MA.L2-3.7.2

Maintenance

System Maintenance Control

"Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance."

Objectives

[a]
Tools used to conduct system maintenance are controlled.

[b]
Techniques used to conduct system maintenance are controlled.

[c]
Mechanisms used to conduct system maintenance are controlled.

[d]
Personnel used to conduct system maintenance are controlled.

Key Discussion Points

Tools Carry Malware:
A maintenance laptop or USB drive brought in from outside can introduce malware — the guide explicitly flags tools as a malware transport vector.

All Four Required:
Tools, techniques, mechanisms, AND personnel — all four must be controlled. Controlling tools but not who uses them is still a gap.

Inspect Before Use:
Maintenance media should be inspected for malicious code before connecting to CUI systems — an unscanned USB is an uncontrolled tool.

Supervision:
Maintenance personnel have elevated privilege by necessity — the guide specifically expects oversight and supervision during all maintenance sessions.

Assessment Methods

EXAMINE

System maintenance policy; procedures addressing system maintenance tools and media; maintenance records; system maintenance tools and associated documentation; maintenance tool inspection records; system security plan.

INTERVIEW

Personnel with system maintenance responsibilities; personnel with information security responsibilities.

TEST

Organizational processes for approving, controlling, and monitoring maintenance tools; mechanisms supporting or implementing inspection of maintenance tools; organizational processes for inspecting media for malicious code.

MA.L2-3.7.2

MAINTENANCE — System Maintenance Control

Plain English

What this control is really saying:

A technician with an infected laptop can introduce malware directly into your CUI environment. This control requires that maintenance tools are approved, techniques are defined, automated mechanisms are restricted, and only authorized personnel perform maintenance — with supervision.

How it is used:

- An approved maintenance tool list is maintained — only tools on the list may be used on CUI systems, and each tool is scanned for malware before use.
- Only the IT admin and one designated backup are authorized to perform maintenance — no other personnel may access administrative interfaces or maintenance ports.
- When an MSP performs remote maintenance, the session is supervised and logged — the IT admin remains connected and the session is terminated when work is complete.
- Maintenance USB drives and laptops are organization-owned, kept current with AV signatures, and scanned before each use — personally owned tools are prohibited.

Real World Example

The Scenario

Acme Defense uses an MSP for server maintenance. The MSP has a permanent VPN connection and admin credentials, connects without notice, and disconnects when done. The IT admin is rarely present. MSP technicians use their own laptops and USB drives.

What the assessor finds

MSP technicians have connected 14 times in the past 90 days with no logs of what was done. Two technicians use personal laptops — one has outdated AV signatures. No maintenance tool approval process exists. The IT admin has no visibility into what tools were connected to CUI systems.

SPRS Score Impact

3.7.2 carries a point value of 3. Uncontrolled maintenance access is a well-documented APT entry vector — attackers specifically target trusted third-party maintenance relationships to gain persistent access to defense contractor networks.

What Good Looks Like

Approved maintenance tool list maintained, tools scanned before use, only authorized personnel perform maintenance, MSP sessions supervised and logged, personally owned tools prohibited, media inspected before connecting to CUI systems, all controls documented in SSP.

Common Gaps

What assessors actually find in the field:

✗ **Any tech can use any tool**

No approved tool list exists — vendor technicians bring their own laptops and USB drives with no inspection or approval.

✗ **Uncontrolled MSP access**

The MSP has standing remote access with no supervision — they can connect at any time and there is no session logging.

✗ **Personally owned tools used**

Technicians use personal laptops for maintenance — these devices are not organization-owned, scanned, or controlled.

✗ **No maintenance personnel list**

Anyone in IT can perform maintenance — no formal authorization list defines who is permitted to conduct maintenance activities.

✗ **Media not inspected**

USB drives brought in for maintenance are connected directly to CUI systems without being scanned for malicious code first.