CSAI Foundation

Cloud Security Alliance AI Safety Initiative

CISA Leadership Vacuum: US Cyber Governance at a Breaking Point

Implications for Enterprise Security Teams and Critical Infrastructure Operators

Unofficial AI-assisted Research

2026-04-24

Key Takeaways

- The Cybersecurity and Infrastructure Security Agency has operated without a Senate-confirmed permanent director since January 2025, an extended period of leadership instability that includes three successive acting directors, a withdrawn Senate nominee, and a series of credibility-damaging scandals in the acting director role [2][10].
- Sean Plankey, the Trump administration's nominee to lead CISA, withdrew from consideration on April 22, 2026, after his nomination stalled for 13 months amid competing legislative holds from members of both parties [3][11].
- CISA has lost more than one-third of its workforce since early 2025, dropping from approximately 3,292 staff to a projected 2,324, through a combination of layoffs, voluntary buyouts, and departures by career staff who cited demoralization and organizational dysfunction as primary factors [4][5].
- The FY2027 budget proposal released in April 2026 would eliminate an additional $707 million in CISA programs, including the complete dissolution of the election security mission and significant reductions to the National Risk Management Center [6].
- The termination of federal funding for the Multi-State Information Sharing and Analysis Center (MS-ISAC) — which provided the substantial majority of threat intelligence distributed to state and local governments — has left thousands of under-resourced government entities with materially degraded cyber defense capability [7].
- Enterprise security teams should treat the federal cybersecurity support network as substantially diminished and adjust their threat intelligence sourcing, incident response planning, and critical infrastructure protection postures accordingly.

Background

For fifteen years, the Cybersecurity and Infrastructure Security Agency and its predecessors served as the central coordinating body for the United States' civilian cybersecurity posture. Created as a standalone agency under the Cybersecurity and Infrastructure Security Agency Act of 2018, CISA consolidated the federal government's civilian cyber defense, infrastructure protection, and emergency

communications functions, becoming the primary interface between federal cybersecurity capacity and the broader ecosystem of state and local governments, critical infrastructure operators, and private sector organizations that constitute the country's digital attack surface.

Under Director Jen Easterly, who led the agency from 2021 through January 2025, CISA developed a recognized international profile for proactive threat disclosure, infrastructure vulnerability coordination, and public-private partnership on cyber resilience. The agency's Known Exploited Vulnerabilities catalog, Shields Up campaign, and joint advisory program with Five Eyes intelligence partners became widely adopted reference points for enterprise security operations. Easterly's departure with the incoming Trump administration set in motion a leadership transition from which the agency has not recovered.

Madhu Gottumukkala, appointed acting director in May 2025, had a tenure that became defined in public perception by two significant security incidents. In the summer of 2025, he failed a polygraph administered in connection with an access request for a controlled access program — an incident that led DHS to place at least five career employees and one contractor on administrative leave before ultimately dropping the investigation without public resolution [8]. More consequentially, sensors detected that Gottumukkala had uploaded multiple documents marked "for official use only" to the public version of OpenAI's ChatGPT platform, generating security alerts that were neither acted upon nor disclosed to Congress despite repeated inquiry [9]. By the time the Trump administration reassigned him to a DHS strategic implementation role in late February 2026, Gottumukkala had drawn sustained congressional criticism and had alienated significant portions of CISA's remaining professional staff [2].

Nick Andersen, the executive assistant director for cybersecurity, assumed the acting director role in late February 2026 following Gottumukkala's reassignment [10]. Andersen brings extensive public-sector cybersecurity experience, having held IT and security roles at the Coast Guard, Navy, and Department of Energy across two decades of federal service [10], but the structural problems confronting the agency extend well beyond personnel. As of the date of this writing, Andersen is the third person to hold the acting director role in fifteen months, leading an agency that has been unable to fill 300 mission-critical vacancies, has cancelled its CyberCorps summer internship program, and is absorbing a second consecutive round of deep budget cuts [3].

