either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.

Key Discussion Points

Identify Then Implement:
[a] and [b] require identifying what you will use — the cryptographic mechanism or physical safeguard must be documented before [c] can be assessed.

Internal Too:
This applies to internal and external networks — CUI sent between servers inside the facility also requires encryption unless on a protected distribution system.

FIPS Required:
This control links to SC.L2-3.13.11 — the cryptographic algorithms used for CUI transmission must be FIPS 140-2 validated, not just any encryption.

TLS Minimum:
TLS 1.2 or higher is the practical baseline — weak cipher suites must be disabled even on servers that support TLS, as they can allow downgrade attacks.

Assessment Methods

EXAMINE

System and communications protection policy; procedures addressing transmission confidentiality; system security plan; system design documentation; system configuration settings; system audit logs.

INTERVIEW

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

TEST

Cryptographic mechanisms or mechanisms supporting transmission confidentiality; organizational processes for defining and implementing alternative physical safeguards.

SC.L2-3.13.8

SYSTEM & COMMS PROTECTION — Data in Transit

Plain English

What this control is really saying:

Any CUI sent over a network can be intercepted if the connection is not encrypted. This control requires encryption in transit — TLS for web traffic and email, SFTP or encrypted VPN for file transfers, and FIPS 140-2 validated cryptography for all of it. The only exception is when a physical safeguard like a protected distribution system makes interception physically impossible.

How it is used:

- All CUI transmitted over the internet uses TLS 1.2 or higher — file sharing uses SFTP or HTTPS, not FTP or plain HTTP.
- Email containing CUI is sent via TLS-enforced SMTP connections — the mail server is configured to reject non-TLS connections and logs when TLS cannot be negotiated.
- VPN connections use FIPS 140-2 validated cryptographic modules — the NIST CMVP validation certificate number is documented in the SSP.
- Web applications that handle CUI are configured to enforce HTTPS — HTTP is redirected to HTTPS and HSTS is enabled.

Real World Example

The Scenario

Acme Defense project managers email CUI design files to the DoD contracting officer using their standard email client. The organization's mail server supports TLS opportunistically but has never verified whether the receiving DoD mail server negotiates TLS.

What the assessor finds

An assessor reviews the mail server logs and finds 47 emails to DoD addresses sent over unencrypted SMTP connections — the receiving mail server didn't support TLS and the sender's server did not enforce it. CUI design files were transmitted in plaintext.

SPRS Score Impact

3.13.8 carries a point value of 5. CUI transmitted without encryption over any network is exposed — a single intercepted session can result in a reportable breach under DFARS 252.204-7012 and False Claims Act liability if the SPRS score claimed this control was met.

What Good Looks Like

All CUI transmission paths encrypted with FIPS 140-2 validated cryptography, TLS 1.2 or higher for web and email, SFTP or encrypted VPN for file transfers, weak cipher suites disabled, encryption configuration documented in SSP with CMVP certificate references.

Common Gaps

What assessors actually find in the field:

✗ FTP used for CUI transfers

Engineers transfer CUI design files via FTP — connections are unencrypted and credentials and file contents are transmitted in plaintext.

✗ Non-FIPS TLS cipher suites

HTTPS is in use but the server allows weak cipher suites including RC4 and 3DES — non-FIPS algorithms fail SC.L2-3.13.11.

✗ Email not TLS-enforced

Email is sent via TLS opportunistically — if the receiving server doesn't support TLS, mail falls back to unencrypted delivery.

✗ Internal transfers unencrypted

CUI is transmitted between internal servers without encryption — internal network connections are assumed to be trusted.

✗ No cryptographic documentation

Encryption is in use but the specific algorithms and FIPS validation status are not documented in the SSP.