INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-05 08:20 UTC

CISA Evaluates Shortened Vulnerability Remediation Deadlines Amid AI-Driven Threat Concerns

GOVERNANCE | MEDIUM

SCC Item ID	SCC-GOV-2026-0029
Type	Governance
Severity	MEDIUM
Affected Products	U.S. federal government IT systems (all civilian executive branch agencies subject to BOD 22-01 and related CISA directives)
Discovery Source	Gemini

Executive Summary

CISA is reported to be evaluating whether to shorten the remediation deadlines in Binding Operational Directive 22-01, which currently governs how quickly federal civilian agencies must patch known exploited vulnerabilities. The evaluation is driven by concern that AI-assisted threat actors can develop and deploy exploits faster than existing deadline windows allow agencies to respond. As of March 4, 2026, no official CISA publication confirming a formal evaluation or proposed timeline change has been located; this item is based on policy reporting and signals. Organizations should treat this as a planning signal, not a confirmed directive change. Federal agencies and their contractors should monitor for updated CISA guidance and assess whether current patching velocity would meet tighter requirements.

Technical Analysis

BOD 22-01, issued October 2021, requires all federal civilian executive branch (FCEB) agencies to remediate vulnerabilities listed in the CISA Known Exploited Vulnerabilities (KEV) catalog within defined windows, typically 2 weeks for critical vulnerabilities and up to 6 months for lower-severity entries. The reported evaluation focuses on whether those windows remain operationally valid given reported AI-accelerated exploit development cycles, where the time from vulnerability disclosure to weaponized exploit deployment may be compressing. No CVE, CWE, or specific technical vulnerability is associated with this item; the risk is policy-structural rather than a discrete vulnerability. Affected scope: all FCEB agencies and their supply chains operating under BOD 22-01 and related CISA vulnerability management directives. Verification against official CISA publications is required before treating proposed timelines as authoritative.

Action Checklist

1. Step 1: Awareness, Monitor the CISA Binding Operational Directives page (https://www.cisa.gov/binding-operational-directives) weekly for any formal updates to BOD 22-01 timelines. Subscribe to CISA updates (https://www.cisa.gov/subscribe-updates-cisa) to receive notifications of policy changes.
2. Step 2: Assessment, Audit your current mean-time-to-patch (MTTP) for KEV-listed vulnerabilities against existing BOD 22-01 deadlines. Identify where you are already at risk of missing current windows before any tightening occurs.
3. Step 3: Gap Analysis, Document: (1) your current inventory completeness, (2) how long patch testing takes, (3) change approval time, (4) deployment time from approval to completion. Determine how much timeline compression your program can absorb before compliance risk materializes.
4. Step 4: Readiness Planning, Identify the top 10 asset classes where patching velocity is slowest (legacy systems, OT/ICS-adjacent, vendor-managed). Begin discussions with system owners or vendors now about what accelerated patching would require (staffing, testing shortcuts, risk acceptance).
5. Step 5: Post-Directive Posture, When a formal directive change is confirmed, conduct a full BOD 22-01 compliance re-baseline against the new timelines. Document the gap, assign owners, and report status to leadership. This item represents a policy risk signal, not an emergency; treat it as a planning trigger.

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to urgent and notify agency CISO and legal counsel immediately if CISA publishes a formal BOD 22-01 amendment shortening remediation windows, if a KEV entry is added for a vulnerability currently unpatched on a FISMA High system, or if the agency's current MTTP audit reveals existing non-compliance with current deadlines prior to any directive change — the latter constitutes an active compliance violation requiring POA&M entry and potential FISMA reporting.
Recovery Notes	This threat represents a policy risk signal rather than an active exploitation event, so 'recovery' applies in the governance sense: once a formal BOD 22-01 directive change is confirmed, re-execute Steps 2 and 3 against the new timelines within 72 hours to produce an updated compliance gap report. Monitor the CISA KEV catalog daily for the first 30 days post-directive-change, as CISA historically adds new KEV entries concurrent with directive updates, potentially compressing timelines for newly listed vulnerabilities that are already present in your environment. Verify that all POA&M entries created during this planning phase are updated to reflect new deadlines and that automated patch management tooling (WSUS scheduled tasks, SCCM deployment rings) has been reconfigured to target the new windows.

