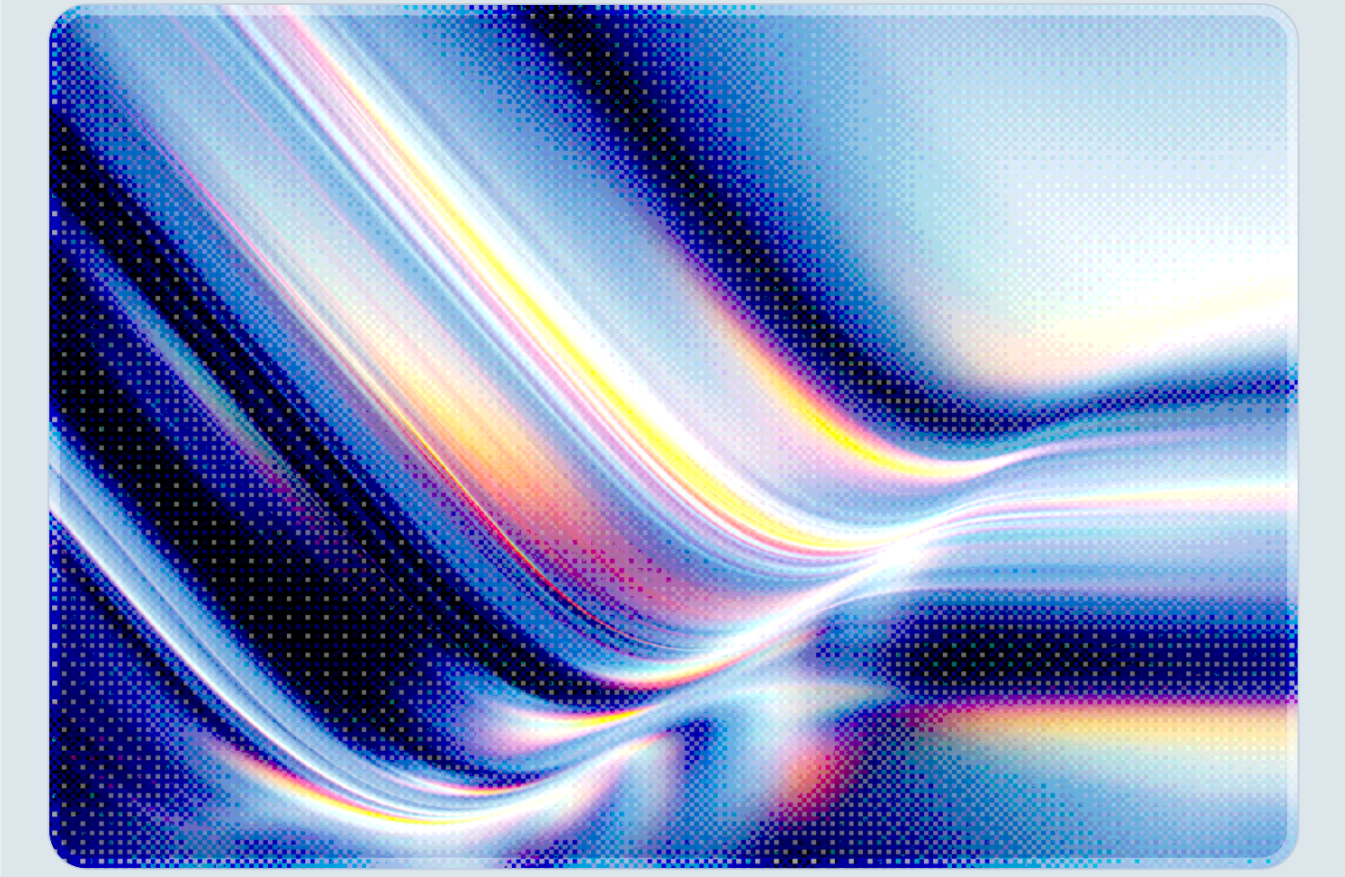
CSAI Foundation | Cloud Security Alliance

