CSAI Foundation

Cloud Security Alliance AI Safety Initiative

CISA's $707M Cut and the Enterprise Risk Coverage Gap

FY2027 Federal Budget Proposal Dismantles Critical Cybersecurity Infrastructure

Unofficial AI-assisted Research

2026-04-08

Key Takeaways

- The Trump administration's FY2027 budget proposes cutting $707 million from the Cybersecurity and Infrastructure Security Agency (CISA), reducing its operating budget from approximately $3 billion (FY2025 baseline) to roughly $2 billion and eliminating approximately 867 authorized positions [1][2][3].
- This follows a period of significant attrition: since January 2025, roughly one-third of CISA's workforce — approximately 1,000 employees — has left through DOGE-driven reductions, voluntary buyouts, and agency-wide layoffs, including the dismantling of its red team [9][10].
- The FY2027 proposal eliminates the Stakeholder Engagement Division almost entirely, cuts the National Risk Management Center's analytical budget by more than half, reduces field advisory support by 71 regional advisers, and eliminates roughly 240 annual vulnerability assessments for critical infrastructure operators [4][8].
- The Multi-State Information Sharing and Analysis Center (MS-ISAC) has already lost approximately half its federal funding, requiring a transition to a paid membership model that raises cost barriers for government and critical infrastructure organizations that previously relied on coordinated threat intelligence at no cost [12][13][14].
- Enterprises across all sectors should treat these cuts as a structural change in the risk landscape — not a temporary policy variance — and begin diversifying threat intelligence sourcing, deepening engagement with sector-specific ISACs, and budgeting for vulnerability management capabilities they previously received at no cost.

Background

CISA was established in 2018 as the federal government's principal civilian cybersecurity agency, chartered to protect critical infrastructure, coordinate threat intelligence sharing between government and private sectors, and provide direct technical assistance to federal agencies and state and local governments. At its peak, the agency had approximately 3,292 authorized positions [11] and administered a broad portfolio of programs spanning vulnerability advisories, incident response support, regional field operations, sector risk management, election security, and international coordination.

The agency's operating model was designed around a fundamental asymmetry: private sector organizations and under-resourced government entities could rely on CISA for threat intelligence, vulnerability assessments, and incident response expertise that would otherwise require substantial internal investment to replicate. When functioning as intended, this model allowed the federal government to absorb the overhead of maintaining the infrastructure — trained analysts, secure information-sharing channels, sector-specific expertise, and bilateral relationships with foreign partners — and distribute the benefit at no cost to thousands of organizations that lacked the scale to build equivalent capabilities independently.

The budget trajectory of the past fifteen months has placed that model under acute stress. The FY2026 budget reduced CISA's authorized workforce from approximately 3,292 to 2,324 positions [11]. DOGE-driven reductions and agency buyouts removed roughly 1,000 additional staff, with reporting indicating extensive senior leadership departures by mid-2025 [9]. The FY2027 proposal, released in the first week of April 2026, represents a further reduction — a $707 million gross-reduction figure that administration documents characterize as refocusing the agency on its "core mission" while eliminating "weaponization and waste" [1][3][7]. Critics and former agency officials argue it removes capabilities with no private-sector equivalent. Regardless of which framing one accepts, the operational consequence is the same: a sustained and accelerating contraction of federal cybersecurity capacity.

Security Analysis

The Scale of the Proposed Reduction

The FY2027 budget request would reduce CISA's total funding to approximately $2 billion from a FY2025 baseline of roughly $3 billion — a cumulative reduction of approximately one-third across two budget cycles [1][2][3]. The single-year figure of $707 million is the headline from administration documents, though budget appendix documents show a different figure of approximately $360–386 million in net cuts, a discrepancy that reflects different baseline comparisons and accounting methodologies [7]. Regardless of which figure is used as the reference, the operational reality is a sustained and accelerating contraction of federal cybersecurity capacity.

