Delinea

June 2026 | Delinea Federal team

BOD 26-04 & Privileged Access Management

How Delinea Secret Server satisfies the forensic triage requirement

What is BOD 26-04?

CISA Binding Operational Directive 26-04, signed June 10, 2026, replaces both BOD 19-02 and BOD 22-01, retiring flat CVSS-based patch deadlines in favor of a dynamic, four-variable risk model that assigns graduated remediation timelines based on the actual threat each vulnerability poses to a specific Federal system.

BOD 26-04 applies to all 100-plus Federal Civilian Executive Branch (FCEB) agencies and all systems they operate, including FedRAMP-hosted environments.

Asset exposure

Is the system publicly reachable from the internet?

KEV catalog status

Is active exploitation confirmed in the CISA KEV catalog?

Exploit automation

Can the vulnerability be fully auto-exploited by an adversary?

Technical impact

Does successful exploitation yield total system control?

Five remediation tiers

Deadline	Tier	Trigger condition	Requirement
3 days	Tier 1	All four factors: exposed, KEV, auto-exploitable and total system control	Forensic triage report required before patching
3 days	Tier 2	High-risk combinations: three of the four highest-risk factors present	No forensic triage required
14 days	Tier 3	Standard accelerated: publicly exposed and at least one other factor	Normal patch process
60 days	Tier 4	Some factors present, but not worst-case combination	Normal patch process
Defer	Tier 5	No risk criteria met, wait until next scheduled upgrade cycle	Formal deferral permitted

Key operational note

The cybersecurity and infrastructure agency (CISA) estimates that approximately 1% of vulnerability instances qualify for the 3-day Tier 1 clock, and approximately 60% qualify for deferral. The directive is designed to focus the remediation effort, not multiply it. But Tier 1 events require a forensic triage report **before patching can begin**.

The Tier 1 forensic triage requirement

For every Tier 1 vulnerability, agencies must complete a forensic triage investigation before applying the patch. CISA's implementation guidance defines six required steps:

1 **Scope the notification**
Identify all systems affected by the vulnerability

2 **Gather evidence**
Collect logs, session data, and access records from the affected system

3 **Implement containment**
Take initial actions to limit the impact of potential exploitation

4 **Take control actions**
Apply compensating controls while preparing the patch

5 **Perform analysis**
Determine if the system was compromised and answer "who, what, where, when"

6 **Produce a forensic triage report**
Document findings for CISA submission; this is required before patching

Step 5 is where most agencies will struggle. Answering "who, what, where, and when" for a privileged system requires complete, tamper-evident session records for every account that accessed it. Without a privileged access management (PAM) solution, this evidence either doesn't exist or takes days to reconstruct.

How Delinea Secret Server satisfies the triage requirement

Secret Server's privileged session management capabilities directly produce the forensic evidence CISA requires automatically and in real time, for every privileged session on every covered system.

Secret Server capability	What it captures	BOD 26-04 triage steps satisfied
Session recording	Full video and keystroke log of every privileged RDP/SSH session	**Steps 2, 5, 6:** primary triage evidence
Session metadata and search	User, account, system, duration, commands run, all fully searchable	**Step 5:** rapid "who, what, when" reconstruction
Iris AI Audit (Platform)	AI-generated session labels (suspicious, privilege elevation) in minutes, not hours	**Step 5:** accelerated analysis for Tier 1 clock
Credential checkout audit	Every secret access: Who checked out what credential, when, and from where	**Step 2:** evidence of account access pre-incident
Real-time alerting	Immediate alerts on anomalous privileged behavior or policy violation	**Step 3:** containment trigger
Tamper-evident audit trail	Immutable log chain, and cryptographically protected session records	**Step 6:** forensic report integrity

Cloud vs. on-premise: What BOD 26-04 changes

	Secret Server cloud (SaaS)	Secret Server on-premise
Patch delivery	Automatic via CI/CD, agency never manually patches	Quarterly feature and as-needed maintenance releases
Tier 1 patch clock	Delinea patches before the 3-day clock starts	Agency owns the 3-day remediation clock
Compensating control	Not needed, patched automatically	Remove from public exposure to downgrade tier
FedRAMP status	Under Assessment for High (UberEther partnership)	On-premise deployment subject to agency ATO
TMF loan eligibility	Yes, PAM explicitly named in TMF eligible categories	Depends on agency modernization plan

Recommendation:

Agencies currently running Secret Server on-premise should evaluate migration to Secret Server cloud or the Delinea Platform. Cloud delivery structurally eliminates the Tier 1 patch window risk. Technology Modernization Fund (TMF) loans are available, and PAM deployments qualify.

Next steps

Request a BOD 26-04 briefing

Schedule a 30-minute session with the Delinea Federal team to map your agency's privileged access environment to BOD 26-04 triage requirements.

Download the ZTMM and PAM compliance mapping

Delinea's Zero Trust Maturity Model whitepaper covers 14 named capability activities agencies can cite in OMB remediation plans.

Contact your Carahsoft representative

Delinea is available through Carahsoft and major federal integrators. TMF loan structuring support available through the Delinea federal channel.

Delinea

Delinea is the identity security control plane enterprises trust to secure human, machine, and AI identities across on-premises, multi-cloud, and dynamic environments. Built for the AI era, Delinea continuously discovers identities, analyzes risk, and enforces least-privilege through just-in-time, policy-based authorization. By supporting both credential-based and ephemeral access models, Delinea enables organizations to reduce risk, simplify governance, and move toward Zero Standing Privilege at their own pace. Easy to deploy and built to scale, Delinea delivers value in weeks, not months, with up to 90% fewer resources required and 99.995% uptime. Learn more at **delinea.com**.