SI.L2-3.14.1

System & Information Integrity

Flaw Remediation [CUI Data]

"Identify, report, and correct system flaws in a timely manner."

Objectives

[a]
The time within which to identify system flaws is specified.

[b]
System flaws are identified within the specified time frame.

[c]
The time within which to report system flaws is specified.

[d]
System flaws are reported within the specified time frame.

[e]
The time within which to correct system flaws is specified.

[f]
System flaws are corrected within the specified time frame.

Key Discussion Points

Three Time Frames:
Identification, reporting, AND correction each require a separate defined time frame — all three must be specified in policy and all three must be demonstrably met.

Evidence Required:
Assessors look for a patch log, POAM entries, and vulnerability scan results that show flaws were identified, reported, and corrected within the defined windows.

Severity-Based Timelines:
Time frames typically vary by CVSS severity — Critical gets the shortest window, Low gets the longest. The policy must specify the timeline for each severity level.

Sources of Flaws:
Flaws come from vulnerability scans, security assessments, continuous monitoring, incident response, and vendor advisories — all must feed the remediation process.

Assessment Methods

EXAMINE

System and information integrity policy; procedures addressing flaw remediation; procedures addressing configuration management; system security plan; list of flaws and vulnerabilities; list of recent security flaw remediation actions; test results from software and firmware updates; installation and change control records.

INTERVIEW

System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for flaw remediation; personnel with configuration management responsibility.

TEST

Organizational processes for identifying, reporting, and correcting system flaws; mechanisms supporting or implementing flaw reporting and correction; mechanisms supporting software and firmware update testing.

SI.L2-3.14.1

SYSTEM & INFO INTEGRITY — Flaw Remediation [CUI Data]

Plain English

What this control is really saying:

Every software and firmware flaw is a potential attack vector. This control requires three things, each with a defined time frame: identify flaws within a specified interval, report them to the right people within a specified interval, and correct them within a specified interval. All three time frames must be documented — and all three must actually be met.

How it is used:

- A patch management policy defines scan frequency (weekly), severity-based remediation timelines (Critical: 15 days, High: 30 days, Medium: 90 days), and who is responsible for each step.
- Vulnerability scans run weekly — results are reviewed within 48 hours and findings are triaged against the patch management schedule.
- Identified flaws are entered into the POAM with owner, severity, and due date — reported to the IT manager within the time frame specified in policy.
- Patch deployment is tracked in the change management log — completion is verified by a follow-up scan before the finding is closed.

Real World Example

The Scenario

Acme Defense's patch policy says critical vulnerabilities must be patched within 30 days. The IT admin applies patches when time permits. Vulnerability scan results from six months ago show 11 critical CVEs on CUI servers. No follow-up scans have been run.

What the assessor finds

An assessor runs a current scan — 9 of the 11 critical CVEs remain unpatched, now 180+ days old. No POAM entries exist for any of them. The IT admin cannot demonstrate when the flaws were identified or reported. The 30-day policy has not been met for any finding.

SPRS Score Impact

3.14.1 carries a point value of 5. Known, unpatched vulnerabilities with no documentation of identification or reporting are among the most direct False Claims Act exposures — the SPRS score cannot honestly claim this control met while critical CVEs sit open for months.

What Good Looks Like

Time frames defined in policy for identification, reporting, and correction by severity, vulnerability scans on schedule, findings entered into POAM with owner and due date, patches deployed within defined time frames, patch log maintained as evidence, overdue items escalated.

Common Gaps

What assessors actually find in the field:

✗ **Time frames not defined**

The SSP says flaws will be remediated 'promptly' but no specific number of days is defined for identification, reporting, or correction.

✗ **Patches applied but not tracked**

Patches are deployed informally but no patch log exists — there is no evidence that corrections occurred within the defined time frame.

✗ **No reporting process**

Flaws are identified by the IT admin but never formally reported — [c] and [d] require a defined reporting process with documented time frames.

✗ **Critical vulns overdue**

The patch management policy says critical vulnerabilities must be patched in 15 days — several are 60+ days past due with no documented exception.

✗ **Scans not on schedule**

The policy defines weekly vulnerability scans but the last scan was three months ago — [a] and [b] are not being met.