NVD Risk-Based Triage: A CISO Compliance Playbook

What the April 15, 2026 Enrichment Policy Means for FedRAMP, PCI DSS, and Cloud Security Programs

2026-04-26

Unofficial AI-assisted Research



CSAI | CSA cloud security alliance®

Key Takeaways

On April 15, 2026, the National Institute of Standards and Technology formally restructured the National Vulnerability Database from a universal CVE enrichment service into a risk-based triage queue. Going forward, NIST will prioritize three categories of vulnerabilities for analyst enrichment — those listed in the CISA Known Exploited Vulnerabilities (KEV) catalog, those affecting software used inside the U.S. federal government, and those involving "critical software" as defined by Executive Order 14028 [16] — with a goal of one business day for KEV records [1][2]. Every other CVE will be ingested but tagged "Lowest Priority — not scheduled for immediate enrichment," and the roughly 29,000 backlogged records published before March 1, 2026 were administratively reclassified into the new "Not Scheduled" status the same week [1][3][4][9]. The agency will also stop authoring a separate CVSS score when the responsible CVE Numbering Authority (CNA) has already supplied one [1].

NIST has framed the change as a capacity response rather than a policy preference [1][2], and the supporting statistics are consistent with that framing. The agency cites a 263% increase in CVE submissions between 2020 and 2025, with first-quarter 2026 submissions running roughly one-third higher than the same period a year earlier; NIST analysts enriched approximately 42,000 CVEs in 2025, 45% more than any prior year, and industry forecasters expect continued growth into 2026 [1][2]. Harold Booth, a NIST computer scientist working on the NVD, framed the shift bluntly: "CVE reporting keeps increasing — and trust me, at the NVD, we see them all — and our ability to keep up is just not there" [4].

For CISOs the consequences reach into core program documentation. Most modern vulnerability management workflows assume that NVD will supply a normalized CVSS v3.1 base score, a Common Platform Enumeration (CPE) applicability tree, a CWE classification, and tagged references for nearly every CVE within a predictable window. That assumption now holds for only a small minority of new records. Caitlin Condon, head of vulnerability research at VulnCheck, warned in response to the announcement that "a significant portion of vulnerabilities now appear to have no clear path to enrichment" through NIST [2]. CISOs who reference "the NVD CVSS score" in policy documents, scanner configurations, or audit narratives will need to either rewrite those documents or accept that the underlying data is becoming progressively less complete for most CVEs published after April 15, 2026.

The ecosystem has developed compensating capabilities since 2022. CNAs now author the majority of CVSS v3.1 vectors, CISA's Authorized Data Publisher (ADP) program delivers Stakeholder-Specific Vulnerability Categorization (SSVC) decisions on most non-priority CVEs within days of publication, the Exploit Prediction Scoring System (EPSS) v4 produces daily probability estimates for any CVE

regardless of NVD status, and CSA's Cloud Controls Matrix (CCM) and AI Controls Matrix (AICM) already specify a vulnerability-management posture that does not depend on NVD as the sole source of truth [5][6][7]. The path forward for CISO programs is to formalize this multi-source posture, update compliance documentation accordingly, and stop treating NVD as a single-vendor authority.

Background

The April 15, 2026 announcement was a formal acknowledgment of a transition that had been visible in the data since 2022. NVD's analyst-driven enrichment program reached peak coverage in 2020-2021, when virtually every CVE received a CVSS v3.1 vector, a CPE applicability tree, a CWE mapping, and reference tagging. Beginning in 2022, NVD reduced CVSS v2 authoring as a redundant workload; by February 2024, when its processing backlog became publicly visible, the agency was already operating in a triage posture. The April 2026 policy makes that posture official and adds explicit prioritization criteria.

The compliance ecosystem evolved on the assumption that NVD would remain a comprehensive enrichment source. FedRAMP's Vulnerability Scanning Requirements explicitly direct cloud service providers to use the CVSS v3 base score "assigned in the latest version of the NVD" as the original risk rating for every finding, falling back to CVSS v2 and then to native scanner scores only when no NVD score exists [5]. Continuous monitoring deliverables, Plans of Action and Milestones (POA&Ms), and authorization decisions all reference these scores. Federal Information Security Management Act (FISMA) reporting and U.S. Department of Defense Risk Management Framework (RMF) packages rely on the same assumption.

