CSAI Foundation

Cloud Security Alliance AI Safety Initiative

The Defender Deficit: CISA Cuts and the Cybersecurity Gap

Assessing the Public-Private Security Fallout from Federal Agency Reductions

Unofficial AI-assisted Research

2026-04-19

Key Takeaways

A series of budget reductions, workforce reductions, and program eliminations has materially reduced the Cybersecurity and Infrastructure Security Agency's (CISA) operational capacity to serve as the linchpin of U.S. cyber defense. The agency's headcount fell from approximately 3,400 employees at the start of fiscal year 2025 to roughly 2,400 by December of that year [1], with the administration's FY2027 budget proposal seeking an additional $707 million in cuts [2]. The services eliminated or curtailed — threat intelligence sharing, critical infrastructure partnership coordination, vulnerability database enrichment, state and local government support — do not simply disappear. Their cost and complexity shift to the private sector, to under-resourced municipal governments, and to the defenders least able to absorb them.

Organizations operating across critical infrastructure sectors, cloud environments, and regulated industries should treat this shift as a structural change to the threat environment — not a temporary policy fluctuation — and calibrate their security programs accordingly.

The most urgent actions for security leaders are:

- Audit dependency on CISA-provided services (vulnerability feeds, threat advisories, incident response support) and document gaps.
- Establish or expand private-sector threat intelligence relationships to compensate for degraded federal sharing.
- Evaluate whether MS-ISAC or EI-ISAC membership is viable and appropriate for your organization and supply chain.
- Accelerate preparation for CIRCIA mandatory reporting obligations, which face continued implementation uncertainty.

Background

CISA was established in 2018 as the federal agency responsible for protecting the nation's civilian federal networks and critical infrastructure — energy, water, finance, healthcare, and more than a dozen other sectors. Unlike the intelligence community, CISA's mandate is explicitly collaborative: it exists to share threat intelligence with private-sector owners and operators, to provide technical assessments and red-

team exercises, to coordinate incident response, and to maintain foundational vulnerability infrastructure that the entire global security ecosystem depends upon. Its effectiveness depends on both budget and trust — the willingness of private organizations to share incident data with a federal partner that, in turn, shares defensive intelligence back.

Starting in early 2025, that collaborative model came under sustained pressure from two directions simultaneously: a Department of Government Efficiency (DOGE)-driven wave of immediate workforce reductions, and a succession of executive budget proposals seeking deep structural cuts. In March 2025, DOGE-initiated actions resulted in the elimination of CISA's entire red team operation — roughly 100 specialists whose work involved penetrating government and critical infrastructure networks to uncover vulnerabilities before adversaries could exploit them [3]. Former NSA cybersecurity director Rob Joyce publicly warned that the cuts would have a "devastating impact on cybersecurity and national security" [4]. The red team's elimination proved to be the first of a series of reductions that would reshape the agency over the following year.

By mid-2025, CISA had launched additional waves of staff reductions. The agency's Stakeholder Engagement Division — which coordinates cybersecurity improvement programs with states, local governments, private businesses, and international partners — saw its workforce drop from 200 positions to approximately 53, effectively closing the division [5][6]. The National Risk Management Center, which analyzes and models threats to critical infrastructure, lost 121 of its 179 positions and faced a 73% funding cut under the FY2026 budget proposal [6]. Cyber defense education and training programs faced a $45 million cut, while the election security mission lost $36.7 million and 14 positions [6]. The administration's FY2027 proposal, released in April 2026, called for an additional $707 million reduction to CISA's budget [2].

CISA's FY2025 budget listed $3.0 billion, 4,021 positions, and 3,641 full-time staff roles. The FY2026 budget lists $2.4 billion, 2,649 positions, and 2,324 full-time staff [7]. The proposed FY2027 figure would reduce the agency further still. In roughly eighteen months, CISA has shed, or is scheduled to shed, a third or more of its workforce and a significant fraction of its operational budget.

Security Analysis

The Collapse of Federal Threat Intelligence Infrastructure

The most immediately consequential dimension of these reductions is the degradation of threat intelligence sharing between the federal government and private sector. For decades, the Cybersecurity Information Sharing Act of 2015 (CISA 2015) provided the legal scaffolding that made this sharing viable

– granting companies liability and antitrust protections when they disclosed cyber threat indicators to DHS and to each other. That act expired on September 30, 2025 [8], and the four-month gap before Congress passed a reauthorization – via the Consolidated Appropriations Act of 2026, enacted February 3, 2026, extending the act through September 30, 2026 – created substantial uncertainty for organizations that depend on those liability and antitrust protections [8]. During the months the act was lapsed, one industry practitioner estimated that the volume of shared threat indicators had declined by more than 70%, with Information Sharing and Analysis Centers (ISACs) experiencing 24-to-48-hour delays in alert dissemination [9].

