

Turning CISA's BOD 26-04 Into Live Clocks for Critical Infrastructure



On June 10, 2026, CISA issued Binding Operational Directive 26-04, Prioritizing Security Updates Based on Risk, replacing years of flat patching guidance with a risk model that gives each vulnerability its own remediation deadline.

Instead of treating every finding as equally urgent, BOD 26-04 uses four signals to determine remediation windows: public exposure, KEV status, exploit automation, and technical impact. When CISA applied this risk model to a real civilian agency's vulnerability instances, only about 1 percent of findings required the urgent 3-day response while more than 60 percent could safely wait for the next scheduled upgrade.

About 1%

of findings required the urgent 3-day response

More than 60%

could safely wait for the next scheduled upgrade

4

signals used to determine remediation windows

For CISOs and platform teams in critical infrastructure and federal-adjacent environments, that is more than a policy update. It is a new operating model for vulnerability management. Teams are now expected to prove that remediation is happening on time against a risk-weighted CISA standard, not just show that scans were run and tickets were filed.

RapidFort believes that security risks in the software supply chain should be eliminated at the source, not managed downstream after they have already entered production.

RapidFort Continuous Compliance applies that principle directly to container security and gives organizations a practical way to operationalize CISA's model across images and running workloads.

Introducing RapidFort Continuous Compliance

RapidFort Continuous Compliance is a BOD 26-04 aligned capability within the RapidFort Platform that identifies Known Exploited Vulnerabilities (KEVs), applies CISA-aligned remediation tiers, and tracks whether every in-scope CVE is inside or outside the required SLA window. For each finding, the platform shows the assigned tier, deadline, and current SLA state, including on-track, overdue, or triage-required.

To accelerate adoption, RapidFort is launching RapidFort Continuous Compliance for eligible critical infrastructure and federal-adjacent organizations. The complimentary program provides one year of free access under a dedicated license that includes scan, curation, and hardening entitlements, enabling qualified teams to begin identifying KEVs, enforcing remediation SLAs, and hardening vulnerable container images immediately.

This solution reflects a simple idea: CISA changed the way vulnerability urgency is defined, and infrastructure operators need more than another scanner. They need a continuous control system that understands the directive, applies it to modern software supply chains, and connects deadlines to concrete remediation action.

How the Capability Works

BOD 26-04 evaluates every vulnerability using four binary variables. Three of those variables come directly from CISA data sources through KEV and Vulnrichment; the fourth, public exposure, is environment-specific and supplied by the operator. RapidFort Continuous Compliance ingests these signals, scores each finding against the directive's model, and places it into one of five remediation tiers ranging from 3 days plus forensic triage to next system upgrade.

RapidFort Continuous Compliance is designed to be continuous rather than static:



Live KEV and Vulnrichment updates

RapidFort refreshes CISA KEV and Vulnrichment data on a 15-minute cycle so changes in exploit status, automation, or technical impact are reflected quickly.



Dynamic SLA clocks

Tier assignments are recalculated whenever any of the four variables changes, so deadlines reflect the current state of risk instead of the state captured at first discovery.



Per-image and per-instance context

Operators can define exposure by image or by application and apply the same logic to running container instances, allowing the platform to distinguish between internal and internet-facing deployments of the same software.

The result is a CISA BOD 26-04 vulnerability management view that reduces risk by being actionable, measurable, and tied to how workloads actually run.

Why This Matters for Critical Infrastructure

Most critical infrastructure organizations are running large amounts of open source and containerized software that they did not write and do not directly control. At the same time, AI-driven development is increasing code volume and accelerating the rate at which vulnerabilities are introduced, while threat actors using AI-assisted offense are compressing the window from disclosure to exploitation. Traditional vulnerability management approaches are struggling because they detect and prioritize risk, but they do not remove enough of it fast enough to keep pace with AI-enabled adversaries.

That is where BOD 26-04 and the associated BOD scanner become operationally relevant. The directive does not just demand faster patching; it demands better prioritization, clearer accountability, and auditable evidence that high-consequence vulnerabilities are being addressed according to risk. For critical infrastructure and federal supply chain organizations, that standard is quickly becoming a de facto expectation, whether or not the directive applies to them directly.

RapidFort addresses this problem by pairing BOD 26-04 scoring with curation and hardening actions. Teams can apply upstream fixes, move to RapidFort curated images, or remove unused risky components to eliminate vulnerabilities, including many cases where no upstream patch exists. That moves the conversation from prioritization alone to continuous threat elimination.

From Intake to Runtime

One of the most important aspects of the release is that it does not stop at static image scanning or registry-only container security. RapidFort applies the same BOD 26-04 scoring model to running container instances through runtime instrumentation, which means teams can evaluate the workloads that are actually exposed in production, not only the artifacts stored in a registry.

This matters because true exposure is runtime contextual. The same image may be harmless in one internal deployment and internet-facing in another. By grounding the exposure signal in runtime reality, RapidFort helps CISOs and platform teams make deadline decisions based on live operational conditions rather than assumptions.

Historically, scanning only took place at build and deploy, which meant risks would only be identified in the next release cycle. For environments with long-lived services, this runtime approach now closes the gap between what was originally built and what is still running today. Findings, tiers, and deadlines stay attached to the live workload where the true risk actually resides.

Making Compliance Operational

BOD 26-04 includes a Highest tier that requires both a 3-day remediation window and forensic triage for KEV-listed vulnerabilities with total technical impact. RapidFort operationalizes this with Jira integration that opens issues when findings enter the triage tier and keeps triage state synchronized through investigation and sign-off.

The platform also supports CSV export of findings, tiers, deadlines, status, and affected assets, allowing teams to move data into their existing reporting, remediation, and audit processes. That is important for public sector and regulated operators that need to demonstrate measurable progress, maintain evidence, and brief leadership using familiar workflows.

RapidFort also surfaces blocked, no-fix findings separately and exposes a Max achievable metric, so compliance posture is reported honestly rather than inflated by findings that cannot yet be patched through conventional means.

The direction from CISA is clear. Vulnerability management is shifting from backward looking deadlines to risk-weighted clocks. RapidFort is responding with equal clarity by delivering a continuous platform that helps critical infrastructure identify what matters, act within the required window, and eliminate attack vectors at the source before they become a path to compromise.

Enroll in the RapidFort Continuous Compliance Program

Organizations operating critical infrastructure or serving adjacent federal supply chains can register interest in the RapidFort Continuous Compliance Program to receive one year of free access to this RapidFort capability, subject to eligibility validation and program terms.

The goal is to help qualified teams stand up a directive-aligned KEV scanning and remediation workflow quickly, reduce friction to adoption, and respond to CISA with a measurable operational plan

[Request Access ↗](#)