PCI DSS v4.0.1 takes a more flexible position. Requirement 6.3.1 directs organizations to assign a risk ranking to all newly discovered vulnerabilities and to use a process that includes "industry-recognized practices" — typically interpreted as CVSS-based scoring with NVD as the canonical source, though the standard explicitly allows organization-defined risk ranking so long as "high" and "critical" levels exist at minimum [8]. Approved Scanning Vendor (ASV) external scans operate on a CVSS-4.0-or-higher fail threshold inherited from the ASV Program Guide. ISO/IEC 27001:2022 control 8.8 (Management of Technical Vulnerabilities) and SOC 2 CC7.1 are similarly reliant on a credible vulnerability identification and ranking process; auditors have generally accepted "NVD CVSS score" as the default evidence.

This shared dependency on NVD as the implicit ranking authority is what changes on April 15, 2026. The records that compliance auditors expect to see scored, classified, and product-mapped will, for most new CVEs, arrive with only whatever data the originating CNA chose to publish. Cross-CNA scoring practices vary substantially: studies of historical CVE data show systematic differences of one to two

CVSS points between CNAs scoring functionally similar vulnerabilities, meaning that treating "the CVSS score" as a uniform compliance threshold is increasingly difficult to defend on methodological grounds [9].

Security Analysis

What the April 15 Policy Actually Changes

NIST's announcement defines four operational changes that take effect simultaneously [1]. First, the agency will prioritize enrichment of CVEs in the CISA KEV catalog with a target of one business day, plus CVEs affecting federal software and critical software per Executive Order 14028. Second, all other CVEs are tagged "Lowest Priority — not scheduled for immediate enrichment" and may not receive analyst review at all. Third, all unenriched CVEs with an NVD publish date earlier than March 1, 2026 — approximately 29,000 records — were moved into the "Not Scheduled" category, replacing the previous "Deferred" status and effectively closing out the visible backlog by reclassifying it [3][4][9]. Fourth, when a CNA has already provided a CVSS vector, NIST will no longer routinely produce a separate score; consumers who want NIST to look at a specific record can request it by emailing nvd@nist.gov.

The fields most affected are the ones NIST analysts historically wrote: CVSS v3.1 vectors, CWE problem types, CPE applicability statements, and reference-tag classifications. Where CNAs supply CVSS and CWE in the cvelistV5 source data — true for the majority of 2026 records, as discussed below — those fields persist. Where CNAs do not supply CPE applicability — which describes most CNAs, particularly large vendors and aggregator advisory programs — the resulting CVE record will lack the machine-matchable product and version identifiers that scanners depend on for asset correlation [9]. Independent ecosystem analyses indicate that CPE coverage on new records has fallen substantially since 2022, with current coverage well below historical norms and no other party stepping in to fill the gap [9][10].

Compliance Framework Exposure

The exposure is not uniform across compliance regimes. The table below summarizes where each major framework sits relative to the new NVD posture.

Framework	Explicit NVD Dependency	What Breaks April 15	Practical CISO Action
FedRAMP (Rev 5)	High — CSP scanning requirements direct use of "CVSSv3 base score assigned in the latest version of the NVD" as original risk rating [5]	Most new CVEs will arrive without an NVD-authored CVSSv3 score; POA&M risk ratings must come from CNA or scanner	Document the source-hierarchy fallback; pre-coordinate with 3PAO on accepting CNA scores
FISMA / NIST SP 800-53 RA-5	Medium — references "credible vulnerability sources" without naming NVD	Relies on agency interpretation; ATO packages that named NVD will need addenda	Update RA-5 evidence to list NVD plus CISA KEV plus EPSS as data sources
PCI DSS v4.0.1	Low to medium — Req. 6.3.1 allows organization-defined ranking; ASV scans use CVSS ≥4.0 threshold [8]	Rankings tied to a specific CVSS source need a defensible substitute; ASV outputs unaffected if scanner uses local engine	Document the ranking methodology in writing; cite KEV and EPSS as supplementary inputs
HIPAA Security Rule §164.308(a)(1)(ii)(A)	Low — risk analysis is required, source unspecified	No direct break; expectations of "current vulnerability data" still apply	Show a vulnerability intelligence pipeline that ingests multiple feeds
ISO/IEC 27001:2022 control 8.8	Low — requires "timely information about technical vulnerabilities"	Auditors may probe whether NVD-only feeds remain "timely" given enrichment lag	Add CISA ADP and vendor advisory feeds to the technical vulnerability register
SOC 2 CC7.1	Low — points-in-fact about "configuration standards" and "vulnerabilities"	Service auditors will expect documented response to the policy change	Issue an internal control update note; show evidence of remediation timing tied to KEV inclusion

