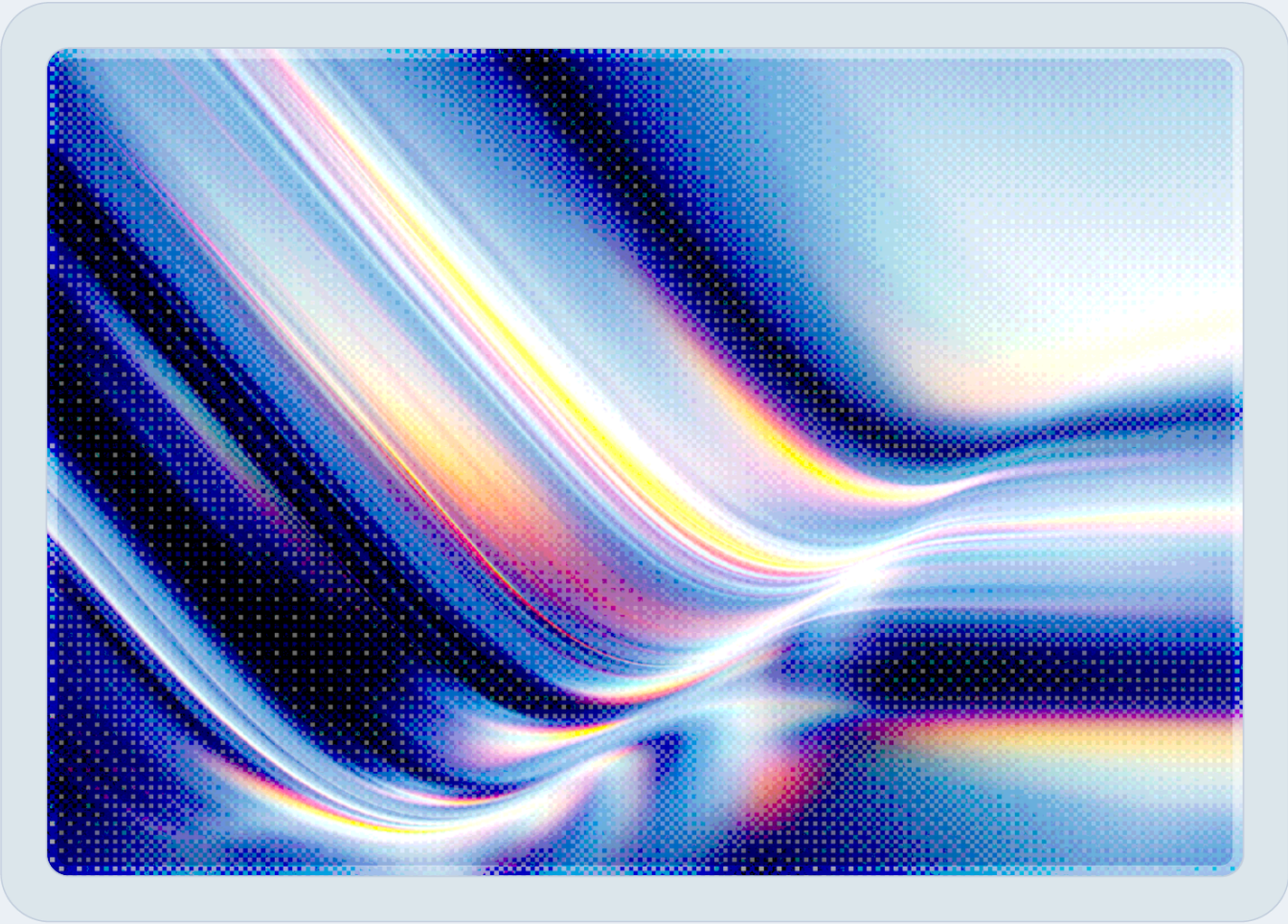
CSAI Foundation | Cloud Security Alliance

