SC.L2-3.13.12

System & Communications Protection

Collaborative Device Control

"Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device."

Objectives

[a]
Collaborative computing devices are identified.

[b]
Collaborative computing devices provide indication to users of devices in use.

[c]
Remote activation of collaborative computing devices is prohibited.

Key Discussion Points

What Devices:
Networked whiteboards, cameras, and microphones — dedicated video conferencing systems (dial-in/dial-out model) are explicitly excluded from this control.

No Remote Activation:
[c] requires that cameras and mics cannot be turned on remotely — application permission settings and OS-level controls implement this requirement.

Indication Required:
[b] requires a visible signal when a device is active — indicator lights, on-screen notifications, or posted notices outside the space all qualify.

Inventory First:
[a] must be met before [b] and [c] — without identifying all collaborative devices in CUI areas, you cannot verify controls are applied to all of them.

Assessment Methods

EXAMINE

System and communications protection policy; procedures addressing collaborative computing; access control policy; system security plan; system design documentation; system audit logs; system configuration settings.

INTERVIEW

System or network administrators; personnel with information security responsibilities; system developer; personnel with responsibilities for managing collaborative computing devices.

TEST

Mechanisms supporting or implementing management of remote activation of collaborative computing devices; mechanisms providing indication of use of collaborative computing devices.

SC.L2-3.13.12

SYSTEM & COMMS PROTECTION — Collaborative Device Control

Plain English

What this control is really saying:

A camera or microphone that can be activated remotely — without the knowledge of people in the room — is a surveillance device. This control requires that cameras and microphones cannot be turned on from a remote connection, and that when they ARE on, there is an obvious physical indication visible to everyone in the room. No hidden activation.

How it is used:

- All cameras and microphones in CUI work areas are inventoried — the SSP lists each device, its location, and the control mechanism applied.
- Remote activation of built-in laptop cameras is disabled via MDM policy — the OS camera permission is restricted so third-party applications cannot activate the camera remotely.
- A physical camera cover is installed on all workstation cameras in CUI areas — when covered, no remote activation can produce usable video even if the device is compromised.
- Cameras have a hardware indicator light that is physically wired to the camera circuit — the light cannot be disabled by software and cannot be spoofed.

Real World Example

The Scenario

Acme Defense engineers work in an open office with laptop cameras. No MDM policy restricts remote camera activation. A remote meeting application on one workstation is granted permanent camera access and can activate the camera at any time without user interaction.

What the assessor finds

The assessor reviews the camera permissions and finds the meeting application has unrestricted camera access. A test confirms the camera can be activated via API without any on-screen indication. CUI is visible in the camera's field of view with no warning to the user.

SPRS Score Impact

3.13.12 carries a point value of 1. An uncontrolled camera or microphone in a CUI workspace is a ready-made surveillance capability — remote activation by a compromised application or a threat actor is a low-effort, high-yield attack against CUI confidentiality.

What Good Looks Like

All collaborative devices in CUI areas inventoried, remote activation disabled via OS policy and MDM, hardware indicator lights present and physically wired, CUI work areas posted if devices are in use, devices covered or disabled when not in use.

Common Gaps

What assessors actually find in the field:

✗ Devices not inventoried

No inventory of cameras and microphones in CUI areas exists — the organization cannot demonstrate that all collaborative devices are controlled.

✗ No in-use indicator

Cameras activate without any visible indication — users in the room have no way to know the camera is on.

✗ Remote activation not blocked

Camera and microphone permissions allow remote activation by applications — a compromised system can silently activate audio and video.

✗ Indicator light software-driven

The camera indicator light can be disabled by software — the physical circuit does not guarantee the light is on when the camera is active.

✗ Dedicated VC excluded but others not

The organization correctly excludes dedicated video conferencing systems but has not addressed laptop cameras and USB microphones in CUI areas.