Forensic Artifacts	CISA KEV catalog CSV export (https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv) with download timestamp — serves as the authoritative record of which vulnerabilities carried BOD 22-01 obligations at any point in time; retain dated copies to reconstruct compliance posture during any given audit window | Patch management system deployment logs showing CVE-to-asset remediation timestamps — for WSUS environments, export from C:\Windows\SoftwareDistribution\ReportingEvents.log and the WSUS SQL database's tbUpdate and tbComputerTarget tables; these logs are the primary evidence of whether BOD 22-01 deadlines were met for specific CVE entries | Change management ticket records for security patches — export from ServiceNow, Jira, or equivalent showing ticket creation date (patch available), change approval date, and deployment completion date for all KEV-related patches; the gap between these timestamps is the forensic record of where your pipeline failed or succeeded | Asset inventory export with last-scan timestamps — produced by your vulnerability scanner (OpenVAS, Nessus, or WSUS computer list) showing all enterprise assets, their software versions, and last assessment date; assets absent from this inventory or with stale scan dates are the forensic evidence of CIS 1.1 and NIST CM-8 gaps that caused KEV misses | POA&M documentation and leadership notification records — dated POA&M entries, email acknowledgments, and status reports constitute the administrative forensic trail demonstrating FISMA-required organizational awareness and response to BOD 22-01 compliance obligations; these are the artifacts an OIG auditor will request first during a FISMA review

Per-Action IR Details

Step 1: Awareness — Monitor the CISA Binding Operational Directives page (https://www.cisa.gov/binding-operational-directives) and the KEV catalog for any formal updates to BOD 22-01 timelines. Set an alert or calendar review cadence — at minimum weekly — given the reported active evaluation.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and maintaining situational awareness of evolving policy requirements that govern agency response timelines

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — requires ongoing receipt and internal dissemination of CISA directives including BOD updates, NIST IR-8 (Incident Response Plan) — IR plans must account for governing directive timelines; a BOD 22-01 timeline change requires plan revision, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — vulnerability management process documentation must reference current BOD 22-01 deadlines and be updated when authoritative guidance changes

Compensating: Create a free CISA govDelivery subscription at public.govdelivery.com/accounts/USDHSCISA to receive email notifications on BOD and KEV updates. Supplement with a weekly 15-minute calendar block where one analyst manually checks https://www.cisa.gov/known-exploited-vulnerabilities-catalog and https://www.cisa.gov/binding-operational-directives for changelog entries. Use a shared markdown log file in a version-controlled repo (e.g., a private GitHub repo) to record each review date and any changes observed — this creates an audit trail at zero cost.

Evidence: This is a policy monitoring step, not an exploitation event — traditional forensic evidence collection does not apply. However, document the review cadence itself: maintain timestamped log entries for each CISA directive check (reviewer name, date, KEV catalog version hash or entry count, any BOD 22-01 changelog observation). These records serve as compliance evidence during FISMA audits or IG reviews demonstrating the agency maintained awareness of evolving CISA directives.

Step 2: Assessment — Audit your current mean-time-to-patch (MTTP) for KEV-listed vulnerabilities against existing BOD 22-01 deadlines. Identify where you are already at risk of missing current windows before any tightening occurs.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Assessing current operational capability and identifying gaps before an incident or directive change forces reactive response

Controls: NIST SI-2 (Flaw Remediation) — requires identification, reporting, and correction of system flaws with tested updates; MTTP measurement is the operational metric demonstrating SI-2 effectiveness against KEV-listed flaws, NIST RA-3 (Risk Assessment) — current BOD 22-01 compliance posture against KEV deadlines is a direct risk assessment input; agencies with MTTP exceeding 15-day windows for critical KEV entries carry quantifiable compliance risk, CIS 7.2 (Establish and Maintain a Remediation Process) — requires a documented risk-based remediation strategy with tracking; MTTP per KEV entry is the primary metric this safeguard demands, CIS 7.3 (Perform Automated Operating System Patch Management) — MTTP audit must include whether OS-level KEV patches are being deployed via automated tooling or manual processes, as manual processes are the primary source of timeline overrun

Compensating: Export the current CISA KEV catalog as CSV from https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv. Cross-reference against your asset inventory using a Python script or Excel VLOOKUP to identify which KEV CVEs affect your environment and their due dates under BOD 22-01 (14 days for critical, 60 days for others). For each matched CVE, query your patch management tool (WSUS, SCCM, or even a manual spreadsheet) for the actual remediation date. Calculate MTTP per CVE. For systems with no patch management tooling, run 'wmic qfe list full' on Windows hosts or 'rpm -qa --last' on RHEL/CentOS to extract installed patch history with timestamps.