The reduction eliminates approximately 867 authorized positions and brings the agency's total authorized headcount to approximately 2,865. That authorized figure overstates operational capacity, because the agency has been operating well below its authorized levels since the departures of the past year — actual staffing is significantly lower than the authorized ceiling. The cumulative effect is an

agency that will enter FY2027 with both a sharply reduced budget and a workforce significantly diminished in senior institutional knowledge through the departure of experienced leadership over the past year.

Programs Being Eliminated or Severely Reduced

The FY2027 budget targets several program areas that directly serve the private sector and critical infrastructure community.

The Stakeholder Engagement Division, which serves as CISA's primary interface with state, local, private-sector, and international partners across sixteen critical infrastructure sectors, would be eliminated almost entirely. Of its four subdivisions, only the Sector Risk Management Agency function for eight infrastructure sectors would survive — and it would be relocated to a different division. The budget eliminates council management, external stakeholder engagement, and all international affairs offices, representing a decrease of 120 positions, 101 FTE, and $50.1 million [8]. For the operators of power grids, water systems, financial systems, and communications networks who relied on these offices for bilateral communication with the federal government, the elimination of this division removes a primary federal coordination channel for real-time threat communication with critical infrastructure operators.

The National Risk Management Center, which analyzes systemic cross-sector infrastructure risks and models cascading failure scenarios, would lose more than half its $64 million budget. The National Infrastructure Simulation and Analysis Center, the unit that develops software for analyzing cross-sector risks from emerging technologies, would lose $18.5 million — the majority of its budget [4][8]. Systemic risk analysis of the kind this center performed — particularly where it incorporates non-public government data and bilateral infrastructure interdependency models — is not commercially replicable in the same form, and no commercial substitute offers equivalent scope at comparable cost.

Vulnerability assessment services for critical infrastructure operators would lose $19.3 million, approximately a 60 percent reduction, resulting in roughly 240 fewer penetration testing assessments annually [4]. Regional field advisory operations would lose $42 million and 71 field advisers who help local governments and utilities harden their defenses [4]. The wing of the Cybersecurity Division responsible for threat hunting, capacity building, and vulnerability management would lose an additional $15.2 million [4]. Taken together, these cuts eliminate or severely reduce the operational infrastructure through which CISA translated threat intelligence into actionable defensive support for organizations that could not procure that support on the commercial market.

The election security program would be eliminated entirely, including defunding of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), which provided threat intelligence and incident response resources to state and local election officials [6]. While the direct enterprise security implications of election security cuts are limited, the elimination of EI-ISAC removes a model for sector-specific information sharing at a time when that model most needs to be expanded, not contracted.

The Compounding Effect: MS-ISAC, CISA 2015, and NIST

These cuts do not occur in isolation. CISA had already cut its funding to the Multi-State Information Sharing and Analysis Center by approximately $10 million — nearly half the total federal budget for the program — requiring MS-ISAC to transition from a free service to a paid membership model [12][13][14]. For state and local governments and smaller critical infrastructure operators who relied on MS-ISAC for threat detection, alerts, and incident response coordination, this transition represents an immediate cost burden on organizations that budgeted for no such expense.

The Cybersecurity Information Sharing Act of 2015 (CISA 2015), which established liability protections, antitrust shields, and FOIA restrictions for organizations that voluntarily share cyber threat indicators with the federal government, expired on September 30, 2025. After a period of lapsed authority during which private threat intelligence sharing operated without the statute's protections, Congress extended the act through September 30, 2026 as part of a government funding bill signed by President Trump in February 2026 [15][16]. The long-term reauthorization remains contested. Sen. Rand Paul, who chairs the relevant committee, has indicated he will not advance any extension that does not address unrelated concerns about CISA's prior activities [15]. If CISA 2015 lapses again without reauthorization, the liability and antitrust protections that underpin voluntary threat sharing in the private sector would be removed, potentially chilling the very intelligence flows that substitute for government-provided intelligence as CISA contracts.

