CM.L2-3.4.7

Configuration Management

Nonessential Functionality

"Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services."

Objectives

[a-c] PROGRAMS
Essential programs defined; nonessential programs defined and restricted, disabled, or prevented.

[d-f] FUNCTIONS
Essential functions defined; nonessential functions defined and restricted, disabled, or prevented.

[g-i] PORTS
Essential ports defined; nonessential ports defined and restricted, disabled, or prevented.

[j-l] PROTOCOLS
Essential protocols defined; nonessential protocols defined and restricted, disabled, or prevented.

[m-o] SERVICES
Essential services defined; nonessential services defined and restricted, disabled, or prevented.

Key Discussion Points

Extends 3.4.6:
3.4.6 establishes the principle. 3.4.7 operationalizes it — specifically naming programs, functions, ports, protocols, and services as the five dimensions.

Whitelist vs. Blacklist:
Whitelisting (approved software only) provides far more security than blacklisting — the guide acknowledges both but favors whitelisting.

Named Examples:
Bluetooth, FTP, and peer-to-peer are explicitly named in the guide — all three are common findings in DIB assessments.

All 5 Dimensions:
Programs, functions, ports, protocols, and services — each must have essentials defined, nonessentials defined, and restrictions enforced.

Assessment Methods

EXAMINE

Configuration management policy; procedures addressing least functionality; configuration management plan; system security plan; security configuration checklists; system configuration settings; specifications for preventing software program execution; documented reviews of programs, functions, ports, protocols, and/or services.

INTERVIEW

Personnel with responsibilities for reviewing programs, functions, ports, protocols, and services; personnel with information security responsibilities; system or network administrators; system developers.

TEST

Organizational processes for reviewing and disabling nonessential programs, functions, ports, protocols, or services; mechanisms implementing review and handling; mechanisms supporting software program usage and restrictions.

CM.L2-3.4.7

CONFIGURATION MANAGEMENT — Nonessential Functionality

Plain English

What this control is really saying:

3.4.6 says configure for least functionality. 3.4.7 tells you exactly what that means: every program, function, port, protocol, and service must be evaluated — essential ones defined, nonessential ones restricted, disabled, or prevented. FTP? Block it. Bluetooth? Off. Games? Gone.

How it is used:

- An approved software list is maintained — only whitelisted applications can execute on CUI workstations via AppLocker.
- All ports other than 22, 25, 53, and 443 are blocked at the firewall and on host-based firewalls — exceptions require documented approval.
- FTP, Telnet, Bluetooth, and peer-to-peer protocols are blocked by policy and enforced at the network and host level.
- An annual review of programs, ports, protocols, and services is documented — any additions or removals are tracked through change control.

Real World Example

The Scenario

Acme Defense workstations have never had a program or port review. Users have installed various utilities over the years — a file sync tool, a media player, and a remote access app. Bluetooth is on by default. FTP is enabled on the server.

What the assessor finds

A port scan reveals 14 open ports across the CUI systems with no documented justification for 9 of them. Three users have unauthorized remote access software installed. FTP is running on the file server. No program whitelist or blacklist exists.

SPRS Score Impact

3.4.7 carries a point value of 5. Unmanaged programs, open ports, and enabled protocols are the most consistently exploited attack surfaces in DIB environments — and the ones most organizations have never formally reviewed.

What Good Looks Like

Approved program list maintained and enforced, all five dimensions (programs, functions, ports, protocols, services) formally defined, nonessentials blocked at host and network, annual review documented, deviations approved in writing.

Common Gaps

What assessors actually find in the field:

✗ **FTP or Telnet still running**

Legacy protocols are still enabled on servers or workstations — commonly missed because they were set up years ago and forgotten.

✗ **No approved software list**

Users can install any software — no whitelist or blacklist is in place to control program execution.

✗ **Ports not reviewed or mapped**

Nobody has ever done a port scan of the CUI environment — open ports are unknown and unmanaged.

✗ **Bluetooth left enabled**

Workstations have Bluetooth enabled by default — no policy disables it despite CUI systems not requiring it.

✗ **Only some dimensions addressed**

Ports were reviewed and locked down, but programs and services were never evaluated — partial compliance only.