CSAI

cloud security alliance®

CSAI Foundation

Cloud Security Alliance AI Safety Initiative

CISA at 38%: Navigating the Enterprise Guidance Vacuum

Practical Guidance for Security Teams as Federal Cybersecurity Capacity Contracts

Unofficial AI-assisted Research

2026-04-23

Key Takeaways

- On February 14, 2026, a DHS appropriations lapse triggered the furlough of 62% of CISA's workforce, reducing the agency to approximately 888 operational staff — 38% of its pre-shutdown complement — and suspending proactive vulnerability scanning, stakeholder outreach, and most preparatory planning activity [1].
- CISA's workforce was already significantly diminished before the shutdown: from approximately 3,300 employees when the Trump administration took office in January 2025, the agency had contracted to roughly 2,400 by late 2025 through a combination of DOGE-driven reductions in force and voluntary departures, losing many senior career officials [2][3].
- The Multi-State Information Sharing and Analysis Center (MS-ISAC), which previously provided federally subsidized cybersecurity services to more than 18,000 state, local, tribal, and territorial organizations, lost its CISA cooperative agreement on September 30, 2025, and has since transitioned to a paid membership model, creating cost barriers for precisely the entities with the smallest security budgets [4][5].
- Finalization of the CIRCIA cyber incident reporting rule — which would impose mandatory 72-hour notification requirements on critical infrastructure operators across 16 sectors — has stalled; scheduled industry town halls for March through April 2026 were cancelled due to the shutdown, further delaying a rule already pushed to May 2026 [6][7].
- The National Vulnerability Database (NVD) simultaneously shifted to a selective CVE enrichment model in April 2026, prioritizing only KEV-listed, federal-use, and critical-software vulnerabilities, degrading the free, comprehensive enrichment data that enterprise vulnerability management programs have long relied upon [8][9].
- Security teams should treat the federal guidance infrastructure as materially degraded for an indeterminate period and take immediate steps to diversify threat intelligence sources, operationalize direct KEV integration, and join sector-specific information-sharing communities.

Background

For more than a decade, the Cybersecurity and Infrastructure Security Agency has served as the primary interface between the federal government and private-sector security organizations. Its role spans multiple functions that enterprises increasingly treat as utility services: the Known Exploited Vulnerabilities (KEV) catalog, which provides a curated and operationally prioritized list of actively exploited CVEs; joint cybersecurity advisories co-authored with the NSA, FBI, and international partners; binding operational directives and emergency directives for federal agencies; proactive vulnerability scanning for critical infrastructure operators; and the CIRCIA incident reporting program, which would extend mandatory cyber disclosure obligations to more than 300,000 private entities. For many organizations, particularly those in regulated critical infrastructure sectors, CISA has functioned as the authoritative backstop against which their own security programs are calibrated.

The agency's operational capacity began contracting in January 2025. When the Trump administration took office, CISA employed approximately 3,300 personnel [2]. The Department of Government Efficiency (DOGE) initiative and two DHS voluntary buyout offers drove significant attrition over the following months. By the time the DHS appropriations lapse began in February 2026, CISA's headcount had already fallen to approximately 2,341, with roughly one-third of its staff having departed in just over a year — including many experienced senior leaders who carried institutional knowledge of sector-specific threat environments and longstanding industry relationships [1][2].

The February 14, 2026, shutdown deepened the crisis. CISA's contingency plan designated only 888 employees as excepted from furlough — those directly supporting active national security and emergency response operations [1]. The remaining 1,453 employees, representing the teams responsible for outreach, preparatory planning, regulatory development, training, and stakeholder engagement, were sent home. In April 2026, approximately 1,200 of those furloughed staff were recalled to work, but CISA's director acknowledged that resources remained "more limited than I would like" and that the agency is still legally prohibited from engaging in certain outreach activities while the appropriations lapse persists [10][11].

Compounding the institutional disruption, CISA's director nominee, Sean Plankey, withdrew from consideration in April 2026, leaving the agency without confirmed permanent leadership at a period of significant operational stress [12]. The FY2026 budget proposal before Congress would reduce CISA's funded positions from 3,732 to 2,649 — a cut of roughly 1,000 positions and $495 million — while the FY2027 proposal, submitted separately by the administration, would cut an additional $707 million and eliminate CISA's election security program entirely [13][14].