# The Hollowing of CISA: Attrition, Credential Exposure, and Defense Risk

2026-06-03

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

## Key Takeaways

- A Nightwing contractor maintained a public GitHub repository named "Private-CISA" that exposed administrative AWS GovCloud credentials, plaintext passwords for dozens of internal CISA systems, SSH keys, SAML certificates, and pipeline secrets for approximately six months beginning November 2025 — a disclosure that Congress characterized as indicative of "a diminished security culture and/or an inability for CISA to adequately manage its contract support." [1][2]
- CISA has lost approximately one-third of its workforce — roughly 1,000 employees — since the start of 2025 through buyouts, early retirements, layoffs, and forced reassignments, leaving the agency without a Senate-confirmed director as of June 2026 and operating with a significantly reduced cybersecurity advising corps. [3]
- The termination of federal funding for the Multi-State Information Sharing and Analysis Center (MS-ISAC) in September 2025, following the earlier termination of the Elections Infrastructure ISAC in February 2025, has broken the primary institutional pathway through which CISA distributed cyber threat intelligence to state, local, tribal, and territorial governments. [5][6]
- Enterprise security teams and critical infrastructure operators should treat the current period as one of structurally reduced federal cyber coordination capacity, and calibrate their threat intelligence sourcing, incident response planning, and vulnerability management programs accordingly — supplementing CISA-dependent workflows with independent sources and industry-led channels.

## Background

The Cybersecurity and Infrastructure Security Agency was established in 2018 as the lead federal civilian cyber defense agency, charged with coordinating threat intelligence across government and critical infrastructure sectors, maintaining the Known Exploited Vulnerabilities (KEV) catalog, supporting state and local governments through shared services, and serving as the primary bridge between the federal government and private sector operators during major incidents. That mandate has not changed. The agency's capacity to execute it has.

Beginning in early 2025, CISA began losing a substantial portion of its workforce under pressure from the Department of Government Efficiency and broader federal workforce reduction initiatives — a trend already visible in mid-2025 reporting [4]. By the time the most recent wave of departures was tallied, approximately 1,000 employees had left the agency — representing nearly one-third of its total staff [3]. The Cybersecurity Division, CISA's largest operational unit, declined from a peak of roughly 1,100 staff to an estimated 800–850 [3]. The agency's nationwide corps of cybersecurity advisers, field personnel who work directly with critical infrastructure operators to assess posture and provide hands-on guidance, fell from approximately 164 to 97 [3]. Senior leadership departed through a combination of forced retirements, political reassignments, and voluntary resignations, and the agency entered 2026 without a Senate-confirmed director after Sean Plankey withdrew his candidacy in April 2026 following thirteen months without a Senate confirmation vote [7][8]. Acting Director Madhu Gottumukkala has defended the reductions, telling the House Homeland Security Committee that "a disciplined mission requires the right workforce — not a larger one, but a more capable and skilled one," while providing limited specifics about operational impact [9].

The May 2026 credential exposure surfaced against this backdrop of institutional contraction. A contractor at Nightwing, a Dulles, Virginia-based government contractor, had maintained a public GitHub repository named "Private-CISA" since November 13, 2025 [1]. The repository contained administrative credentials for three AWS GovCloud accounts, plaintext usernames and passwords for dozens of internal CISA systems stored in a CSV file named "AWS-Workspace-Firefox-Passwords.csv," SSH keys, Entra ID SAML certificates, API tokens, and internal log files [1][2][14]. The repository also held detailed information about CISA's "Landing Zone DevSecOps" environment — the agency's secure software build, test, and deployment pipeline — and credentials for the internal "artifactory" code repository used across CISA software projects [1]. Security researcher Guillaume Valadon of GitGuardian identified the exposure on May 14–15, 2026, and brought it to the attention of journalist Brian Krebs, who broke the story publicly [1][10]. The repository owner had explicitly disabled GitHub's built-in secret scanning protections, preventing automated detection at the platform layer [1]. After notification, the repository was taken offline, but the exposed AWS GovCloud keys remained active for approximately 48 hours before revocation [1].

