CSAI Foundation

Cloud Security Alliance AI Safety Initiative

CISA Governance Disruption: Enterprise Cybersecurity Implications

Navigating Reduced Federal Oversight and the Erosion of the U.S. Cybersecurity Safety Net

Unofficial AI-assisted Research

2026-04-09

Key Takeaways

- The Cybersecurity and Infrastructure Security Agency (CISA) has lost roughly one-third of its workforce over the past 14 months, with staffing falling from approximately 3,400 employees at the start of fiscal year 2025 to around 2,341 by early 2026, compounded by a February 2026 DHS funding lapse that furloughed an additional 1,453 staff — leaving the agency operating approximately 888 essential personnel, roughly 38% of its already-reduced workforce and approximately 26% of original authorized strength [1][2][3].
- Programs that enterprises and critical infrastructure operators have routinely relied upon — including CISA's red team, continuous monitoring operations, incident response cadre, pre-ransomware notification initiative, and the Election Security Program — have been significantly curtailed or lost key personnel, with the FY2027 administration budget proposing a further $707 million in cuts [4][5][6].
- The February 2026 DHS shutdown forced CISA to cancel physical and cyber assessments, halt vulnerability scanning for critical infrastructure, and postpone planned stakeholder forums on the forthcoming Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) final rule, which has been pushed to May 2026 at the earliest [7][8].
- The near-lapse of CISA's contract with MITRE to fund the Common Vulnerabilities and Exposures (CVE) program in April 2025 — averted only by an 11th-hour 11-month extension — exposed a fragility in the global vulnerability management ecosystem that enterprises had long treated as stable infrastructure rather than a contingency dependent on annual contract renewal [9].
- The operational disruptions documented here mean that organizations can no longer treat CISA services as a reliable backstop for threat intelligence, incident response surge capacity, and vulnerability guidance — a changed risk environment that warrants explicit governance attention and compensating investment.

Background

Since January 2025, CISA has undergone the most significant staffing and budgetary disruptions the agency has experienced since its establishment in 2018. The agency was created with a mandate to protect federal civilian networks and serve as the primary national coordinator for critical infrastructure cybersecurity. In that role, it grew to roughly 3,400 employees and operated dozens of programs that the private sector, state and local governments, and critical infrastructure operators came to depend on either directly or indirectly.

Beginning in early 2025, the Department of Government Efficiency (DOGE) initiative drove rapid workforce reductions across the federal government. CISA was among the most heavily affected agencies within DHS. In the initial wave, DOGE terminated contracts and eliminated staff in ways that effectively dismantled several operationally critical units: CISA's entire red team was eliminated, along with more than 80 employees working in continuous monitoring and between 30 and 50 staff handling incident response [4][10]. These were not administrative positions — they represented CISA's most technically specialized and operationally consequential capabilities.

Through voluntary buyouts, deferred resignations, and directed terminations, headcount continued to fall throughout 2025. By the time the Trump administration's FY2026 budget request was submitted in May 2025, the proposal called for cutting a further 1,000 positions from the 3,732 authorized at the start of the administration — which would have brought CISA to roughly 2,649 funded positions, reflecting both prior DOGE-driven attrition and the proposed additional reductions [11]. (The agency's funded position count at the start of the administration was approximately 3,732 [11], while actual on-board headcount at the start of FY2025 was approximately 3,400 [1].) Congress moderated the cut somewhat; the House homeland security subcommittee passed a 4.6% reduction ($134 million) rather than the proposed 17% ($491 million) [12]. The FY2027 budget subsequently proposed an even deeper cut of $707 million and the elimination of 860 additional positions, including the complete elimination of the Election Security Program [5][13].