Security Analysis

The Nomination Failure and Its Governance Cost

The withdrawal of Sean Plankey on April 22, 2026, is more than a personnel setback — it illustrates how CISA's leadership continuity has become a casualty of unrelated political disputes in a Senate with competing legislative priorities [3]. Plankey, a former Coast Guard officer with cybersecurity policy credentials, was first nominated in March 2025. The Senate Homeland Security and Governmental Affairs Committee voted to advance his nomination in July 2025. He was re-nominated following the start of the 119th Congress, but the nomination stalled again in the Senate through the spring of 2026.

The proximate causes of the failure illuminate the degree to which CISA's leadership continuity has become collateral damage in unrelated political disputes. Senator Rick Scott of Florida placed a hold on Plankey's nomination tied to a Coast Guard shipbuilding contract dispute with no direct connection to cybersecurity policy [11]. Senator Ron Wyden of Oregon conditioned his support on the public release of a classified 2022 report on security problems at US telecommunications companies — a legitimate oversight concern, but one that nevertheless blocked agency leadership for over a year [11]. Plankey's withdrawal letter acknowledged the impasse directly, writing that "after thirteen months since my initial nomination, it has become clear the Senate will not confirm me" [3].

The consequence is that the nation's primary civilian cyber defense agency has now gone more than sixteen months without a Senate-confirmed director, during a period in which publicly reported adversary targeting of US critical infrastructure has shown no signs of diminishing. An agency without permanent leadership operates under structural constraints on strategic planning, interagency coordination, and staff retention that cannot be remediated through operational competence alone.

Workforce and Institutional Knowledge Attrition

The staffing losses at CISA represent a compounding problem that will outlast any eventual resolution of the leadership question. The agency's workforce declined from approximately 3,292 employees at the start of FY2025 to a projected 2,324 by the end of the budget cycle, driven by DOGE-related layoffs, a DHS-wide voluntary buyout program that a significant number of CISA employees accepted, and a wave of voluntary departures by career staff who cited demoralization and organizational dysfunction [4][5]. The Trump administration's FY2026 budget proposal confirmed the trajectory toward a workforce roughly 32% smaller than the agency entered the year with [5].

What aggregate staffing numbers obscure is the disproportionate loss of institutional knowledge and experienced personnel. Senior professionals with deep understanding of critical infrastructure relationships, threat actor tradecraft, and interagency coordination processes are among the hardest to replace. CISA's regional advisors, who maintained direct relationships with state and local government cyber programs, were among the staff categories most affected by the buyout program. The agency's Cybersecurity State Coordinators — who serve as CISA's primary points of contact for state-level cyber officials — have seen their ranks thinned at precisely the moment their state-level counterparts most need federal support.

The FY2027 budget proposal, released in April 2026, would further reduce CISA's workforce and eliminate approximately $707 million in program funding [6]. The National Risk Management Center, which coordinates risk assessments across sixteen critical infrastructure sectors including power, water, and transportation, faces a severe proposed funding reduction and significant position losses under this proposal [6]. The NRMC's cross-sector risk modeling function has no private-sector analog and no standing state-level equivalent, meaning its effective elimination would create a gap in national-level infrastructure risk synthesis for which no standing substitute exists.

Program Dismantlement and the State and Local Intelligence Gap

Among the most consequential operational changes of the past year has been the termination of federal funding for the Multi-State Information Sharing and Analysis Center. For over two decades, MS-ISAC — operated by the Center for Internet Security — served as the primary cybersecurity resource for state, local, tribal, and territorial government entities, most of which lack the resources to maintain independent threat intelligence operations. CISA terminated its cooperative agreement with CIS effective September 30, 2025, ending the flow of federal funding that had supported MS-ISAC's threat analysis, incident response services, and member account management [7].