# Security Analysis

## The Incident as Institutional Signal

The credential leak is best understood not as an isolated contractor failure but as a symptom of a deeper institutional dynamic. When organizations lose one-third of their workforce — including losses among senior personnel who carry institutional knowledge, security culture norms, and contractor oversight expertise — the conditions for this kind of failure multiply. Insider risk research broadly identifies workforce transitions, reduced management bandwidth, and diminished security culture as conditions that precede credential exposure incidents. The House Homeland Security Committee letter to acting Director Gottumukkala explicitly connected these dots, characterizing the breach as reflecting "a diminished security culture and/or an inability for CISA to adequately manage its contract support" [2]. Sen. Maggie Hassan's separate demand for a classified briefing emphasized the contradiction directly: "This reported incident raises serious questions about how such a security lapse could occur at the very agency charged with helping to prevent cyber breaches" [13].

The specific failure mechanism matters as much as the high-level narrative. The contractor had disabled GitHub's automated secret scanning — a configuration state that bypassed a platform control specifically designed to catch credential exposure in repositories. This was not a case of a naive user unaware that secrets should not be committed to version control. It reflects either a policy gap in CISA's contractor security requirements, a failure of CISA's oversight capacity to verify contractor compliance with those requirements, or both. In a fully-staffed agency with active contractor oversight programs, this kind of deviation from baseline controls would be more likely to be caught through periodic audit. In an agency that has lost a third of its workforce, contractor oversight activities are among the functions most easily deprioritized.

The sensitivity of what was exposed amplifies the risk considerably. AWS GovCloud environments are specifically provisioned for workloads handling Controlled Unclassified Information (CUI) and sensitive government data. Administrative credentials to multiple GovCloud accounts, combined with the internal DevSecOps pipeline configuration, would provide a sophisticated adversary with the means to map CISA's internal software infrastructure, understand build and deployment workflows, and potentially position for supply chain attacks against CISA-developed tools or the agency's internal systems. The forty-eight-hour window during which exposed AWS keys remained active after the repository was taken offline represents a meaningful threat window for a well-resourced adversary monitoring for such exposures.

## The Compounding Effect: Lost Programs and Diminished Channels

Beyond the credential incident itself, the structural reduction in CISA's capacity has broken or degraded several specific functions that enterprise security teams and state and local governments have historically relied upon.

The most consequential program loss is the Multi-State Information Sharing and Analysis Center. For twenty-one years, CISA funded CIS to operate MS-ISAC as the primary mechanism for distributing cyber threat intelligence to state, local, tribal, and territorial governments — a constituency that includes the networks supporting elections, public utilities, emergency services, and public health systems. More than 90 percent of the state and local threat intelligence that CISA distributed flowed through MS-ISAC [5]. When CISA terminated the cooperative agreement on September 30, 2025, it eliminated that channel, offering as a replacement a combination of grant funding pathways and no-cost tools such as vulnerability scanning and phishing assessments [5][6][12]. These are not equivalent substitutes. Vulnerability scanning and phishing assessments address point-in-time posture; real-time threat intelligence sharing addresses the continuous adversarial environment. The practical result is that state and local governments — many of which joined MS-ISAC precisely because the cost and expertise requirements of independent threat intelligence programs exceed their available resources — now face their threat environments with a substantially degraded information channel.

The Elections Infrastructure ISAC, whose federal funding was terminated in February 2025, represents a second significant loss in a domain where CISA's coordination role was uniquely important. Election infrastructure security had been one of CISA's signature mandates since 2017, and the agency had invested heavily in building direct relationships with state election officials and county election boards. Dissolving that institutional structure does not simply reduce a budget line; it eliminates the trust relationships and communication protocols that make rapid information sharing possible during a crisis. Those relationships, once broken, are difficult to reconstitute on short notice.

The reduction in CISA's cybersecurity adviser corps from 164 to 97 nationwide directly affects critical infrastructure operators in sectors where federal coordination is most consequential: energy, water, transportation, healthcare, and communications [3]. Cybersecurity advisers function as the human-layer interface between CISA's central analytical capability and the specific operational environments of individual infrastructure operators. Their reduction degrades the agency's ability to deliver timely, context-aware guidance to the operators who need it most.