Simultaneously, DHS disbanded the Critical Infrastructure Partnership Advisory Council (CIPAC) in March 2025 – the primary venue for sensitive cross-sector threat discussions – removing a key institutional mechanism for coordinating private-sector defensive responses to nation-state intrusions [20]. As of this writing, no institutional mechanism has emerged to replicate the CIPAC's cross-sector coordination function at comparable scale. The consequence is that private organizations operating in critical infrastructure sectors now face the same adversaries with less federal support and fewer sanctioned channels for collective defense.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) serves as the primary cybersecurity intelligence and coordination resource for state, local, tribal, and territorial (SLTT) governments. More than 90% of the state and local threat intelligence that CISA distributes flows through the MS-ISAC [10]. Federal funding for the MS-ISAC – approximately $10 million annually, accounting for nearly half of the center's operating budget – ended on September 30, 2025, when CISA concluded its cooperative agreement with the Center for Internet Security (CIS) [11]. A National Association of Counties survey found that a substantial majority of MS-ISAC members reported the elimination of services would negatively affect their cybersecurity posture [12]. Rural and under-resourced counties, which rely on free tools and technical assistance from both the MS-ISAC and its elections-focused counterpart the EI-ISAC, face the most acute exposure. To compensate for lost federal funding, the MS-ISAC has begun raising membership fees; the lowest-cost tier has increased to $1,495 annually – a cost that may be manageable for large enterprises but represents a meaningful barrier for small municipal governments already stretched thin [13].

Vulnerability Infrastructure Under Stress

CISA's reductions have reverberated through the global vulnerability management infrastructure in ways that extend well beyond U.S. borders. In April 2025, the CVE Program – maintained by MITRE Corporation under a federal contract – narrowly avoided a complete shutdown when CISA executed an 11-month contract extension at the last moment, averting what would have been a catastrophic disruption to vulnerability tracking worldwide [14][15]. The episode revealed how much of the global

security ecosystem depends on a single contract that had gone unnoticed by senior policymakers until days before its expiration. CVE submission volume had grown 263% between 2020 and 2025, and the infrastructure supporting it had not scaled proportionately [16].

The National Vulnerability Database (NVD), maintained by the National Institute of Standards and Technology (NIST), provides the enriched metadata — severity scores, exploitability data, affected platform details — that security teams rely on to prioritize remediation. In April 2026, NIST acknowledged it would no longer enrich every CVE filed in the database, instead focusing enrichment efforts on vulnerabilities in the CISA Known Exploited Vulnerabilities (KEV) catalog, software used by the federal government, and software designated as critical [16]. All other CVEs will remain in the database without contextual metadata unless specifically requested. The practical effect for organizations that depend on NVD data for automated vulnerability prioritization is an expanding class of vulnerabilities that lack the enrichment context necessary to assess their urgency. Security teams will likely need to perform enrichment manually, invest in third-party vulnerability intelligence, or accept longer windows of uncertainty between disclosure and remediation decision — or pursue some combination of these approaches.

It is worth noting that the KEV catalog itself has continued to be updated actively — as recently as April 13, 2026, CISA added seven new known-exploited vulnerabilities — suggesting that at least some core operational functions have been preserved despite the broader degradation [17]. However, the sustainability of even these core functions under continued budget pressure is not guaranteed.

The Regulatory Vacuum and CIRCIA's Uncertain Path

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was designed to give CISA the mandatory incident reporting data it needs to understand the true scope of attacks on critical infrastructure, enabling earlier warnings and better-targeted defensive guidance. The act requires covered critical infrastructure entities to report significant cyber incidents to CISA within 72 hours of discovery and ransom payments within 24 hours. However, CISA has repeatedly delayed publication of the final implementing rule, most recently pushing it to May 2026 — and even that deadline is at risk because appropriations lapses forced cancellation of scheduled CIRCIA public comment town halls [18] [21]. The combination of CISA workforce reductions and delayed rulemaking means that the agency may lack both the staff to process incoming reports and the completed regulatory framework to compel them.