The operational disruption reached a new threshold on February 14, 2026, when the DHS appropriation lapsed and a government shutdown took effect. CISA, already operating at reduced strength, furloughed 1,453 of its 2,341 remaining employees — roughly 62% of the workforce — and continued partial operations with just 888 essential personnel [2][3]. Critical infrastructure assessments, simulation exercises, and vulnerability scanning programs were suspended. Within weeks, a March 11, 2026 breach of Stryker Corporation by the Iranian-linked group Handala occurred while CISA was operating at a fraction of normal capacity. Whether CISA's reduced capacity affected that specific outcome cannot be established from available information, but the concurrence illustrates the risk environment enterprises face when federal cybersecurity support is severely constrained [3].

Security Analysis

The Erosion of the Federal Cybersecurity Safety Net

For most of its history, CISA functioned less like a traditional regulator and more like a shared services provider for national cybersecurity resilience. Its advisories on actively exploited vulnerabilities — codified in the Known Exploited Vulnerabilities (KEV) catalog — became an industry-standard input for vulnerability prioritization. Its ICS security advisories guided operators of industrial control systems who lacked the internal expertise to evaluate proprietary vendor disclosures. Its Automated Indicator Sharing (AIS) service pushed machine-readable threat intelligence directly to participating organizations. Its pre-ransomware notification initiative, which alerted victim organizations that ransomware deployment appeared imminent, represented a form of early warning with no direct commercial equivalent.

Each of these services operated at a scale and cost structure that most enterprises — and virtually all smaller organizations such as municipalities, rural electric cooperatives, community hospitals, and water utilities — could not individually replicate. Those smaller entities relied on CISA not as an option but as their primary cybersecurity resource. The reductions of the past 14 months have not redistributed this capability — they have severely degraded it, with some programs eliminated outright and others continuing at a fraction of prior capacity. An agency operating at $2 billion with 860 fewer staff will almost certainly produce fewer advisories, respond to fewer incidents, and reach fewer of the operators it was designed to support [5][6].

The departure of David Stern, the operational lead behind the Pre-Ransomware Notification Initiative, illustrates the human dimension of the disruption. While CISA stated that the program "has not stopped and continues to operate," the loss of institutional expertise in operationally complex programs seldom corresponds cleanly to the formal headcount numbers — program effectiveness often depends on specific individuals and accumulated organizational knowledge that is difficult to replace [14]. Similar attrition risks affect the agency's ICS advisory program, its Secure by Design initiative, and its threat hunting and vulnerability disclosure functions.

Regulatory Uncertainty and CIRCIA

For enterprises in critical infrastructure sectors, the most consequential near-term governance disruption may be the regulatory uncertainty surrounding CIRCIA. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 requires CISA to promulgate rules mandating that covered entities

report significant cyber incidents within 72 hours and ransomware payments within 24 hours. The proposed rule was projected to apply to more than 300,000 entities across 16 critical infrastructure sectors [8].

The final rule, already delayed from an earlier target of October 2025 to May 2026, has been further disrupted by the DHS shutdown: CISA postponed stakeholder town halls scheduled for early 2026, and the shutdown has made it likely the May 2026 deadline will also slip [7][8]. This creates a compliance planning problem. Organizations subject to CIRCIA face the dual burden of preparing for a rule whose final shape remains unknown while simultaneously building the internal capabilities — log retention, incident classification, legal coordination, and regulatory reporting workflows — that compliance will require regardless of the precise timeline. The governance disruption at CISA does not remove the compliance obligation; it merely reduces the government's ability to help regulated entities prepare for it.

Vulnerability Management Infrastructure at Risk

The April 2025 CVE program funding crisis brought a different dimension of the problem into relief. On April 15, 2025, DHS failed to renew its contract with MITRE for the CVE program — the foundational infrastructure through which security vulnerabilities are tracked, numbered, and publicly disclosed worldwide — and the program faced shutdown within approximately 36 hours. CISA reversed course approximately 17 hours after the contract lapse became public — well within the window before program operations would have ceased — executing an 11-month extension [9]. But the episode revealed that what the global security industry had widely assumed to be permanent infrastructure was in fact a contract relationship that could lapse without warning.