The implications are significant because the overwhelming share of state and local threat intelligence that CISA distributed came through the MS-ISAC [7]. The termination forced the Center for Internet Security to restructure the program as a fee-based service, with fees scaled to operating budget — a shift that, despite provisions for discounted or reduced-cost access for some members, is likely to create meaningful affordability barriers for the smallest and most resource-constrained governments. For those entities, the practical result is a return to isolated, unsupported operations with limited visibility into threats affecting their networks and limited access to incident response assistance when those threats materialize.

The Critical Infrastructure Partnership Advisory Council — which facilitated sensitive, pre-competitive collaboration between CISA and critical infrastructure operators on shared risk and defense — was shuttered as part of the reorganization [4]. CISA's election security program, which had fielded a

dedicated national staff and supported the Elections Infrastructure Information Sharing and Analysis Center, would be eliminated entirely under the FY2027 budget proposal [5][6]. Cyber defense education and training programs face proposed reductions of similar magnitude [5][6]. Each of these program eliminations represents not just a budget line but a set of relationships, institutional processes, and accumulated expertise that cannot be reconstituted quickly.

Enterprise and Private Sector Exposure

For private sector organizations, the deterioration of CISA's operational capacity translates into specific, practical deficits. The agency's joint cybersecurity advisory program — which produced authoritative technical guidance on threat actor TTPs, coordinated with Five Eyes partners and sector-specific agencies — is likely to have slowed substantially, as staffing reductions reduce the analytical capacity required to produce timely, technically grounded advisories. Training exercises designed to help critical infrastructure operators rehearse coordinated cyber incident response have been reduced or suspended; organizations should verify the status of exercises relevant to their sector directly with CISA regional contacts. Direct engagement between CISA regional staff and private infrastructure operators has declined as travel allowances were cut and regional advisor positions were reduced [4].

Organizations that previously relied on CISA for early-warning threat intelligence, incident response coordination, or regulatory guidance should not expect the same service levels that characterized the pre-2025 period. The combination of workforce attrition, program eliminations, and leadership instability has materially changed what the agency can deliver. Enterprises operating in critical infrastructure sectors — financial services, energy, healthcare, water and wastewater, transportation — face a landscape in which the federal backstop for cybersecurity coordination is substantially thinner than it was two years ago, at a time when publicly reported adversary targeting of US infrastructure shows no signs of diminishing.

The governance vacuum also creates regulatory ambiguity. CISA's role as the primary civilian authority for critical infrastructure cybersecurity has not been formally reassigned, but the agency's practical capacity to fulfill that role is diminished. Sector-specific regulators — NERC/FERC for energy, OCC for banking, HHS for healthcare — retain their independent authorities, but cross-sector coordination and the synthesis of multi-sector threat intelligence are functions that exist primarily within CISA's remit. Organizations that comply diligently with sector-specific requirements should not mistake that compliance for comprehensive coverage of the cross-sector risk landscape that CISA previously managed.

Recommendations

Immediate Actions

Organizations should audit their current dependency on CISA-provided threat intelligence, advisories, and support services and develop alternatives where practical. This includes joining sector-specific ISACs if not already members, establishing direct relationships with the FBI's Cyber Division and IC3, and evaluating commercial threat intelligence subscriptions to fill gaps created by reduced CISA advisory output. State and local government entities that previously relied on MS-ISAC services should assess whether participation in the restructured fee-based program is affordable and, if not, identify alternative intelligence-sharing arrangements through regional networks or sector associations.

Critical infrastructure operators should review their incident response plans under the assumption of reduced federal coordination capacity. Plans that assume timely CISA engagement during a significant incident may need to be updated to reflect realistic response timelines given current staffing, and relationships with CISA regional staff who remain in place should be reinforced through direct outreach before an incident occurs.

Short-Term Mitigations

Organizations should increase their direct engagement with sector-specific ISACs, with Five Eyes partner advisories (from NCSC, ACSC, CCCS, and GCSB, which continue to produce joint technical guidance), and with the cybersecurity research community as alternative sources of timely threat intelligence. The CISA Known Exploited Vulnerabilities catalog remains a valuable and maintained resource; organizations not already managing against it should integrate it into their vulnerability management programs.