Evidence: Pull patch deployment records from your patch management system for all KEV-listed CVEs in the past 12 months — specifically: CVE ID, asset hostname, patch available date (vendor advisory publish date), patch deployed date, and days-to-remediation. For Windows environments, query Windows Update logs at C:\Windows\Logs\WindowsUpdate\ for CBS.log and WindowsUpdate.log to reconstruct actual patch installation timestamps. For Linux, review /var/log/yum.log or /var/log/apt/history.log. These timestamps are the evidentiary baseline proving or disproving current BOD 22-01 compliance before any deadline tightening is formalized.

Step 3: Gap Analysis — Map your patching pipeline — asset inventory completeness, patch testing cycles, change management lead times — to determine how much timeline compression your program can absorb before compliance risk materializes.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Identifying capability gaps in tools, processes, and workflows that would prevent effective response under tightened BOD 22-01 timelines

Controls: NIST CA-7 (Continuous Monitoring) — continuous monitoring strategy must account for the velocity at which KEV-listed vulnerabilities must be detected, assessed, and remediated; pipeline bottlenecks represent monitoring gaps, NIST CM-8 (System Component Inventory) — asset inventory completeness is the first pipeline stage; gaps in CM-8 compliance directly cause KEV misses because untracked assets cannot be patched within any deadline, NIST SI-2 (Flaw Remediation) — change management lead times and patch testing cycles are the operational components of SI-2; this gap analysis documents where SI-2 implementation is insufficient for compressed timelines, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — an incomplete asset inventory is the most common root cause of BOD 22-01 deadline failures; inventory gaps must be quantified before timeline compression is assessed, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — the vulnerability management process documentation must include change management lead times; if the documented process cannot complete within a hypothetical 7-day window, that is a documented program risk

Compensating: Use osquery with the 'programs' and 'os_version' tables to enumerate software inventory across endpoints without a commercial scanner: 'SELECT name, version, install_date FROM programs;' Export results to CSV and cross-reference against KEV CVE entries using the NIST NVD CPE data. For change management lead time analysis, export your change management ticket history (ServiceNow, Jira, or even a shared spreadsheet) and calculate median days from 'patch available' to 'change approved' to 'deployed' — this three-stage breakdown reveals exactly where the pipeline is slowest. Document findings in a gap matrix with columns: Asset Class | Current MTTP | BOD 22-01 Deadline | Gap (days) | Pipeline Bottleneck.

Evidence: The primary evidence artifacts for this step are process documentation gaps, not forensic artifacts. Collect: (1) your current asset inventory export with last-scan timestamps to identify stale or missing records (assets not

scanned in >30 days are inventory gaps under CIS 1.1); (2) your change management system's average cycle time report for security patches in the past 6 months; (3) any patch testing exemption records showing which asset classes receive abbreviated or waived testing. These documents constitute the compliance evidence demonstrating whether your program can absorb compressed BOD 22-01 timelines.

Step 4: Readiness Planning — Identify the top 10 asset classes where patching velocity is slowest (legacy systems, OT/ICS-adjacent, vendor-managed). Begin pre-negotiating accelerated patching SLAs with those system owners or vendors now.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing relationships, agreements, and pre-authorized actions with third parties and system owners to enable faster response when directive timelines tighten

Controls: NIST IR-4 (Incident Handling) — incident handling capability must address systems that cannot be patched within standard timelines; pre-negotiated SLAs and compensating controls are the IR-4 mechanism for those asset classes, NIST SA-9 (External System Services) — vendor-managed systems subject to BOD 22-01 must have contractual provisions for security patch delivery timelines; pre-negotiating SLAs is the SA-9 enforcement action for KEV compliance, NIST CP-2 (Contingency Plan) — legacy and OT/ICS-adjacent systems that cannot meet compressed patching timelines require documented contingency plans including isolation procedures and compensating controls, CIS 2.2 (Ensure Authorized Software is Currently Supported) — vendor-managed and legacy assets that are end-of-life or unsupported cannot receive KEV patches at any speed; identifying these in the top-10 slowest asset classes triggers CIS 2.2 remediation actions (upgrade, replace, or document exception)

Compensating: For OT/ICS-adjacent and legacy systems that cannot be patched within compressed windows, document a formal compensating control package for each asset class using the CISA BOD 22-01 exception process. Compensating controls for these systems specifically include: (1) network segmentation — verify with 'netstat -an' or firewall rule export that the asset has no direct internet-facing exposure; (2) application whitelisting using free tools such as Windows Defender Application Control (WDAC) policies or fapolicyd on Linux; (3) deploy Sysmon on Windows legacy hosts using the SwiftOnSecurity config (github.com/SwiftOnSecurity/sysmon-config) to increase detection visibility on systems that cannot be patched. For vendor-managed systems, send written notice to vendors citing BOD 22-01 obligations and request written SLA commitments with specific day-count targets.