The National Vulnerability Database (NVD) at NIST experienced a separate but related crisis. An analysis backlog had already developed at NVD by 2024; CISA's subsequent pause of $3.7 million in annual NVD funding compounded this pre-existing problem, leaving organizations uncertain whether published CVEs had complete enrichment data — the CVSS scores, CPE identifiers, and CWE classifications needed for automated vulnerability management tooling [15][16]. CISA subsequently launched a Vulnrichment program as a stopgap, but the underlying funding instability for these shared public goods has not been resolved. An 11-month CVE contract extension is not the same as a durable commitment, and enterprises whose vulnerability management workflows depend on the CVE and NVD ecosystem should treat that dependency as a material risk.

Information Sharing Deterioration

The Cybersecurity Information Sharing Act of 2015 (CISA-Act), which underpins the legal framework for the AIS program and the liability protections that encourage private-sector information sharing with the federal government, was temporarily reauthorized only through a continuing resolution, with its longer-term status uncertain [17]. A Department of Justice audit — as reported by SecurityWeek — found that CISA faces challenges in cyber threat information sharing and that participation has hit record lows, reflecting a broader erosion of the government-industry information sharing relationship that took more than a decade to build [17]. If the act lapses without reauthorization, the legal protections that encourage companies to share threat data with CISA — and with each other — may be weakened at a moment when multiple threat intelligence assessments suggest nation-state and criminal activity targeting U.S. infrastructure has been increasing.

Recommendations

Immediate Actions

Organizations should audit their current dependencies on CISA-provided services and identify gaps that will not be filled by the agency in the near to medium term. This includes reviewing whether incident response plans assume CISA surge support or notification services, whether vulnerability management workflows rely exclusively on NVD enrichment data, and whether any staff training or tabletop exercise programs have been built around CISA resources that may no longer be reliably available.

Enterprises should immediately subscribe to vendor security advisory feeds for all critical systems, particularly those in industrial control, OT, and healthcare environments where CISA ICS advisories have historically been a primary source of threat-relevant vulnerability intelligence. Direct engagement with product vendors and their disclosure programs reduces dependence on government aggregation.

Short-Term Mitigations

Joining a sector-specific Information Sharing and Analysis Center (ISAC) — where one exists for your sector — provides a peer-operated threat intelligence and coordination capability that is not subject to federal budget cycles. The financial services (FS-ISAC), health (H-ISAC), electricity (E-ISAC), and water (WaterISAC) sectors each maintain active programs. Organizations not yet participating in their relevant ISAC should treat enrollment as a near-term priority rather than an aspirational objective.

CIRCIA compliance preparation should proceed regardless of rulemaking delays. The core requirements — an ability to determine that a significant cyber incident has occurred, to notify relevant authorities within 72 hours, and to track and report ransom payments — reflect sound incident response practices independently of regulatory obligation. Organizations in the 16 covered critical infrastructure sectors should initiate gap assessments now, so that when the final rule is published, they are not starting from zero [8].

Enterprises should evaluate commercial threat intelligence services as a replacement or supplement for CISA advisories, particularly for sectors with high exposure to ransomware or nation-state threat actors. This does not require replacing all government-sourced intelligence with paid alternatives — but it does mean ensuring that no critical threat intelligence function has a single point of failure in a federal agency operating at reduced capacity.

Strategic Considerations

The governance disruption at CISA reflects a broader structural shift in how U.S. cybersecurity is resourced at the federal level. As a planning posture — not a certain forecast — organizations should assume that the federal cybersecurity safety net will remain thinner than it was in 2024 for a multi-year period under current policy trajectories, even accounting for the possibility of partial restoration, and that the appropriate response is to build organizational resilience rather than wait for prior capability levels to return.

This means investing in internal threat intelligence capabilities, structured threat modeling, and incident response preparedness. It also means engaging with industry coalitions — including the CVE Foundation, which is developing a community-operated alternative to the current government-dependent CVE program structure, and ISAOs that fill gaps between formal ISAC memberships — to support the non-governmental information sharing infrastructure that becomes more important as federal capacity declines [9].