Enterprise AI operators should pay particular attention to the reduced advisory capacity given the accelerating pace of AI infrastructure vulnerabilities. The federal government's capacity to coordinate rapid, multi-sector responses to emerging AI security threats has been further constrained by the CISA workforce reductions, underscoring the need for organizations to invest in their own AI security intelligence capabilities. In the absence of timely federal guidance, organizations must rely more heavily on their own research, vendor advisories, and community intelligence sharing.

Strategic Considerations

The current degradation of federal cybersecurity governance capacity represents a structural shift that may persist beyond any single administration or leadership cycle. The institutional knowledge, stakeholder relationships, and program infrastructure that have been lost over the past fifteen months will require years to rebuild, regardless of future policy direction. Security leaders should calibrate their long-term strategy accordingly, investing in organizational capabilities and external partnerships that do not assume a robust federal support function.

At the policy level, CSA urges its members and the broader security community to engage with congressional oversight processes, sector-specific regulatory bodies, and international coordination mechanisms to ensure that the gaps created by CISA's reduced capacity are named, measured, and addressed. The appropriate level of federal civilian cybersecurity capacity is a policy question that ultimately requires democratic resolution — but the security community is well-positioned to articulate the operational consequences of the current trajectory to policymakers, boards, and public stakeholders.

CSA Resource Alignment

This research note addresses governance and operational gaps that directly intersect with several CSA frameworks and programs.

The CSA AI Controls Matrix (AICM) provides enterprise security teams with a structured, vendor-agnostic governance framework for AI security that does not depend on federal coordination. As federal cybersecurity support becomes less reliable, the AICM's 243 control objectives across 18 security domains offer a practical foundation for organizations seeking to maintain rigorous AI security governance in an environment of diminished federal guidance.

The MAESTRO framework for agentic AI threat modeling is particularly relevant in the current context: as CISA's capacity to produce timely threat intelligence and coordinated advisories on emerging AI security threats diminishes, organizations need internal frameworks to systematically model adversarial scenarios that federal agencies might previously have synthesized and communicated. MAESTRO's structured threat modeling methodology supports that internal capability.

The CSA STAR for AI program provides a pathway for verifiable AI assurance that operates independently of national regulatory enforcement, which is particularly valuable in a period when the agencies responsible for critical infrastructure oversight are operating at reduced capacity. Organizations

seeking to demonstrate responsible AI governance to customers, partners, and auditors can leverage STAR for AI as a credible, internationally recognized standard.

The CSA Cloud Controls Matrix (CCM v4.1) and its associated STAR assurance program provide critical infrastructure operators with a framework for cloud security governance that complements sector-specific regulatory requirements and can help fill gaps where CISA's cross-sector risk coordination capacity has been reduced.

References

[1] Federal News Network. "CISA leadership shakeup comes amid 'pressure' moment for cyber agency." Federal News Network, February 2026.

[2] TechCrunch. "CISA replaces acting director after a bumbling year on the job." TechCrunch, February 27, 2026.

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

[4] Cybersecurity Dive. "CISA's 7 biggest challenges in 2026." Cybersecurity Dive, 2026.

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

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

[7] StateScoop. "CISA confirms it's ending MS-ISAC support." StateScoop, 2025.

[8] Nextgov/FCW. "DHS drops investigation into former acting CISA chief's failed polygraph exam." Nextgov, March 2026.

[9] TechCrunch. "Trump's acting cybersecurity chief uploaded sensitive government docs to ChatGPT." TechCrunch, January 28, 2026.

[10] CyberScoop. "Gottumukkala out, Andersen in as acting CISA director." CyberScoop, February 2026.

[11] The Record. "Trump's pick to lead CISA withdraws from consideration." The Record from Recorded Future News, April 2026.