Security Analysis

The Scope of the Guidance Gap

The most immediate operational consequence of CISA's reduced capacity is a measurable decline in the frequency and depth of proactive security guidance. Proactive vulnerability scanning of federal networks and critical infrastructure — a service offered at no charge to qualifying organizations — has stopped [1]. Advisory output, while still occurring through the KEV catalog and some joint advisories, reflects a fraction of the agency's prior production capacity. The CISA director has confirmed that "a lot of the preparatory activities and outreach that we would typically be able to do, that's simply not possible or legally allowed during the period of a shutdown" [11].

This matters for enterprise security programs because CISA's guidance has historically served two distinct functions. The first is operational: advisories and the KEV catalog translate raw CVE data into prioritized, context-rich remediation guidance that organizations with limited threat intelligence capacity use to triage their patching programs. The second is normative: CISA's documented best practices and sector-specific guidance provide a defensible external standard that security teams use to justify resource allocation, satisfy audit requirements, and establish organizational baseline expectations. Both functions are impaired by the current environment.

Advisory distribution practices have been unstable even outside the shutdown period. In May 2025, CISA announced plans to significantly alter how it shares cybersecurity updates, triggering concern in the security community; the agency subsequently reversed its position following public backlash from security professionals and operational stakeholders [15][16]. The episode signaled organizational instability in one of CISA's most operationally critical functions before the shutdown began.

CIRCIA's Compliance Deadline Uncertainty

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) represents the most significant expansion of federal cyber disclosure obligations in decades. The statutory framework would require covered entities to notify CISA within 72 hours of discovering a significant cyber incident and within 24 hours of making a ransom payment [7]. CISA has estimated that the final rule, once published, will apply to more than 300,000 organizations across 16 critical infrastructure sectors.

The rule's finalization has been a casualty of CISA's capacity constraints. Originally due in October 2025, the deadline was extended to May 2026 [17]. The DHS shutdown then eliminated the industry town halls scheduled for March through April 2026, at which CISA was expected to present its revised scope determinations and collect final stakeholder comment [6]. The shutdown further paused the regulatory

staff work needed to finalize the rule itself [7]. Legal and compliance observers have noted that continued appropriations lapses will "likely result in a delay to the issuance of the final rule," though no revised deadline has been announced [7].

For enterprise compliance teams, this creates a difficult planning environment. Organizations subject to CIRCIA cannot complete their compliance gap assessments against a finalized rule text; cannot calibrate their incident notification workflows to confirmed deadlines; and cannot rely on the previously scheduled public engagement process to surface interpretive guidance on scope and definitional questions. Compliance planning must proceed under significant regulatory uncertainty, with organizations advised to build CIRCIA-ready reporting infrastructure regardless of the final publication timeline.

The MS-ISAC Transition and the SLED Security Gap

Among the changes with the most direct operational impact on public-sector organizations, the end of CISA's cooperative agreement with the Center for Internet Security (CIS) for the Multi-State Information Sharing and Analysis Center stands out. For many years, CISA's annual cooperative agreement with CIS subsidized MS-ISAC services for state, local, tribal, and territorial (SLTT) governments at no cost to members. Those services included 24/7 security operations center monitoring, threat intelligence sharing, incident response coordination, and vulnerability scanning — the equivalent of an enterprise-grade security program offered to organizations that often lack the budget or staff to build one independently [4][5].

That cooperative agreement expired on September 30, 2025 [4]. The MS-ISAC has since transitioned to a fee-based membership model [18], with the lowest-cost tier serving organizations with annual budgets under $25 million at $1,495 per year — a new direct cost for organizations that previously received these services at no charge under the federal cooperative arrangement [22]. The federal State and Local Cybersecurity Grant Program, which might logically fund these memberships, has been explicitly barred from covering MS-ISAC membership fees [5]. The result is that many of the 18,000-plus organizations that previously benefited from subsidized MS-ISAC services face a choice between absorbing a new membership cost or losing access to a core intelligence and monitoring service at a moment when the federal government is providing less direct support, not more.

NVD Selective Enrichment and the Vulnerability Intelligence Gap

The National Vulnerability Database, operated by NIST, has long been the authoritative, freely available source of enriched CVE metadata — CPE designations, CVSS scoring, CWE classification, and cross-reference links — that vulnerability management platforms and security tools depend on to provide

actionable context around raw CVE identifiers. In April 2026, NIST changed its enrichment policy in response to a 263% surge in CVE submissions between 2020 and 2025, a volume that NIST's flat funding could not support [8][9].