Security and risk executives should be transparent with boards about the changed risk environment. The baseline assumption that a federal agency would provide early warning of significant threats, assist with incident response, and maintain the vulnerability tracking infrastructure the enterprise depends on is no longer operationally reliable. That is a material change in enterprise risk posture, and it warrants explicit governance attention.

CSA Resource Alignment

The governance disruption at CISA reinforces the value of independent, industry-developed security frameworks that do not depend on government-issued guidance to remain operational. As federal advisory capacity diminishes, vendor-neutral control frameworks maintained by organizations like CSA provide a stable reference point that enterprises can use regardless of the federal funding environment.

The **CSA Cloud Controls Matrix (CCM)** and the **AI Controls Matrix (AICM)** are vendor-neutral, publicly available control frameworks that enterprises can use to assess and demonstrate security posture without relying on federal advisory services. While these frameworks address governance and controls — rather than real-time threat intelligence or incident response — they provide a consistent baseline for both cloud and AI security controls at a time when CISA's Secure by Design guidance program is operating with reduced staff.

The **CSA Security Trust Assurance and Risk (STAR) program** takes on particular relevance when federal oversight capacity is constrained. Third-party assessments conducted through STAR provide independent verification of cloud service provider security posture that does not depend on federal audit or inspection functions. Enterprises relying on cloud service providers for critical infrastructure workloads should consider requiring STAR Level 2 or Level 3 certifications as a condition of vendor selection, given reduced federal capacity to conduct the kind of sector-specific assessments CISA previously provided.

The **CSA MAESTRO framework** for agentic AI threat modeling provides a structured methodology for evaluating AI-related risks in the absence of government-issued guidance, which has been disrupted by CISA's reduced capacity for its emerging technology security work. As organizations deploy AI systems in operational environments, MAESTRO offers the threat modeling discipline that government advisory services would have previously helped provide — though it addresses a different function than CISA's operational threat intelligence and incident response roles.

CSA's **Zero Trust guidance** is directly relevant to the strategic response. A Zero Trust architecture does not assume that network adjacency — including proximity to federal security infrastructure — provides inherent protection. Organizations that have implemented Zero Trust principles are better positioned to operate resiliently when the external governance structures they had previously relied upon are weakened.

References

[1] TechCrunch. "US cybersecurity agency CISA reportedly in dire shape amid Trump cuts and layoffs." TechCrunch, February 25, 2026.

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

[3] State of Surveillance. "CISA Running at 38% Capacity as DHS Shutdown Guts America's Cyber Defense." State of Surveillance, February 2026.

[4] SC World. "A sober look at the recent DOGE cuts at CISA." SC World, 2025.

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

[6] SOCRadar. "CISA Budget Cuts and the U.S. Cyber Defense Gap in 2026." SOCRadar Blog, 2026.

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

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

[9] CyberScoop. "Behind the struggle for control of the CVE program." CyberScoop, October 2025.

[10] CGNET. "The Impact of DOGE Cuts to CISA and Organizational Cybersecurity." CGNET Blog, 2025.

[11] Federal News Network. "DHS budget request would cut CISA staff by 1,000 positions." Federal News Network, May 2025.

[12] Federal News Network. "House lawmakers' CISA budget reprieve comes with questions." Federal News Network, June 2025.

[13] Risk Management Magazine. "The Impact of Federal Budget Cuts on Cyber Defenses." Risk Management Magazine, October 2025.

[14] Cybersecurity Dive. "CISA loses key employee behind early ransomware warnings." Cybersecurity Dive, 2025.

[15] CSO Online. "CVE program averts swift end after CISA executes 11-month contract extension." CSO Online, 2025.

[16] Phoenix Security. "The CVE & NVD Crisis: A Wake-Up Call for Application Security." Phoenix Security, 2025.

[17] SecurityWeek. "Cyber Insights 2026: Information Sharing." SecurityWeek, 2026.