## The Adversarial Timing Problem

The institutional attrition at CISA is occurring precisely as the adversarial threat landscape is undergoing a qualitative escalation driven by AI-assisted attack tooling. CSA AI Safety Initiative research this cycle has documented ransomware operators using AI coding agents — specifically Cursor and Claude Opus — to iteratively develop and test EDR-evasion malware against live security stacks, representing an early-documented instance of this capability being applied in actual intrusions. AI-accelerated malware development compresses the window between vulnerability discovery and weaponized deployment, placing a premium on rapid threat intelligence sharing, coordinated incident response, and pre-attack resilience investments across the critical infrastructure ecosystem.

The timing mismatch creates compounding risk: reduced federal coordination capacity arriving precisely as adversary automation shortens attack cycles. A national cyber defense agency whose core mandate is to accelerate threat intelligence sharing and coordinate incident response is losing a third of its workforce at precisely the moment when the threat environment requires faster, not slower, institutional response. Reduced contractor oversight capacity, degraded adviser coverage, and eliminated threat intelligence channels are liabilities that compound as adversary automation increases. The credential leak reinforces this analysis: the same institutional conditions that allowed a contractor to maintain a public repository of government secrets for six months are the conditions under which a sophisticated adversary's dwell time goes undetected.

## What Remains Operational

It is important to distinguish between CISA functions that have been degraded and those that remain substantively intact. The Known Exploited Vulnerabilities catalog continues to receive updates: the agency published additions to the catalog as recently as May 27, 2026, indicating that the core vulnerability tracking function remains operational [11]. CISA's direct relationships with major critical infrastructure sector operators, particularly in energy and financial services, appear to be maintained through the existing sector-specific ISAC structure, which operates independent of CISA's internal staffing levels. The agency's published advisories, alerts, and binding operational directives continue to be issued. The risk is not that CISA has ceased to function; the risk is that it is operating at materially reduced capacity in exactly the coordination and outreach functions that serve organizations with the least independent security capability — state and local governments, smaller critical infrastructure operators, and mid-market enterprises.

# Recommendations

## Immediate Actions

Enterprise security teams and critical infrastructure operators that have historically relied on CISA for primary threat intelligence sourcing should treat the current environment as one requiring diversification of intelligence channels. Subscriptions to sector-specific ISACs that operate independently of federal funding — including the financial services FS-ISAC, the health sector H-ISAC, and the communications sector Communications ISAC — provide a partial substitute for the threat intelligence functions that MS-ISAC previously delivered to state and local constituencies. Organizations that have relied on CISA's cybersecurity adviser program for periodic assessment and guidance should assume lower availability of those advisory services and plan accordingly, either through independent assessment programs or through their sector ISAC's advisory services where available.

Security teams should also audit their current dependency on CISA-mediated communications during an active incident. The incident response playbooks of many organizations, particularly those in critical infrastructure sectors, include steps that assume CISA notification and coordination within specific timeframes. As CISA's advising capacity contracts, those timeframes may lengthen. Organizations should identify alternative points of contact — sector ISACs, FBI field offices, and regional Secret Service Electronic Crimes Task Forces — and ensure those relationships are established before they are needed.

## Short-Term Mitigations

The credential exposure incident highlights a specific risk management gap that applies well beyond CISA: contractor repositories and development environments require active monitoring for secret exposure, not just policy requirements. Organizations that rely on contractors for software development, cloud infrastructure management, or DevSecOps pipeline work should verify that those contractors have secret scanning enabled on all code repositories, that periodic audits of repository visibility and access control settings are part of the vendor management program, and that contractor compliance with credential management policies is verified rather than assumed. GitHub's built-in secret scanning, available on all public and most private repositories, is a first-order control that should be verified as enabled through API-based audit, not self-reported compliance.

State and local government security programs that previously relied on MS-ISAC threat intelligence should explore whether their state CIO or CISO offices have established replacement programs, and if not, should escalate that gap to state leadership as a funding and planning priority. The State and Local

Cybersecurity Grant Program, which CISA has identified as the replacement funding mechanism, requires active applications and has variable disbursement timelines — it does not function as a real-time intelligence substitute.

### Strategic Considerations

At the enterprise level, the broader lesson is that national cyber defense is not a fixed infrastructure that enterprises can treat as a dependable background input. Institutional capacity at federal agencies is subject to political, budgetary, and operational variation, and security programs built on the assumption of stable federal coordination will be exposed when that coordination degrades. The response is not to assume adversarial conditions and eliminate federal collaboration, but to ensure that enterprise security programs maintain independent capability across the core functions — threat intelligence, vulnerability management, incident response coordination, and sector-specific information sharing — that matter most.