Framework	Explicit NVD Dependency	What Breaks April 15	Practical CISO Action
DoD RMF / CMMC 2.0	High – vulnerability management practices reference NVD-supplied data and CVSS thresholds	DISA STIG and ACAS workflows depend on enriched NVD content for federal systems	Federal systems remain in NIST's prioritized scope; private contractors must validate their DIB-only inventories

Among civilian programs, FedRAMP is the most exposed, because the Vulnerability Scanning Requirements name NVD explicitly as the canonical CVSS source and bind 30-day, 90-day, and 180-day remediation timelines to High, Moderate, and Low CVSS bands. A vulnerability with no NVD-authored CVSSv3 score, a CNA-authored CVSSv3 vector, and a different scanner-derived score will create a documentation problem unless the cloud service provider has a written, 3PAO-acknowledged source hierarchy. FedRAMP PMO guidance on this question is likely within the next two quarters given typical FedRAMP responsiveness windows, but no timeline has been publicly committed; CSPs should pre-document their interpretation rather than wait for an audit finding. DoD RMF and CMMC 2.0 carry an equivalent dependency in the table, but their exposure is partly offset because federal-software CVEs remain inside NIST's prioritized scope under the new policy – the residual gap falls primarily on private-contractor-only inventories.

PCI DSS programs are less exposed in form but more exposed in practice. Requirement 6.3.1 allows organization-defined ranking, so a written risk-ranking methodology that cites multiple sources (CNA score, KEV inclusion, EPSS probability, CSA-published guidance) is defensible. The operational risk is that automated tooling – particularly Approved Scanning Vendor reports and vulnerability management platforms – was tuned against the assumption that "the CVSS score" was a single number from NVD. Those configurations need re-validation.

What Disappears Versus What Persists

The narrower honest framing is that the April 15 policy completes a redistribution that has been underway since 2022, and the redistributed work is largely intact. CNA-authored CVSS v3.1 coverage has risen substantially since 2020, more than offsetting NVD's decline; total CVSS v3.1 coverage on 2026 records remains above 85% based on independent ecosystem reporting [9][10]. CWE classification has similarly migrated to CNAs without meaningful loss of coverage. CISA's ADP program publishes SSVC decisions on most non-priority CVEs within days of publication and provides CVSS validation for federal-priority software [6]. The EPSS Special Interest Group, hosted by FIRST, publishes daily exploit-

probability estimates for every CVE with a published identifier, and EPSS v4 (released in early 2025) handles CVEs that lack NVD enrichment by using CNA-supplied data plus public exploit-and-PoC signals [7][11].

The genuine gap is CPE applicability. No major actor has stepped in to supply machine-matchable product and version identifiers in a public, free-of-charge feed for the records NVD has stopped enriching; commercial vulnerability intelligence vendors do supply equivalent identifiers in licensed products, but no equivalent free corpus exists. CISOs whose scanners depend on NVD CPE strings to answer "do I have this?" will see scanner coverage degrade for a substantial share of post-April-2026 CVEs — derived from the inverse of the CPE-coverage figure, this is roughly 40% based on early-2026 trend data [9][12]. Programs in this position will need to migrate to Software Bill of Materials (SBOM) reachability analysis or to vendor-direct advisory ingestion.

