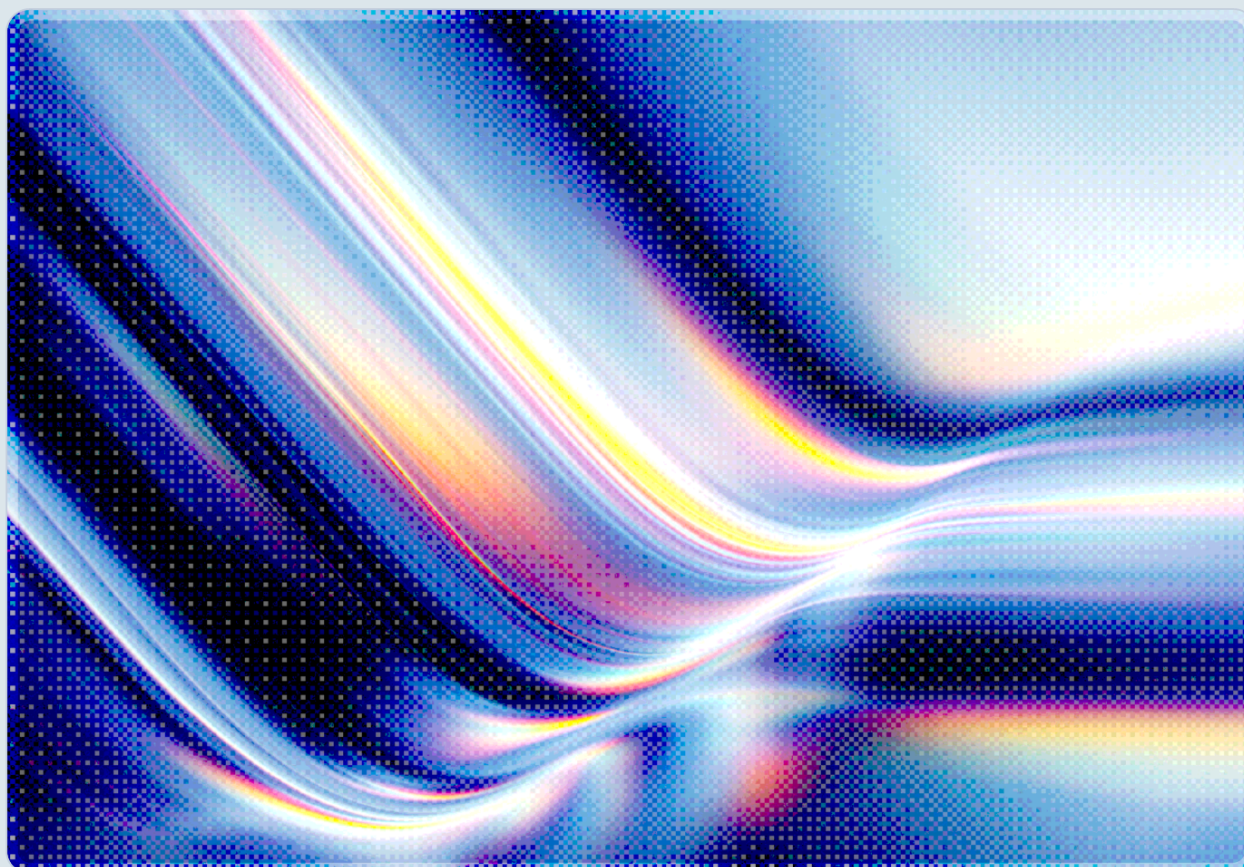


CISA's 'Quality Era' Signals a Structural CVE Program Reset

2026-09-29

 AI-assisted Rapid Research



CSAI

cloud
security
alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

CISA published "CVE Program: Establishing a Quality Era Framework" on September 22, 2026, declaring that the 26-year-old Common Vulnerabilities and Exposures Program is moving from a "Growth Era," defined by expanding the number of participants and records, into a "Quality Era," defined by the reliability, governance, and usability of the data those participants produce [1][2]. The framework organizes this shift around four dimensions, program governance, ecosystem participation, data infrastructure, and CVE record content, and maps them to six existing lines of effort spanning community partnerships, government sponsorship, modernization, transparency, data quality, and the CNA of Last Resort program [4]. The reset arrives as CVE volume has grown sharply: more than 67,000 CVEs had been published by mid-September 2026, with independent forecasters projecting roughly 96,000 by year's end, against a 263 percent increase in submissions between 2020 and 2025 [1][4], growth that CISA's own framework describes as straining the program's prior operating model. Security researchers who reviewed the whitepaper offered measured, not uniformly positive, reactions: several welcomed the acknowledgment that quality depends on governance and infrastructure rather than record volume alone, while others flagged that the document sidesteps the program's most consequential technical gap, the continued absence of machine-readable software identifiers in a large and growing share of new CVE records, and criticized CISA for not publishing the metrics needed to judge whether quality is actually improving [3]. For CSA's constituency, the practical significance is less about any single new control and more about timing: the Quality Era framework lands five months after CISA's Binding Operational Directive 26-04 replaced severity-based patch timelines with risk-based prioritization, and less than a year and a half after the CVE Program itself nearly lost its federal funding, so organizations should treat this as the latest step in a broader, still-unsettled restructuring of how vulnerability data is governed, funded, and consumed rather than as a stable, finished framework.