Evidence: Before finalizing the top-10 asset class list, capture current exposure evidence for each candidate: run 'nmap -sV --script vulners [asset IP range]' or use OpenVAS (free) to generate a vulnerability scan report showing which KEV CVEs are currently unpatched on each asset class. For OT/ICS-adjacent systems, capture network traffic baselines using Wireshark or tcpdump to document normal communication patterns — this baseline becomes critical if a compensating control (network segmentation) is later applied and you need to verify no operational disruption occurred. Retain these scan reports as the pre-SLA-negotiation evidence baseline.

Step 5: Post-Directive Posture — When a formal directive change is confirmed, conduct a full BOD 22-01 compliance re-baseline against the new timelines. Document the gap, assign owners, and report status to leadership. This item represents a policy risk signal, not an emergency — treat it as a planning trigger.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Applying lessons learned and updating policies, plans, and controls in response to a confirmed change in the governing threat or regulatory environment — in this case, a formalized BOD 22-01 timeline revision

Controls: NIST IR-8 (Incident Response Plan) — a confirmed BOD 22-01 timeline change requires formal revision of the IR plan to reflect new patching deadlines; assign a plan owner and document the revision date, NIST SI-2 (Flaw Remediation) — flaw remediation procedures must be updated to reflect the new BOD 22-01 windows; assign SI-2 procedural ownership to a named role with a revision deadline, NIST CA-5 (Plan of Action and Milestones) — the compliance gap documented in this step is a POA&M entry; each gap item requires owner assignment, milestone dates, and resource identification consistent with FISMA POA&M reporting requirements, CIS 7.2 (Establish and Maintain a Remediation Process) — the remediation process documentation must be updated to reflect new BOD 22-01 timelines with monthly tracking; leadership reporting described in this step is the CIS 7.2 reporting mechanism, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — the vulnerability management process itself must be updated; re-baselining against new timelines is the CIS 7.1 annual review trigger executed on a non-annual

forcing function

Compensating: For small teams without GRC platforms, manage the BOD 22-01 re-baseline using a structured spreadsheet with columns: CVE ID | Affected Asset | Asset Owner | Current Patch Status | Old Deadline | New Deadline | Gap (days) | Assigned Remediator | Target Completion | Status. Track this weekly in a shared drive accessible to leadership. For leadership reporting, generate a one-page summary using the KEV catalog CSV cross-referenced against your asset inventory showing: total KEV-applicable CVEs in environment, count compliant under old timeline, count non-compliant under new timeline, and top-5 highest-risk gaps by asset criticality. This is achievable with Python pandas or Excel pivot tables at zero tool cost.

Evidence: The post-directive evidence package should include: (1) a point-in-time snapshot of your KEV compliance posture taken immediately when the formal directive change is published — export the KEV catalog CSV and your patch status data on that date and retain as a timestamped baseline; (2) your POA&M entries created for each identified gap, with creation timestamps; (3) written leadership acknowledgment of the gap report (email thread or signed document) to establish the organizational notification record. These artifacts collectively demonstrate FISMA-required awareness and response to a changed CISA directive, which may be reviewed during OIG audits or FISMA reporting cycles.

Detection Guidance

There is no technical vulnerability to detect in this item. The relevant monitoring is policy-track, not threat-track. Actions: (1) Monitor the CISA Binding Operational Directives page (https://www.cisa.gov/binding-operational-directives) weekly for any formal amendment or superseding directive to BOD 22-01. Subscribe to CISA updates (https://www.cisa.gov/subscribe-updates-cisa) to receive notifications. (2) Track CISA KEV catalog additions weekly; an acceleration in KEV additions or a formal reduction in remediation windows will appear there first. (3) Review DHS cybersecurity policy announcements at https://www.dhs.gov/topics/cybersecurity. No log queries, IOC patterns, or behavioral indicators apply to this item.

Framework Mappings

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

Sources

Source	URL	Tier
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
NVD - Home	https://nvd.nist.gov/	T1

Source	URL	Tier
America's Cybersecurity Risks and How GAO Is Helping to Address ...	https://www.youtube.com/watch?v=31XedNZrVcw	T3
Cybersecurity - Homeland Security	https://www.dhs.gov/topics/cybersecurity	T1
What are the Biggest Challenges to Federal Cybersecurity? (High ...	https://www.gao.gov/blog/what-are-biggest-challenges-federal-cybers...	T1

Generated 2026-05-05 08:20 UTC by TJS Security Command Center