Recommendations

Immediate Actions (next 30 days)

CISOs should begin with a documentation audit. Identify every governance document, control narrative, scanner configuration, and audit response template that says "NVD CVSS score," "NIST-supplied severity," or any equivalent phrase. Each instance is a structural assumption that no longer holds for most new CVEs. Replace those references with a documented source hierarchy: NIST-enriched score where available, CNA-supplied CVSS where present, EPSS probability and KEV inclusion as orthogonal exploitability inputs, and an organization-defined fallback procedure when none of those produce a confident rating. The cost of pre-documenting this hierarchy is small; the cost of explaining it for the first time during an audit is large.

The second immediate action is a scanner-coverage audit. Vulnerability scanners that derive their match decisions from NVD CPE strings will lose coverage on records published after April 15, 2026 unless the vendor has compensating logic. Operations teams should request from each scanner vendor an explicit statement of which CVE attributes the engine uses for matching, where those attributes come from when NVD is not the source, and what the vendor's plan is for CPE-equivalent identification on unenriched CVEs. Scanner vendors that have already made this transition should be able to answer in writing within days; vendors that cannot are a procurement risk.

The third immediate action is to subscribe operational systems directly to the CISA KEV feed and to EPSS daily updates. KEV inclusion is the single highest-confidence signal that a CVE warrants emergency action, and the new NVD policy explicitly elevates KEV to first-class enrichment status [1].

EPSS provides a probabilistic exploitation forecast that can stand in for CVSS where CVSS quality is uncertain. Both feeds are public and can be ingested without licensing cost.

Short-Term Mitigations (30-180 days)

Programs governed by FedRAMP, FISMA, or DoD RMF should request written acknowledgment from their authorizing officials, 3PAOs, and cognizant compliance bodies that the NVD policy change has been considered in the organization's risk management framework. The right artifact is a brief Plan of Action and Milestones entry or an interim authorization memorandum that documents the source hierarchy in use, the controls compensating for any reduction in NVD-supplied data, and the timeline for any necessary re-baselining once federal compliance bodies issue formal guidance. This is a low-cost defensive action that prevents the policy change from becoming an audit finding by inattention.

PCI DSS programs should formally update their Requirement 6.3.1 risk-ranking methodology document. The methodology should explicitly name the data sources used, describe how the organization weights each source, and include worked examples that show how a CVE with no NVD enrichment is ranked. Approved Scanning Vendor selection and contract negotiation should add language requiring the ASV to disclose whether and how it handles unenriched CVEs in scan reporting.

For all programs, the medium-term priority is to migrate vulnerability triage from CVSS-as-threshold to CVSS-plus-context. The KEV catalog plus EPSS plus internal exposure data — asset criticality, network reachability, compensating controls, and business impact — is the model that vulnerability management practitioners, including CISA, FIRST, and CSA, have been recommending for several years. The April 15 policy makes the transition operationally necessary rather than optional.

Strategic Considerations (180+ days)

CISOs should plan for the new NVD posture to persist. NIST has framed the change as a structural response to volume rather than a temporary triage measure, and the underlying CVE-submission growth is projected to continue. Programs that invest in CSA-aligned vulnerability management practice, SBOM-driven asset correlation, and multi-source intelligence ingestion will be durable across whatever further evolution NVD undergoes. Programs that defer adaptation in the hope of NVD restoration will face increasing audit and operational friction.

Two longer-term opportunities deserve attention. First, organizations that participate in CSA working groups can shape the emerging public response to the enrichment gap; CSA working groups are actively examining community-hosted approaches to fill the CPE applicability shortfall, and practitioners can engage these efforts directly through the STAR program and Top Threats Working Group. Second, organizations subject to international compliance regimes — the EU AI Act, NIS2, India's Digital Personal

Data Protection Act, and similar — should evaluate whether their localized vulnerability-data pipelines depend on NVD-equivalent feeds in their language and jurisdiction; the language and tagging gaps that NVD's retreat exposes are a global problem, not a U.S.-specific one.