Background

The CVE Program has functioned since 1999 as the de facto naming and cataloging authority for publicly disclosed software vulnerabilities, operated under a Department of Homeland Security contract with the MITRE Corporation and coordinated through a CVE Board drawn from vendors, researchers, and government stakeholders [7]. That arrangement came under acute strain in April 2025, when MITRE notified the CVE Board that its DHS contract was set to lapse on April 16, 2025, threatening an abrupt

interruption of new CVE assignments and updates across the global vulnerability-management ecosystem [6]. CISA averted the immediate lapse by exercising a contract option hours before expiration, extending funding by roughly eleven months, but the episode exposed the program's dependence on a single national sponsor and prompted a coalition of CVE Board members to establish the CVE Foundation, an independent nonprofit intended to reduce that dependency over the longer term [6][7].

Against that backdrop, the volume the program must process has continued to climb. CISA's own figures put 2026 CVE publication past 67,000 records by September 18, with CVEForecast.org projecting approximately 96,000 by the end of the year, while the National Vulnerability Database recorded a 263 percent increase in submissions between 2020 and 2025 and first-quarter 2026 submissions running roughly a third above the same period the prior year, per Infosecurity Magazine's reporting [1][4]. CISA attributes a substantial share of this acceleration to the expansion of the CNA ecosystem itself, as new CVE Numbering Authorities and Roots join from around the world, combined with AI-enabled tools that are compressing the time between vulnerability discovery and public disclosure [1]. Acting Executive Assistant Director Chris Butera framed the announcement as continuity rather than departure, stating that "CISA remains committed to leading, growing and sustaining the CVE Program into the foreseeable future, just as we've done for more than 25 years" [1][4], a statement of continuity that does not directly address whether the same forces driving growth are also exposing gaps in process and accountability as submission quality becomes uneven.