NIST, whose National Cybersecurity Center of Excellence and standards development programs provide much of the technical guidance on which enterprises and government agencies base their security architectures, faces a proposed $993 million reduction in the same FY2027 budget [5]. This compounds the risk picture: at the moment CISA is reducing its operational support, the federal agency most responsible for technical security standards and guidance is also under significant financial pressure.

What Enterprises Actually Lose

The practical implications of these cuts extend across several categories of enterprise security operations. Free threat intelligence, including vulnerability advisories, joint cybersecurity advisories co-published with the FBI and NSA, and the Known Exploited Vulnerabilities catalog, depends on the

analytical capacity of the teams being reduced. The KEV catalog, which many enterprises and their vendors use as a prioritization tool for patch management, reflects the outputs of CISA analysts who track and validate active exploitation evidence. A significant reduction in that analytical workforce raises legitimate questions about the catalog's future update frequency and completeness, even if the catalog itself is not formally targeted for elimination in the budget proposal.

Organizations in critical infrastructure sectors who have depended on CISA's free vulnerability assessment and penetration testing services will need to evaluate whether to procure equivalent commercial services. With approximately 240 fewer assessments annually, availability will narrow to a fraction of the organizations that previously qualified. Regional field advisers, who provided hands-on guidance to utilities, hospitals, water systems, and municipal governments, will no longer be geographically distributed in ways that made them reachable at low friction.

The differential impact across organizational size matters significantly. Large enterprises with mature security programs, commercial threat intelligence subscriptions, and internal red teams are better positioned to absorb these changes and are less likely to experience acute disruption in the near term. Mid-market organizations and smaller critical infrastructure operators — precisely the entities CISA's programs were designed to serve — will face the largest relative increase in their residual risk exposure.

Recommendations

Immediate Actions

Organizations that currently rely on CISA services for any portion of their threat intelligence or vulnerability management programs should conduct an immediate inventory of those dependencies. For each dependency, the appropriate question is whether a commercial, consortium-based, or sector-ISAC alternative exists and what the procurement timeline and cost would be. Organizations should not wait for the FY2027 budget to be enacted — the agency's operational capacity has already declined substantially from its FY2025 levels, and even significant congressional restoration is unlikely to fully reverse the institutional knowledge lost through the departure of experienced personnel over the past year.

Organizations that have not yet joined their sector-specific Information Sharing and Analysis Center should do so promptly. Sector ISACs — including FS-ISAC for financial services, H-ISAC for healthcare, E-ISAC for electricity, and their counterparts across other sectors — have invested years building the

bilateral trust relationships and threat intelligence infrastructure that CISA's stakeholder engagement programs once supplemented. Those relationships become the primary channel for peer-to-peer threat intelligence as federal capacity contracts.

Short-Term Mitigations

In the near term, enterprises should evaluate commercial threat intelligence platforms to fill advisory gaps left by reduced CISA publication frequency. Commercial platforms aggregating indicators of compromise, active exploitation data, and sector-specific threat context can partially substitute for government-sourced intelligence, though the integration cost and ongoing subscription expense represent a budget line that previously did not exist for organizations relying on CISA's free services.

Organizations in sectors that received CISA vulnerability assessments should evaluate commercial alternatives such as external attack surface management services, third-party penetration testing engagements, and continuous vulnerability scanning programs. The cost-per-assessment comparison will not favor the commercial option, but the alternative — an unassessed attack surface — carries its own risk premium that now needs to be accounted for explicitly.

State and local government entities that depended on MS-ISAC's free services should engage their state homeland security offices to understand what support remains available under the new paid membership structure and whether state-level pooled procurement can reduce per-entity costs. Some states may have the capacity to coordinate this transition collectively, reducing per-entity costs through shared procurement.

Strategic Considerations

For planning purposes, enterprises should treat this as a potential long-term realignment rather than a temporary operational gap — the institutional knowledge and program infrastructure lost over the past year will not be quickly restored even if funding levels are subsequently increased. Organizations that treat it as a temporary inconvenience will find themselves systematically under-resourced.

