AC.L2-3.1.20

Access Control

External Connections [CUI Data]

"Verify and control/limit connections to and use of external systems."

Objectives

[a]
Connections to external systems are identified.

[b]
The use of external systems is identified.

[c]
Connections to external systems are verified.

[d]
The use of external systems is verified.

[e]
Connections to external systems are controlled/limited.

[f]
The use of external systems is controlled/limited.

Key Discussion Points

Six Objectives:
[a]-[b] identify, [c]-[d] verify, [e]-[f] control — all three pairs apply to both connections and uses of external systems. Each is evaluated independently.

Terms and Conditions:
Agreements with external system owners must define security requirements — where terms cannot be established, the organization must restrict its own personnel from using those systems for CUI.

External Includes Cloud:
v2.13 explicitly includes cloud services (IaaS, PaaS, SaaS) — a cloud backup, M365 tenant, or collaboration platform accessed from CUI systems is an external system requiring verification.

Internal Can Be External:
v2.13 notes that an organization's own systems outside the CUI assessment scope may be treated as external — isolated labs or non-CUI networks require the same verification approach.

Assessment Methods

EXAMINE

Access control policy; procedures addressing the use of external systems; terms and conditions for external systems; system security plan; list of applications accessible from external systems; system configuration settings; system connection or processing agreements; account management documents.

INTERVIEW

Personnel with responsibilities for defining terms and conditions for use of external systems; system or network administrators; personnel with information security responsibilities.

TEST

Mechanisms implementing terms and conditions on use of external systems.

AC.L2-3.1.20

ACCESS CONTROL — External Connections [CUI Data]

Plain English

What this control is really saying:

Every external system that touches the CUI environment is a potential attack vector. This control requires identifying all external connections and uses, verifying that external systems meet security requirements, and limiting what they can access. Cloud backup services, prime contractor portals, payroll systems, and personal devices are all external systems — and each one needs to be inventoried, verified, and controlled.

How it is used:

- An inventory of all external system connections is documented in the SSP — prime contractor portal, cloud backup, payroll service, and government submission systems are each listed with security verification status.
- Written agreements (ISAs, contracts, subcontracts) with external parties define the security requirements their systems must meet before connecting to the CUI environment.
- Cloud services that process CUI are verified to hold FedRAMP authorization or equivalent — the FedRAMP authorization status is documented in the SSP.
- External connections are limited to specific IP ranges and port numbers via firewall rules — open-ended external access is not permitted.

Real World Example

The Scenario

Acme Defense submits deliverables through the prime contractor's web portal, uses a shared SharePoint site for project collaboration, employs a third-party payroll service, and uses a consumer cloud backup service that backs up all files including CUI.

What the assessor finds

The cloud backup service has never been security-vetted and stores CUI files on servers in an unknown location. There is no written agreement with the backup provider. The SharePoint site's security configuration has never been reviewed. No external connection agreements exist for any current connection.

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

External connection inventory in SSP, written agreements for all external systems, external systems verified for security adequacy, cloud services FedRAMP authorized or equivalent, firewall rules limit external access to minimum necessary, stale connections reviewed and terminated.

Common Gaps

What assessors actually find in the field:

✗ **No external connection inventory**

The organization has no list of external system connections — [a] and [b] are not met and the scope of unverified external exposure is unknown.

✗ **Unvetted cloud backup service**

CUI data is backed up to a third-party cloud service that has never been security-vetted — no agreement exists and its FedRAMP status is unknown.

✗ **No written agreements**

External systems connect to the CUI environment with no formal agreements defining security requirements — [c] and [d] cannot be demonstrated.

✗ **Unrestricted external access**

External systems can reach any internal resource once connected — no firewall rules limit what external parties can access within the network.

✗ **Stale external connections**

Connections established for past contracts remain active with no review — former external systems retain access to CUI infrastructure.