The Quality Era whitepaper is not CISA's only recent move to recalibrate how vulnerability data drives action. Binding Operational Directive 26-04, effective June 10, 2026, replaced the prior BOD 22-01 and directs federal civilian executive branch agencies to prioritize remediation based on real-world risk factors, including evidence of active exploitation and exposure, rather than CVSS severity scores alone, using a four-variable risk matrix that can compress remediation deadlines to as little as three days for the highest-risk findings [5][13]. CISA reinforced that pivot on September 28, 2026, by discontinuing its long-running weekly vulnerability bulletin, a further signal that the agency appears to intend to steer the ecosystem toward continuously updated, risk-weighted signals such as the Known Exploited Vulnerabilities catalog rather than static, periodic summaries [5]. The CVE Program's governance is also decentralizing beyond CISA and MITRE: the European Union Agency for Cybersecurity, ENISA, expanded during 2026 from a single CVE Root into an organization managing twenty CVE Numbering Authorities, twelve newly onboarded and eight transferred from MITRE, a restructuring that CSA has separately analyzed as a deliberate hedge against concentration risk in the wake of the 2025 funding scare, and one that includes AISLE, the first primarily AI-driven vulnerability discovery firm to receive CNA authority [8]. In CSA's view, read together, the Quality Era framework, BOD 26-04, and the ENISA expansion describe a CVE ecosystem that is simultaneously growing more distributed in who submits records and more centralized in how CISA expects those records to be used for prioritization.

Security Analysis

In CSA's assessment, the Quality Era framework's four dimensions correspond closely to problems the vulnerability-management community has documented for years. CSA's own 2024 research on vulnerability data identified CVSS scoring inconsistency, incomplete or delayed enrichment, and poor interoperability between CVE records and the asset inventories organizations actually use to triage them as structural weaknesses in the ecosystem, well before AI-driven discovery volume made those weaknesses more visible [9]. What has changed since that analysis is less the nature of the defects than their consequence: when tens of thousands of new records arrive annually and a defender's remediation capacity is fixed, an unreliable or incomplete record is no longer a minor annoyance corrected on the next enrichment pass; at current volumes, it risks becoming a triage failure that leaves an exploitable exposure unaddressed. CSA's more recent analysis of AI-accelerated discovery similarly found that National Vulnerability Database enrichment has been unable to keep pace with submission volume, with only a fraction of new CVEs receiving full enrichment shortly after publication, and that the resulting backlog falls into distinct validation, prioritization, and remediation stages that get obscured when organizations track a single "open vulnerabilities" count [10]. CISA's decision to name "data infrastructure" and "CVE record content" as two of its four quality dimensions suggests the agency recognizes this dynamic, but the whitepaper as published does not specify the metrics, staffing, or timelines that would demonstrate progress, an omission that several reviewers raised directly.

Reactions from the security community reflect that gap between stated intent and demonstrated capability. Brian Fox, co-founder and CTO of Sonatype, credited CISA for extending its definition of quality beyond the individual record to governance, infrastructure, and participation, but was explicit that he would consider the Quality Era genuinely underway only once the improvement is visible in the data itself, not merely described in a framework document [3]. Caitlin Condon, vice president of security research at VulnCheck, characterized the whitepaper as a preliminary statement of intent rather than a comprehensive plan, noting that CISA already has the ability to measure and publish many of the success metrics implied by the framework but has chosen not to make that data public, which limits the ecosystem's ability to independently verify whether the Quality Era is producing results [3]. Tom Alrich, who leads the OWASP PURL Expansion Working Group, raised a more specific and, for enterprise vulnerability management, more consequential objection: a large and growing share of new CVE records still lack a machine-readable software identifier such as a Package URL, which means automated matching between a CVE record and the specific software components an organization runs remains unreliable regardless of how well-governed the program's other processes become [3]. That gap sits squarely inside the "CVE record content" dimension the framework itself names, and its absence from the published document suggests CISA's initial framing may prioritize organizational and procedural quality over the specific data-format problem that most directly determines whether automated vulnerability-management tooling can act on a record without manual verification. Russel Van Tuyl of

SpecterOps offered a more favorable read, noting that the framework at least connects better vulnerability data explicitly to faster coordination, a linkage that has often been treated as two separate problems in prior CVE Program communications [4].