The result is a regulatory vacuum that benefits neither defenders nor the government. Organizations that have invested in CIRCIA compliance preparation are operating against a moving target. Those that have deferred preparation may find themselves out of compliance the moment a final rule is published.

And CISA, even if the rule takes effect, faces the challenge of handling a mandatory reporting program with substantially fewer staff than existed when CIRCIA was conceived.

The Transfer of Governmental Cyber Defense Functions

Among the structural shifts underway, the transfer of historically governmental functions to private organizations may carry the longest-term consequences. The closure of CISA's stakeholder engagement operations, the elimination of red team capacity, and the withdrawal from MS-ISAC funding all push the cost and complexity of collective cyber defense onto private organizations. Large enterprises with mature security operations centers, existing relationships with managed security service providers (MSSPs), and access to commercial threat intelligence platforms will absorb this burden more readily. They may even benefit, in a narrow sense, from a market structure that now prices things they already have. The organizations most harmed are those at the bottom of the security maturity distribution: small and mid-sized businesses that relied on free CISA scanning services, small municipalities that depended on MS-ISAC membership, and rural electric cooperatives or water utilities that had no meaningful security program of their own and looked to CISA for basic guidance.

As one industry analysis noted, the elimination of stakeholder engagement programs leaves enterprise security teams to confront nation-state threats without the support of a centralized federal clearinghouse [19]. Sophisticated adversaries — particularly nation-states — are able to concentrate resources and intelligence in ways that fragmented private-sector defenders cannot match; fragmenting the defensive response into thousands of individual organizational efforts is likely to produce systematically worse aggregate outcomes.

Recommendations

Immediate Actions

Organizations should audit their current dependencies on CISA-provided services and create a gap inventory. This includes CISA's free vulnerability scanning, the Automated Indicator Sharing (AIS) feeds, the KEV catalog subscription, and any incident response relationships with regional CISA advisors. Where gaps are identified, prioritize establishing commercial or consortium alternatives before those gaps become exploitable. Organizations in critical infrastructure sectors should also verify the current status of any CISA stakeholder engagement contacts they maintain, as the personnel supporting those relationships may no longer be in their roles.

Short-Term Mitigations

Security teams should establish or strengthen private-sector threat intelligence sharing relationships through existing ISAC membership, information sharing agreements with peers in their sector, or commercial threat intelligence platforms. If your organization operates infrastructure that serves state or local government clients, assess whether MS-ISAC membership — now transitioning to a fee-based model — should be funded directly or facilitated. Organizations that have not yet begun CIRCIA compliance preparation should treat the rule's eventual finalization as imminent and begin assessing what constitutes a "covered cyber incident" under their operations, building internal reporting workflows that meet the 72-hour incident and 24-hour ransomware payment requirements.

Vulnerability management programs should no longer assume that NVD enrichment will be available for all CVEs on a timely basis. Supplement NVD feeds with CISA's KEV catalog, which continues to receive active updates, and with vendor-specific advisories. For organizations operating software outside the federal government's priority stack, consider deploying supplemental vulnerability intelligence from commercial providers that perform independent enrichment.

Strategic Considerations

The longer-term implication of the defender deficit is that cybersecurity has crossed a threshold from a shared public-private responsibility to a primarily private one — at least for the foreseeable future. Strategic security investments should reflect this. Capabilities that were previously available at no cost through CISA — threat hunting support, red team exercises, incident response coordination, sector-specific threat briefings — must now either be built internally, procured from commercial vendors, or obtained through peer-sharing consortia. Security leadership should make this cost transfer explicit in their budgeting conversations with executives and boards, framing it not as an expansion of the security program but as an assumption of costs previously borne by the federal government.

Cloud security architectures in particular should be designed with the assumption that no federal backstop exists. This means implementing continuous monitoring, behavioral detection, and automated response capabilities that would previously have been supplemented by CISA's 24/7 operational functions. Organizations should evaluate whether current security architectures can detect and contain intrusions without the benefit of government-issued indicators of compromise, and invest in detection engineering capabilities accordingly.

CSA Resource Alignment

The conditions described in this note intersect directly with several active Cloud Security Alliance frameworks and initiatives.