Under the new policy effective April 15, 2026, NIST will prioritize CVE enrichment for vulnerabilities in the CISA KEV catalog, software used by the federal government, and software designated as critical under Executive Order 14028 [8]. All other CVEs will be listed in the NVD without detailed enrichment unless specifically requested. NIST noted it enriched nearly 42,000 CVEs in 2025 — 45% more than any prior year — but that this output remains insufficient to keep pace with submission volumes [8]. The change effectively converts the NVD from a comprehensive enrichment service into a triage queue, concentrating its limited resources on the highest-priority subset of the CVE universe.

For enterprise vulnerability management programs that rely on NVD enrichment to automate severity scoring and patching prioritization, the practical consequence is a growing portion of the CVE inventory that will arrive without CVSS scores, CPE identifiers, or CWE classifications — at least initially. Organizations will need to either supplement NVD data with commercial enrichment sources or accept reduced automation fidelity for the long tail of lower-priority CVEs.

Information Sharing Legal Framework Uncertainty

A less widely discussed but legally significant complication arose on October 1, 2025, when the Cybersecurity Information Sharing Act of 2015 (CISA 2015) lapsed without immediate reauthorization. CISA 2015 provides the primary legal authorization framework under which private organizations share cyber threat indicators with the federal government and each other, with associated liability protections that are essential to voluntary information sharing programs. The lapse created temporary uncertainty about the legal basis for certain sharing activities [19]. Congress subsequently re-authorized CISA 2015 through September 30, 2026, as part of the Consolidated Appropriations Act of 2026, signed February 3, 2026 [20], but the episode highlighted the fragility of the legal infrastructure underlying public-private information sharing — and the likelihood that this authorization will again require renewal before the end of 2026.

Recommendations

Immediate Actions

Security teams should not wait for CISA's capacity to recover before adapting their programs. The immediate priority is reducing single-source dependency on federal guidance infrastructure. Organizations relying primarily on CISA advisories for vulnerability prioritization should integrate the KEV catalog directly via its machine-readable JSON feed, available at CISA's website, rather than depending on downstream advisory summaries that may be slower or less complete during periods of reduced staff [21]. The KEV catalog remains one of CISA's most consistently maintained outputs and represents the highest-confidence signal for prioritizing active exploitation risk.

Organizations that were relying on free CISA proactive scanning services should initiate commercial or open-source alternatives for external attack surface monitoring. Several vendor platforms offer continuous external exposure assessment, and open-source tools such as Shodan and Censys provide partial coverage for internet-exposed assets. Internal vulnerability scanning cadences should be reviewed to confirm they do not depend on CISA-delivered scanning reports.

For SLTT organizations that were MS-ISAC members under the federally subsidized model, evaluating membership under the new paid structure is urgent. The new membership cost may still represent favorable economics relative to the alternatives for organizations without in-house SOC capability. For organizations that can absorb the fee, core MS-ISAC services — including 24/7 SOC monitoring, threat intelligence sharing, and incident response coordination — remain available through CIS [22]. Organizations that cannot absorb the cost should explore whether sector-specific ISACs in their functional domain offer equivalent services at different price points.

Short-Term Mitigations

CIRCIA compliance planning should continue regardless of the final rule's publication date. The 72-hour notification and 24-hour ransom payment reporting requirements reflect reasonable operational response targets that align with existing incident response best practices. Building and tabletop-testing these workflows now — against the published proposed rule and available CISA guidance — reduces the compliance gap that will need to close when the final rule does publish. Organizations that choose to report incidents to CISA voluntarily in the interim gain the dual benefit of familiarizing their teams with the reporting process and contributing to the threat intelligence ecosystem during a period when that ecosystem is under pressure.

For vulnerability management programs affected by NVD's selective enrichment policy, security teams should evaluate commercial CVE enrichment platforms including those from Tenable, Qualys, Rapid7, and others that maintain independent enrichment pipelines. These platforms continue to provide full CVSS scoring and contextual metadata independent of NVD's enrichment cadence. Organizations with significant open-source software exposure should also review the CVE Foundation's independent CVE numbering authority structure, which operates separately from NIST's enrichment workflow and continues to issue CVEs regardless of NVD enrichment delays.

Sector-specific ISACs represent an increasingly important channel for actionable threat intelligence sharing. The Financial Services ISAC (FS-ISAC), Health-ISAC, and similar sector bodies have historically complemented CISA's cross-sector work and now serve as more reliable sources of timely, sector-tailored intelligence than the reduced federal program can currently provide. Organizations not already participating in their sector ISAC should prioritize joining.