For CSA's constituency, the operational risk in the near term is not that the Quality Era framework introduces a new compliance obligation, it does not, but that it signals a period of continued flux in the data federal risk-prioritization guidance depends on. BOD 26-04's four-variable risk matrix and the KEV catalog it prioritizes are, by construction, only as reliable as the CVE records feeding them; the Known Exploited Vulnerabilities catalog stood at roughly 1,705 entries as of September 2026 [5], yet Verizon's 2026 Data Breach Investigations Report found that full remediation of KEV-listed vulnerabilities fell to 26 percent in 2025, down from 38 percent the prior year, with median resolution time rising from 32 to 43 days [12]. That decline occurred even as CISA was narrowing its own directive language toward risk-based prioritization, which suggests the operational bottleneck for most organizations is not which scoring model CISA endorses but the industrial capacity to validate, test, and deploy patches at the rate new findings arrive, a constraint that a governance-focused whitepaper cannot resolve on its own [10]. Organizations that treat the Quality Era announcement as evidence the underlying data problem is being solved, rather than as a roadmap for solving it, risk under-investing in the internal triage and validation capacity that current remediation statistics show is still the limiting factor.

Recommendations

Immediate Actions

Security and vulnerability-management teams should not change existing CVE-consumption workflows on the basis of the Quality Era whitepaper alone, since it commits to no new data formats, SLAs, or enrichment guarantees that would justify a process change; instead, teams should continue prioritizing remediation using the risk factors named in BOD 26-04, active exploitation, public exposure, and exploitation automation potential, rather than reverting to CVSS-only triage. Teams should also confirm that their vulnerability-management tooling and processes do not assume complete or timely NVD enrichment, since the enrichment backlog CSA's own research has flagged predates and is not resolved by this whitepaper, independent of the separate machine-readable identifier gap Tom Alrich raised [10].

Short-Term Mitigations

Organizations should audit how much of their vulnerability-matching pipeline depends on machine-readable software identifiers, such as Package URLs or CPE strings, versus manual mapping from CVE descriptions to installed software, since Alrich's criticism of the framework indicates this gap is likely to persist through at least the next several quarters of CVE Program evolution. Where CVE records lack usable identifiers for critical or internet-facing software, organizations should supplement CVE-based triage with vendor advisories, software bills of materials, and exploit-intelligence feeds rather than waiting on record-level fixes the framework does not yet commit to a timeline for. Security leaders briefing executives or boards on vulnerability-management posture should also distinguish clearly between CISA's stated intent to improve CVE data quality and the absence of published metrics demonstrating that improvement, consistent with Caitlin Condon's observation that current performance data exists but is not yet public.

Strategic Considerations

Over the coming year, CSA's constituency should watch three developments that will determine whether the Quality Era framework produces measurable change: whether CISA follows the whitepaper with published metrics on record completeness, enrichment timeliness, and CNA data quality, as VulnCheck has called for; whether the CVE Program's governance continues to decentralize through mechanisms like ENISA's expanded CNA authority and the CVE Foundation, which would reduce single-sponsor risk but could also introduce inconsistency in record quality across Roots during a transition period; and whether CISA addresses the machine-readable identifier gap that Alrich identified, since that gap, more than any governance structure, determines whether automated vulnerability-management tooling can act on new CVE records without manual intervention. Organizations building longer-term vulnerability-management strategy should treat the current CVE ecosystem as being in transition on funding, governance, and data-format dimensions simultaneously, and should design triage and remediation processes that do not assume any single source, whether the NVD, a specific CNA, or CISA's own KEV catalog, will remain the sole or most current source of prioritization signal.

CSA Resource Alignment

This research note builds directly on four pieces of recent CSA analysis. CSA's research note "ENISA Restructures CVE Governance for the AI-Discovery Era" examined the same underlying dynamic from a different vantage point, documenting how ENISA's expansion to twenty CVE Numbering Authorities and the onboarding of AI-native discovery firms such as AISLE represents a parallel, non-U.S. response to

the capacity and concentration-risk pressures that also motivate CISA's Quality Era framework [8]. Readers evaluating whether CISA's governance and ecosystem-participation dimensions are likely to succeed should read that note alongside this one, since it provides a concrete case study of multi-root CNA expansion already underway.

