MP.L2-3.8.8

Media Protection

Shared Media

"Prohibit the use of portable storage devices when such devices have no identifiable owner."

Objectives

[a]

The use of portable storage devices is prohibited when such devices have no identifiable owner.

Key Discussion Points

Owner Required:
No identifiable owner = prohibited. An organization, individual, or project must be assignable to the device before it can be used.

Accountability Purpose:
Owner identification enables responsibility assignment — if a device introduces malware, the owner is accountable for its security state.

Extends 3.8.7:
3.8.7 controls removable media use generally; 3.8.8 adds a specific prohibition — even an allowable media type is banned if it lacks an owner.

Label and Register:
Practical implementation: label all organization-issued drives with owner info and maintain a device registry so ownership can be verified.

Assessment Methods

EXAMINE

System media protection policy; system use policy; procedures addressing media usage restrictions; system security plan; rules of behavior; system configuration settings; system design documentation; system audit logs.

INTERVIEW

Personnel with system media use responsibilities; personnel with information security responsibilities; system or network administrators.

TEST

Organizational processes for media use; mechanisms prohibiting use of media on systems or system components.

MP.L2-3.8.8

MEDIA PROTECTION — Shared Media

Plain English

What this control is really saying:

Someone leaves a USB drive in the parking lot. A curious employee picks it up and plugs it into their workstation. This is a classic social engineering attack — a loaded drive left where someone will find it. This control prohibits plugging in any portable storage device that cannot be traced to a known, accountable owner.

How it is used:

- All organization-issued USB drives are labeled with the owner's name, department, and a device serial number — any unlabeled drive is prohibited from use.
- Staff policy requires that found or unidentified storage devices be turned in to the IT help desk immediately — plugging them in is expressly prohibited.
- IT maintains a device registry mapping every approved portable storage device to a named owner — only registered devices may be connected to CUI systems.
- New employees are trained during onboarding on the prohibition against using unidentified portable storage devices.

Real World Example

The Scenario

An employee finds an unmarked USB drive in the company parking lot. Curious about its contents, he plugs it into his CUI workstation. The drive contains a malicious payload designed to execute automatically on insertion.

What the assessor finds

The malicious code executes, establishes a backdoor, and begins harvesting files from the CUI workstation. No policy prohibited the employee from plugging in the unidentified drive and no technical control blocked it. The attack is discovered two weeks later during a log review.

SPRS Score Impact

3.8.8 carries a point value of 1. The 'found drive' attack is a well-documented physical social engineering technique — a drive in a parking lot is a $5 attack that can compromise a multi-million dollar defense contract.

What Good Looks Like

All portable storage devices labeled with identifiable owner, device registry maintained, staff trained on prohibition against unidentified devices, found devices turned in to IT help desk, policy and technical controls documented in SSP.

Common Gaps

What assessors actually find in the field:

✗ **Found drive plugged in**

An employee found a USB drive and plugged it in — no policy prohibits this and no technical control prevented it.

✗ **Drives not labeled**

Organization-issued drives have no owner markings — there is no way to distinguish an owned drive from an unidentified one.

✗ **No device registry**

No list of approved portable storage devices exists — there is no way to verify whether a device has an identifiable owner.

✗ **Staff not trained**

Employees have never been trained on the prohibition against unidentified media — plugging in found drives is normalized behavior.

✗ **Policy exists but not enforced**

The policy prohibits unidentified drives but no technical control blocks them and no one monitors for violations.