Strategic Considerations

The sustained reduction in CISA capacity — which has been in progress for over a year and reflects both a specific administration's policy priorities and a structural underfunding trend that predates the current administration — warrants strategic reassessment of how enterprise security programs are architected around federal resources. Programs that have used CISA guidance as their primary normative standard should develop independent governance frameworks that define security requirements based on the organization's own risk profile, drawing on multiple external standards including NIST CSF 2.0, ISO 27001, and sector-specific frameworks, rather than remaining dependent on a federal advisory cadence that may be intermittent.

The FY2027 budget proposal — which would cut an additional $707 million from CISA and eliminate major programs — suggests that even if the current appropriations situation is resolved, CISA's long-run capacity to deliver the breadth of services it has historically provided is not assured [14]. Security executives should communicate this risk explicitly to board and executive leadership, framing the investment in independent threat intelligence, information sharing memberships, and internal security program maturity as a hedge against continued federal capacity contraction, not a temporary gap-fill.

CSA Resource Alignment

This situation directly engages several dimensions of CSA's published guidance frameworks. The MAESTRO threat modeling methodology for agentic and AI-enabled systems emphasizes the importance of continuous, authoritative threat intelligence as a prerequisite for accurate threat

modeling; degradation of the federal advisory infrastructure represents a structural impairment to the MAESTRO input layer for any organization that has built its threat model around CISA guidance as a primary signal source.

The Cloud Controls Matrix (CCM) and the AI Controls Matrix (AICM) address threat and vulnerability management under control domains including TVM (Threat and Vulnerability Management) and GRC (Governance, Risk, and Compliance). The current environment does not reduce the compliance obligations under these frameworks but does alter the recommended evidence sources. Organizations mapping to CCM TVM controls should document their use of multiple supplementary sources — sector ISACs, commercial threat feeds, direct KEV integration, independent NVD enrichment — to demonstrate continued rigor in the absence of full CISA advisory coverage.

CSA's Zero Trust guidance and its AI Organizational Responsibilities publications both emphasize the operational principle that security posture must be maintained regardless of external guidance availability. The CISA capacity contraction is a live test of this principle: organizations whose security programs depend structurally on federal guidance availability will experience degraded posture; those that have built independent program governance will be less exposed. CSA's STAR for AI Catastrophic Risk Annex initiative — focused on the highest-consequence end of organizational risk — similarly assumes that organizations cannot delegate their threat awareness function to any single external authority.

References

[1] Nextgov/FCW. "CISA to furlough most of its workforce under impending DHS shutdown." February 2026.

[2] Axios. "One-third of U.S. cyber agency CISA has left since Trump took office." June 2025.

[3] Nextgov/FCW. "CISA projected to lose a third of its workforce under Trump's 2026 budget." June 2025.

[4] Infosecurity Magazine. "US Cuts Federal Funding for MS-ISAC Cybersecurity Program." 2025.

[5] Cybersecurity Dive. "Federal cuts force many state and local governments out of cyber collaboration group." 2025.

[6] Federal News Network. "CISA delays cyber incident reporting town halls due to shutdown." March 2026.

[7] Bloomberg Government. "Shutdown Stalls Compliance Plans for Cyber Breach Reporting Rule." 2026.

[8] NIST. "NIST Updates NVD Operations to Address Record CVE Growth." April 2026.

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

[10] GovInfoSecurity. "CISA Workers Recalled Despite Shutdown." April 2026.

[11] Nextgov/FCW. "CISA resources 'more limited than I would like' amid shutdown, top official says." April 2026.

[12] Federal News Network. "Plankey withdraws as CISA nominee." April 2026.

[13] Cybersecurity Dive. "Trump's CISA budget lays out deep job cuts, program reductions." 2025.

[14] The Next Web. "Trump's FY27 budget would cut $700M from CISA and kill election security." 2026.

[15] CISA. "Update to How CISA Shares Cyber-Related Alerts and Notifications." May 2025.

[16] Infosecurity Magazine. "CISA Reverses Decision on Cybersecurity Advisory Changes." 2025.

[17] CyberScoop. "CISA pushes final cyber incident reporting rule to May 2026." 2025.

[18] StateTech Magazine. "States Step Up as MS-ISAC Moves to Paid Model After Federal Funding Ends." February 2026.

[19] Morrison Foerster. "Can Cyber Threat Intelligence Sharing Continue After CISA 2015's Lapse?" October 2025.

[20] Davis Wright Tremaine. "Congress Extends CISA 2015 Through September 2026." February 2026.

[21] CISA. "Known Exploited Vulnerabilities Catalog." Continuously updated.

[22] Center for Internet Security. "MS-ISAC Membership." Continuously updated.