For organizations with significant public-sector supply chains or critical infrastructure exposure, the current period warrants a formal review of how federal coordination dependencies are documented in business continuity and incident response plans. An enterprise that discovers mid-incident that a key coordination channel is less responsive than assumed is in a significantly worse position than one that identified the gap in advance and established alternatives. This is the same principle that underlies geographic redundancy for data centers and supplier diversification for procurement — the goal is not to predict the specific failure but to avoid single points of dependency in critical paths.

The credential exposure also reinforces a principle that applies across organizations of all sizes: contractor oversight is a security control, not an administrative formality. Contractors operate within the security posture of the organizations they serve, and gaps in oversight — whether caused by workforce reduction, bandwidth constraints, or organizational priority shifts — translate directly into gaps in posture. Embedding contractor oversight verification into security programs, rather than treating it as a procurement function, is a concrete mitigation against the class of failure that the Private-CISA incident represents.

## CSA Resource Alignment

The CSA AI Controls Matrix (AICM) addresses contractor and third-party risk through its supply chain and vendor management control domains, providing a structured framework for organizations assessing their contractor oversight posture. The MAESTRO threat modeling framework, developed for agentic AI systems, offers analogous principles for any environment where delegated authority — whether to AI

agents or human contractors — requires explicit scoping, monitoring, and revocation protocols. Organizations reviewing their contractor security management practices in light of the Private-CISA incident will find MAESTRO's treatment of principle-of-least-privilege and delegation scope relevant.

The CSA STAR program provides a mechanism for cloud service providers and federal contractors to demonstrate security assurance through self-assessment and third-party certification. The disclosure that a CISA contractor had disabled GitHub's secret scanning and maintained a publicly accessible repository of government credentials for six months underscores the gap between policy compliance (meeting a stated requirement) and verifiable assurance (demonstrating continuous adherence to a control). STAR's continuous monitoring tier addresses precisely this gap by moving from point-in-time attestation to ongoing evidence of control operation.

CSA's Zero Trust guidance directly addresses the architectural assumptions that the Private-CISA incident exposes as insufficient. A Zero Trust architecture treats every credential as a potential point of compromise and requires that access decisions be made on the basis of verified identity, device posture, and least-privilege scope — not on the basis of assumed trust in a network segment or contractor relationship. The forty-eight-hour window during which exposed AWS GovCloud keys remained active after repository takedown illustrates the operational cost of not having automated credential rotation and anomaly detection integrated into the access management architecture.

# References


[1] Brian Krebs. "CISA Admin Leaked AWS GovCloud Keys on Github." Krebs on Security, May 2026.

[2] Tim Starks. "CISA credential leak raises alarms, and Capitol Hill demands answers." CyberScoop, May 2026.

[3] Eric Geller. "CISA workforce cut by nearly one-third so far." Cybersecurity Dive, 2025–2026.

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

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

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

[7] Justin Doubleday. "Plankey withdraws as CISA nominee." Federal News Network, April 2026.

[8] Federal News Network Staff. "CISA director void leaves cyber agency embroiled in uncertainty." Federal News Network, January 2026.

[9] Eric Geller. "Acting CISA chief defends workforce cuts, declares agency 'back on mission'." Cybersecurity Dive, 2026.

[10] Guillaume Valadon / GitGuardian. "How We Got a CISA GitHub Leak Taken Down in Under a Day." GitGuardian Blog, May 2026.

[11] CISA. "CISA Adds Three Known Exploited Vulnerabilities to Catalog." CISA.gov, May 27, 2026.

[12] Kevin Poireault. "US Cuts Federal Funding for MS-ISAC Cybersecurity Program." Infosecurity Magazine, September 2025.

[13] Tonya Riley. "Senator requests 'urgent' classified briefing on CISA's internal credential leaks." Axios, May 19, 2026.

[14] Zack Whittaker. "US cyber agency CISA exposed reams of passwords and cloud keys to the open web." TechCrunch, May 19, 2026.