SC.L2-3.13.13

System & Communications Protection

Mobile Code

"Control and monitor the use of mobile code."

Objectives

[a]
Use of mobile code is controlled.

[b]
Use of mobile code is monitored.

Key Discussion Points

What Mobile Code Is:
JavaScript, Java, ActiveX, Flash, VBScript, PDF scripts — any code that downloads and executes automatically when content is accessed qualifies.

Control = Policy + Tech:
Controlling mobile code requires both a documented policy defining what is permitted and technical controls (group policy, proxy) that actually enforce it.

Monitor = Log + Review:
Monitoring requires that mobile code execution is logged AND that logs are reviewed — generating logs nobody looks at does not satisfy [b].

Exception Process:
Departments with legitimate needs for prohibited technologies must use a documented exception and approval process — ad hoc enablement by users is not control.

Assessment Methods

EXAMINE

System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions; system security plan; list of acceptable and unacceptable mobile code and technologies; authorization records; system monitoring records; system audit logs.

INTERVIEW

System or network administrators; personnel with information security responsibilities; personnel with responsibilities for managing mobile code.

TEST

Organizational processes for controlling, authorizing, monitoring, and restricting mobile code; mechanisms supporting the management and monitoring of mobile code.

SC.L2-3.13.13

SYSTEM & COMMS PROTECTION — Mobile Code

Plain English

What this control is really saying:

Mobile code — JavaScript, Java, ActiveX, PDF scripts — executes on your system automatically when content is loaded. An employee opens a malicious PDF or visits a compromised website and code runs without any action on their part. This control requires a policy defining what mobile code is authorized, technical controls to enforce it, and monitoring to detect when unauthorized mobile code runs.

How it is used:

- The mobile code policy defines authorized technologies (e.g., JavaScript for internal applications only) and prohibited ones (Flash, ActiveX, legacy Java applets).
- Browser group policy disables Flash and ActiveX globally — exceptions require IT approval with a documented business justification and change record.
- The web proxy logs all mobile code execution and generates alerts when prohibited technologies are detected — logs are reviewed on a defined schedule.
- Endpoint protection software monitors for unauthorized script execution at the workstation level — suspicious activity generates alerts for the security team.

Real World Example

The Scenario

Acme Defense has no mobile code policy. All browser plug-ins including Flash and legacy Java are enabled on CUI workstations. An engineer receives an email with a PDF attachment — the PDF contains malicious JavaScript that executes automatically on open.

What the assessor finds

The malicious script reads CUI files from the mapped network drive and beacons them to an external server. No mobile code controls existed to block the execution and no monitoring detected the exfiltration. The breach is discovered three weeks later during a log review.

SPRS Score Impact

3.13.13 carries a point value of 1. Uncontrolled mobile code execution is a primary initial access vector — malicious scripts in PDFs, web pages, and email attachments execute automatically without additional user action.

What Good Looks Like

Mobile code policy documented with authorized and prohibited technologies, technical controls enforce restrictions via group policy and browser configuration, exception process requires IT approval, use monitored via proxy logs and endpoint alerts, logs reviewed on schedule.

Common Gaps

What assessors actually find in the field:

✗ No mobile code policy

There is no policy defining which mobile code technologies are authorized — any website can execute any code on CUI workstations.

✗ Flash and Java not disabled

Legacy mobile code technologies (Flash, legacy Java browser plug-ins) remain enabled on CUI workstations — they are known attack vectors.

✗ No exception process

Mobile code is nominally prohibited but no exception process exists — departments enable what they need without authorization or tracking.

✗ No monitoring

Mobile code controls are configured but execution is not logged or monitored — unauthorized use is not detected.

✗ Policy but no technical control

A mobile code policy exists but no technical enforcement is in place — users can install browser plug-ins and enable content at will.