CSA Resource Alignment

CSA has anticipated the operational and governance implications of an over-reliance on a single vulnerability data source. The 2024 publication *Top Concerns with Vulnerability Data* explicitly warned that "CVE and CVSS are simply not sufficient for managing the threat intelligence of multiple modern systems on a rolling basis," and identified outdated information, limited context, and inefficient scoring as the most consequential ecosystem weaknesses [13]. The November 2024 CSA research blog *A Vulnerability Management Crisis: The Issues with CVE* extended that argument and previewed the multi-source approach the April 2026 NVD policy now operationally requires [14].

The Cloud Controls Matrix (CCM) Threat & Vulnerability Management (TVM) domain specifies controls that already accommodate a multi-source vulnerability intelligence posture: TVM-04 (External Library Vulnerabilities), TVM-05 (Penetration Testing), and TVM-07 (Vulnerability Identification) all describe processes that reference "credible vulnerability sources" without binding the program to NVD specifically. The AI Controls Matrix (AICM), released in July 2025 with 243 control objectives across 18 domains and explicit mappings to ISO 42001, ISO 27001, and the NIST AI RMF, carries the same TVM domain forward into AI workloads and is the right reference framework for organizations that need to extend vulnerability management into agentic AI, foundation models, and AI supply chain risk [15].

The STAR program's Continuous Auditing Working Group should be a forum for any CSP, scanner vendor, or compliance practitioner who wants to coordinate the documentation updates this policy change requires. CSA's Top Threats Working Group has already begun tracking the policy implications as part of the 2026 update cycle for *Top Threats to Cloud Computing*. Practitioners are encouraged to engage these working groups directly rather than relying on third-party interpretation, which is currently uneven across the security press.

For organizations using AI-assisted vulnerability triage internally, CSA's MAESTRO threat-modeling framework provides agentic-AI-specific guidance on how to evaluate the trustworthiness of AI-derived vulnerability rankings — a question that becomes operationally significant when the underlying CVE data itself is incomplete and AI is filling the gap.

References

[1] National Institute of Standards and Technology. "NIST Updates NVD Operations to Address Record CVE Growth." NIST News, April 15, 2026.

[2] The Hacker News. "NIST Limits CVE Enrichment After 263% Surge in Vulnerability Submissions." The Hacker News, April 17, 2026.

[3] SecurityWeek. "NIST Prioritizes NVD Enrichment for CVEs in CISA KEV, Critical Software." SecurityWeek, April 16, 2026.

[4] Infosecurity Magazine. "NIST Drops NVD Enrichment for Pre-March 2026 Vulnerabilities." Infosecurity Magazine, April 16, 2026.

[5] FedRAMP Program Management Office. "FedRAMP Vulnerability Scanning Requirements, Version 3.0." FedRAMP, February 15, 2024.

[6] Cybersecurity and Infrastructure Security Agency. "Stakeholder-Specific Vulnerability Categorization (SSVC)." CISA, accessed April 26, 2026.

[7] Forum of Incident Response and Security Teams. "Exploit Prediction Scoring System (EPSS)." FIRST, accessed April 26, 2026.

[8] Thoropass. "The PCI Council's Vulnerability Risk Ranking Guidance Changes the Game for Compliance Teams." Thoropass, 2024.

[9] Resilient Cyber. "The NVD Just Threw In The Towel — Now What?." Resilient Cyber, April 22, 2026.

[10] Hive Pro. "The Backlog Became Policy." Hive Pro Threat Intelligence, April 23, 2026.

[11] Risk Based Prioritization Project. "Exploit Prediction Scoring System (EPSS) — Introduction." Open-source documentation, 2025.

[12] Cybersecurity and Infrastructure Security Agency. "Known Exploited Vulnerabilities Catalog." CISA, accessed April 26, 2026.

[13] Cloud Security Alliance. "Top Concerns with Vulnerability Data." CSA, 2024.

[14] Cloud Security Alliance. "A Vulnerability Management Crisis: The Issues with CVE." CSA Blog, November 21, 2024.

[15] Cloud Security Alliance. "AI Controls Matrix (AICM)." CSA, July 2025.

[16] Federal Register. "Executive Order 14028: Improving the Nation's Cybersecurity." Federal Register, May 17, 2021.