Security leadership should incorporate the reduced federal baseline into enterprise risk assessments and board-level risk disclosures. The change in the external risk environment created by CISA's contraction is material for organizations in critical infrastructure sectors, for organizations with significant federal contractor exposure, and for organizations that participated in CISA's free services as a meaningful component of their security program.

Organizations with the capacity to do so should strengthen internal cyber threat intelligence capabilities. The shift from a model in which the federal government aggregates and distributes threat intelligence to one in which enterprises must source that intelligence commercially or through peer networks increases both the cost and the strategic value of internal CTI functions. Those who invest in collection, analysis, and dissemination capabilities now will be better positioned as the competitive landscape for threat intelligence shifts.

CSA Resource Alignment

The CSA AI Controls Matrix (AICM) and Cloud Controls Matrix (CCM) provide governance frameworks that enterprises can use to assess and document the residual risk created by reductions in external security support. Control domains addressing threat and vulnerability management, incident response, and supply chain assurance are directly relevant when the federal services that previously supplemented those controls are no longer available at previous levels. Enterprises should review their AICM and CCM implementations to identify controls whose effectiveness was predicated on CISA support and develop compensating control strategies for those areas.

CSA's Zero Trust guidance is particularly relevant in this environment. Zero Trust architecture reduces dependence on perimeter-based defenses and the network-centric threat models those defenses required, shifting the security model toward identity verification, least-privilege access, and continuous validation — capabilities that enterprises control internally. While threat intelligence remains valuable in a Zero Trust environment, its application becomes more targeted and less dependent on perimeter-specific indicators, giving organizations greater autonomy in how they source and apply intelligence as federal capacity contracts.

The CSA Security Trust Assurance and Risk (STAR) program provides a vehicle for enterprises to evaluate their third-party and supply chain partners' security postures against a common framework. In an environment where federal vulnerability advisories and sector-wide alerts may arrive less frequently, the ability to assess partner security maturity independently takes on additional value. Encouraging suppliers and partners to maintain current STAR attestations strengthens the collective security posture of enterprise ecosystems.

CSA's MAESTRO framework for agentic AI threat modeling remains relevant as AI systems increasingly handle sensitive workloads across enterprise environments. As CISA's capacity to issue timely advisories on AI-relevant vulnerabilities and to conduct threat hunting across federal and critical infrastructure networks contracts, enterprises deploying AI agents and inference infrastructure carry a greater share of the responsibility for identifying and mitigating AI-specific threats.

References

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

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

[3] Cybersecurity Dive Staff. "Trump's FY2027 budget again targets CISA." Cybersecurity Dive, April 2026.

[4] E. Geller. "CISA's vulnerability scans, field support on chopping block in Trump budget." Cybersecurity Dive, April 7, 2026.

[5] B. Kahn. "Cuts hit CISA, NIST and IRS in Trump's FY27 budget." Government Executive, April 2026.

[6] J. Bannon. "Trump proposes cutting CISA election security program in FY27 budget." Nextgov/FCW, April 2026.

[7] MeriTalk Staff. "Trump FY2027 Budget Cuts CISA by $707M, Reduces S&T Agencies." MeriTalk, April 2026.

[8] InsideCybersecurity Staff. "CISA proposes drastic changes to stakeholder engagement efforts in fiscal 2027 budget request." InsideCybersecurity, April 2026.

[9] S. Turton. "Exclusive: One-third of top U.S. cybersecurity agency has left since Trump took office." Axios, June 3, 2025.

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

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

[12] StateScoop Staff. "MS-ISAC loses federal support for threat intelligence, incident response." StateScoop, March 11, 2025.

[13] Infosecurity Magazine Staff. "US Cuts Federal Funding for MS-ISAC Cybersecurity Program." Infosecurity Magazine, September 30, 2025.

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

[15] Hunton Andrews Kurth. "Congress Extends Cybersecurity Information Sharing Act of 2015 through September 2026." Privacy and Cybersecurity Law Blog, 2026.

[16] Cybersecurity Dive Staff. "Government funding bill temporarily revives cybersecurity information-sharing law." Cybersecurity Dive, 2025.