



TECHNICAL BRIEF · BASED ON BOD 26-04 · CIVILIAN AGENCIES, VA, HHS, DHS, GSA

BOD 26-04: WHAT THE THREE-DAY PATCH WINDOW MEANS BY DECEMBER 7

3 days

SHORTEST BOD 26-04 REMEDIATION WINDOW, PAIRED WITH FORENSIC TRIAGE FOR THE HIGHEST-RISK TIER

CISA's BOD 26-04, a non-GAO directive, replaced the flat two-week clock for known exploited vulnerabilities with risk-based windows as short as three days. Civilian agencies start working to those timelines on December 7, 2026, and the patching work sits mostly with contractors.

THE FINDING

On June 10, 2026, CISA issued [Binding Operational Directive 26-04, Prioritizing Security Updates Based on Risk](#). It is a non-GAO directive, binding on federal civilian executive branch agencies, and it revokes the two directives agencies had patched to for years: BOD 22-01 on known exploited vulnerabilities and BOD 19-02 on internet-accessible systems.

The old rule was mostly one clock. A vulnerability in CISA's Known Exploited Vulnerabilities (KEV) catalog got roughly two weeks. BOD 26-04 replaces that with four yes-or-no questions: is the vulnerability in KEV, is the asset publicly exposed, is exploitation automatable, and does it give an attacker total or partial control. The answers set the window: three days, 14 days, 60 days, or a fix at the asset's next scheduled upgrade.

The deadlines have already started. [FedRAMP's notice on the directive](#) (FedRAMP Notice 0014) puts agency policy updates at August 7, 2026, and says that by December 7, 2026, agencies must begin evaluating and remediating vulnerabilities on the directive's timelines.

WHY IT KEEPS HAPPENING

CISA's stated reason is speed. [CISA officials pointed to AI](#) helping both researchers and adversaries find flaws faster, which shrinks the time between disclosure and exploitation. A fixed two-week clock treated an internal file server and an internet-facing gateway the same way.

The harder problem is operational. Most agency patching runs on a monthly rhythm: advisories arrive, patches go through a test group, the change advisory board approves a window, and deployment follows. That rhythm cannot produce a three-day fix without a separate emergency lane, and few operations contracts were written with one.

The top tier adds a second job. [CERT/CC's published response model for the directive](#) shows the three-day window carries a forensic triage requirement when a KEV vulnerability gives total control and the asset is either publicly exposed or automatable. Patching does not remove an attacker who got in first, so the agency has to check whether the system is already compromised.

Some systems cannot be patched quickly at all. In [GAO-25-107795](#), GAO found that 7 of the 11 most critical federal legacy systems were operating with known cybersecurity vulnerabilities, and 4 had unsupported hardware or software.

WHY IT MATTERS TO YOUR BID

Federal patching mostly happens inside contractor O&M and cyber support task orders. A performance work statement that says "apply patches monthly" or "remediate KEVs within 14 days" now sits under a directive with a three-day tier. Agencies have every reason to rewrite those requirements, and evaluators on recompetes after December 7 are likely to look for an offeror that can show the clock assignment, the emergency lane, and the evidence trail.

Cloud offerings get their own deadline. FedRAMP's notice makes its Vulnerability Detection and Response and Vulnerability Evaluation and Reporting rules mandatory on December 7, 2026. Providers that miss them can operate under corrective action plans with agency notification through March 7, 2027; after that, FedRAMP says certification will be revoked for non-compliant offerings. A prime reselling or operating a FedRAMP service inherits that date.

Pricing changes too. A three-day window needs defined coverage hours and a surge path, and a proposal that prices only the monthly cycle will not match the requirement.

TECHNICAL APPROACH

The method below comes from Avalon's [Remediation & Patch Management service](#). It describes how the work is done, at the methodology level.

- 1. Normalize the findings into one backlog.** Ingest scan exports, penetration test reports, IG or GAO findings, assessor results, and open POA&M items, then deduplicate them and map each one to an asset and a system owner. The same flaw often appears three times in three tools; the dedupe changes the size of the problem.
- 2. Assign each finding its clock.** Score every item on the directive's four decision points, using the KEV catalog and CISA's Vulnrichment data, the agency's own determination of public exposure, and SSVC decision logic. EPSS and mission context break ties. CVSS stays as supporting context only, because the directive no longer uses it to set deadlines. The output is a deadline-tagged plan the ISSO can defend.
- 3. Run tested waves, with an emergency lane.** Patches go through a test ring, a change package for the CAB, an approved window, and a validation rescan, with a rollback plan for every wave. Three-day items run through a separate, pre-agreed emergency lane with defined coverage hours instead of waiting for the monthly cycle.
- 4. Coordinate the triage step.** For top-tier items, the check for prior compromise runs before or alongside the fix. A confirmed compromise goes to the agency's incident response process; it is never closed as a patch.
- 5. Handle the unpatchable and prove closure.** Where no patch can be applied, document compensating controls such as isolation, virtual patching, or privilege reduction, with a residual-risk memo written for the authorizing official. Every closed item gets an evidence package: before-and-after scans from the same scanner and policy, change records, and POA&M input rows. The patch SOP is updated to NIST SP 800-40 Rev. 4 and the directive's policy requirements.

WHAT "FIXED" LOOKS LIKE

BOD 26-04 is new, so there is no closure history yet. These are targets, drawn from the directive's milestones:

- A vulnerability management policy that uses the four decision points, in place since the August 7 milestone.
- From December 7, every open finding carries an assigned window, and the agency can show remediation inside it, by tier.
- Each top-tier item has a triage record alongside the fix.
- Unpatchable systems have documented compensating controls and an accepted residual risk, not an open-ended exception.

STATUS CHECK

OPEN BOD 26-04 has been in effect since CISA issued it on June 10, 2026.

MILESTONE	DATE	APPLIES TO
Agency policies support the directive	August 7, 2026	Civilian agencies
Remediation on BOD 26-04 timelines begins	December 7, 2026	Civilian agencies
FedRAMP VDR and VER rules mandatory	December 7, 2026	FedRAMP cloud providers
End of corrective action grace period	March 7, 2027	FedRAMP cloud providers

TEAMING FIT

NAICS	541512, 541519
AVALON'S SUB ROLE	Remediation backlog normalization, BOD 26-04 clock assignment, tested patch waves, and closure evidence under the prime's O&M or cyber support task order
SMALL-BUSINESS STATUS	Small business; HUBZone (in progress)
LIKELY VEHICLES	GSA MAS (SIN 54151S IT Professional Services); GSA MAS (SIN 54151HACS Highly Adaptive Cybersecurity Services); GSA OASIS+

If civilian agency O&M or cyber support work is in your capture plan, Avalon teams as the sub that turns the remediation backlog into BOD 26-04 clocks, tested fixes, and closure evidence before December 7.

BRANDON IRELAND, FOUNDER · CONTACT@AVALONTECHSERVICES.COM · AVALONTECHSERVICES.COM

This brief analyzes publicly released oversight reports. It does not describe work Avalon performed for any agency named.