CSA's research note "CISA's BOD 26-04: A Risk-Based Reset of Patch Rules" provides the direct primary-source analysis of the four-variable risk matrix and remediation-tier structure this note references in Background and Security Analysis, and readers seeking the full mechanics of that directive, including how its sixteen variable combinations map to five remediation tiers, should treat that note as the authoritative CSA reference rather than the third-party compliance summaries cited alongside it here [13].

CSA's 2024 research report "Top Concerns With Vulnerability Data" remains the most relevant CSA foundation for the "CVE record content" dimension of CISA's framework specifically, having identified CVSS scoring inconsistency, incomplete enrichment, and poor interoperability between CVE records and downstream tooling as structural weaknesses well before the current volume surge made them acute [9]. The gap Tom Alrich raised regarding machine-readable software identifiers is a direct extension of the interoperability concerns that report catalogued, and organizations should treat that CSA analysis as a checklist against which to measure whatever record-content commitments CISA eventually publishes.

CSA's whitepaper on AI-accelerated vulnerability discovery and the patch-debt crisis provides the operational counterpart to CISA's governance framework, analyzing how the same submission-volume growth CISA cites, driven substantially by autonomous and AI-assisted discovery tools, is outstripping enterprise and open-source patch capacity regardless of how well the CVE Program itself is governed [10]. That analysis reinforces the recommendation in this note that organizations should not expect improved CVE Program governance to resolve their own remediation bottleneck, since discovery volume and remediation capacity are governed by largely independent constraints. Finally, CSA's AI Controls Matrix version 1.1, in its Threat and Vulnerability Management domain, offers the most directly applicable standing framework for organizations formalizing how AI-influenced vulnerability data, whether from AI-native CNAs, AI-assisted discovery tools, or AI-driven triage systems, should be governed within an existing security-control program [11].

References

- [1] Cybersecurity and Infrastructure Security Agency. "[CISA Whitepaper Charts Path to Establishing and Maturing CVE Program Quality](#)." CISA, September 22, 2026.
- [2] Cybersecurity and Infrastructure Security Agency. "[CVE Program: Establishing a Quality Era Framework](#)." CISA, September 22, 2026.
- [3] CyberScoop. "[CISA outlines improvement plan for CVE program](#)." CyberScoop, September 2026.
- [4] Infosecurity Magazine. "[CISA Charts New 'Quality Era' for Global CVE Program](#)." Infosecurity Magazine, September 2026.
- [5] ComplianceHub.Wiki. "[CISA's New CVE Program 'Quality Era': Changes to Vulnerability Disclosure Compliance](#)." ComplianceHub.Wiki, September 2026.
- [6] Nextgov/FCW. "[CISA extends MITRE-backed CVE contract hours before its lapse](#)." Nextgov/FCW, April 16, 2025.
- [7] CVE Foundation. "[CVE Foundation Launched to Secure the Future of the CVE Program](#)." CVE Foundation, April 16, 2025.
- [8] Cloud Security Alliance. "[ENISA Restructures CVE Governance for the AI-Discovery Era](#)." CSA, August 11, 2026.
- [9] Cloud Security Alliance. "[Top Concerns With Vulnerability Data](#)." CSA, 2024.
- [10] Cloud Security Alliance. "[The Bugpocalypse Threshold: AI-Accelerated Vulnerability Discovery and the Patch Debt Crisis](#)." CSA, May 21, 2026.
- [11] Cloud Security Alliance. "[AI Controls Matrix \(AICM\) v1.1](#)." CSA, 2026.
- [12] Verizon. "[2026 Data Breach Investigations Report](#)." Verizon Business, 2026.
- [13] Cloud Security Alliance. "[CISA's BOD 26-04: A Risk-Based Reset of Patch Rules](#)." CSA, August 20, 2026.