CSA's **AI Controls Matrix (AICM)** – a superset of the Cloud Controls Matrix (CCM) – addresses the governance, risk, and compliance dimensions of security program management. As the federal regulatory environment becomes less stable and CISA's guidance capacity contracts, organizations should treat the AICM as a primary source of authoritative control requirements rather than supplementing it with federal-specific guidance that may no longer be reliably available. The AICM's coverage of Supply Chain Management, Threat and Vulnerability Management, and Incident Management controls is directly relevant to the gaps created by CISA's reduction in vulnerability enrichment and threat intelligence services.

The **MAESTRO framework** (Multi-layer AI Emergent Threat and Risk Observatory), CSA's threat modeling taxonomy for agentic AI systems, takes on additional relevance in this context because AI-powered security operations have been proposed as a compensating control for the loss of human federal capacity. Organizations considering deployment of AI-powered threat detection, automated incident triage, or autonomous response capabilities should use MAESTRO's threat layers to evaluate whether those systems introduce new attack surfaces – particularly given that CISA's red team, which might previously have evaluated such systems, no longer exists.

CSA's **Zero Trust Guidance for Critical Infrastructure** addresses how organizations can build security postures that are not dependent on perimeter-based or government-provided defensive layers. The core principle – never trust, always verify – maps directly to a threat environment where the assumption of federal protection has been demonstrably weakened. Critical infrastructure operators should prioritize the Zero Trust roadmap elements that reduce dependence on network perimeter controls and government-supplied threat intelligence feeds.

The **STAR (Security Trust Assurance and Risk)** program provides a continuous assurance mechanism for cloud environments. In the absence of CISA's sector-specific risk assessments and threat briefings, STAR attestation and third-party audit results become more important as evidence of security posture to regulators, business partners, and boards. Organizations should consider accelerating or expanding STAR participation as a mechanism for demonstrating due diligence in a period when federal oversight capacity is contracting.

Finally, CSA's **AI Safety Initiative** research on organizational responsibilities for AI security notes that effective AI governance requires stable reference frameworks and reliable threat intelligence inputs. Both conditions are under strain. As federal intelligence sharing infrastructure degrades, organizations

integrating AI into security operations must establish alternative intelligence pipelines — and the absence of those pipelines should itself be treated as a risk requiring disclosure and mitigation.

References

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

[2] TechCrunch. "Trump administration plans to cut cybersecurity agency's budget by $700 million." TechCrunch, April 7, 2026.

[3] TechCrunch. "DOGE axes CISA 'red team' staffers amid ongoing federal cuts." TechCrunch, March 11, 2025.

[4] The Register. "Ex-NSA boss warns job cuts will have 'devastating effect'." The Register, March 5, 2025.

[5] Cybersecurity Dive. "CISA's international, industry and academic partnerships slashed." Cybersecurity Dive, October 22, 2025.

[6] Cybersecurity Dive. "Trump's CISA budget lays out deep job cuts, program reductions." Cybersecurity Dive, June 2, 2025.

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

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

[9] CyberScoop. "CISA's expiration leaves a dangerous void in US cyber collaboration." CyberScoop, 2025. *(Op-ed commentary.)*

[10] Cybersecurity Dive. "Federal cuts force many state and local governments out of cyber collaboration group." Cybersecurity Dive, October 1, 2025.

[11] The Record. "CISA cuts $10 million annually from ISAC funding for states amid wider cyber cuts." Recorded Future News, March 12, 2025.

[12] National Association of Counties. "Multi-State Information Sharing and Analysis Center (MS-ISAC) loses federal funding." NACo, March 25, 2025.

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

[14] CSO Online. "CVE program averts swift end after CISA executes 11-month contract extension." CSO Online, April 16, 2025.

[15] CyberScoop. "Behind the struggle for control of the CVE program." CyberScoop, October 20, 2025.

[16] Help Net Security. "NIST admits defeat on NVD backlog, will enrich only highest-risk CVEs going for ward." Help Net Security, April 16, 2026.

[17] CISA. "CISA Adds Seven Known Exploited Vulnerabilities to Catalog." CISA, April 13, 2026.

[18] Davis Wright Tremaine. "CISA Delays Cyber Incident Reporting Rules Until May 2026." Davis Wright Tremaine, September 17, 2025.

[19] MSSP Alert. "CISA Budget Cuts Could Push More Security Burden onto MSSPs." MSSP Alert, 2025.

[20] Axios. "Industry groups' government partnerships tested after DHS terminates key council." Axios, March 18, 2025.

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

