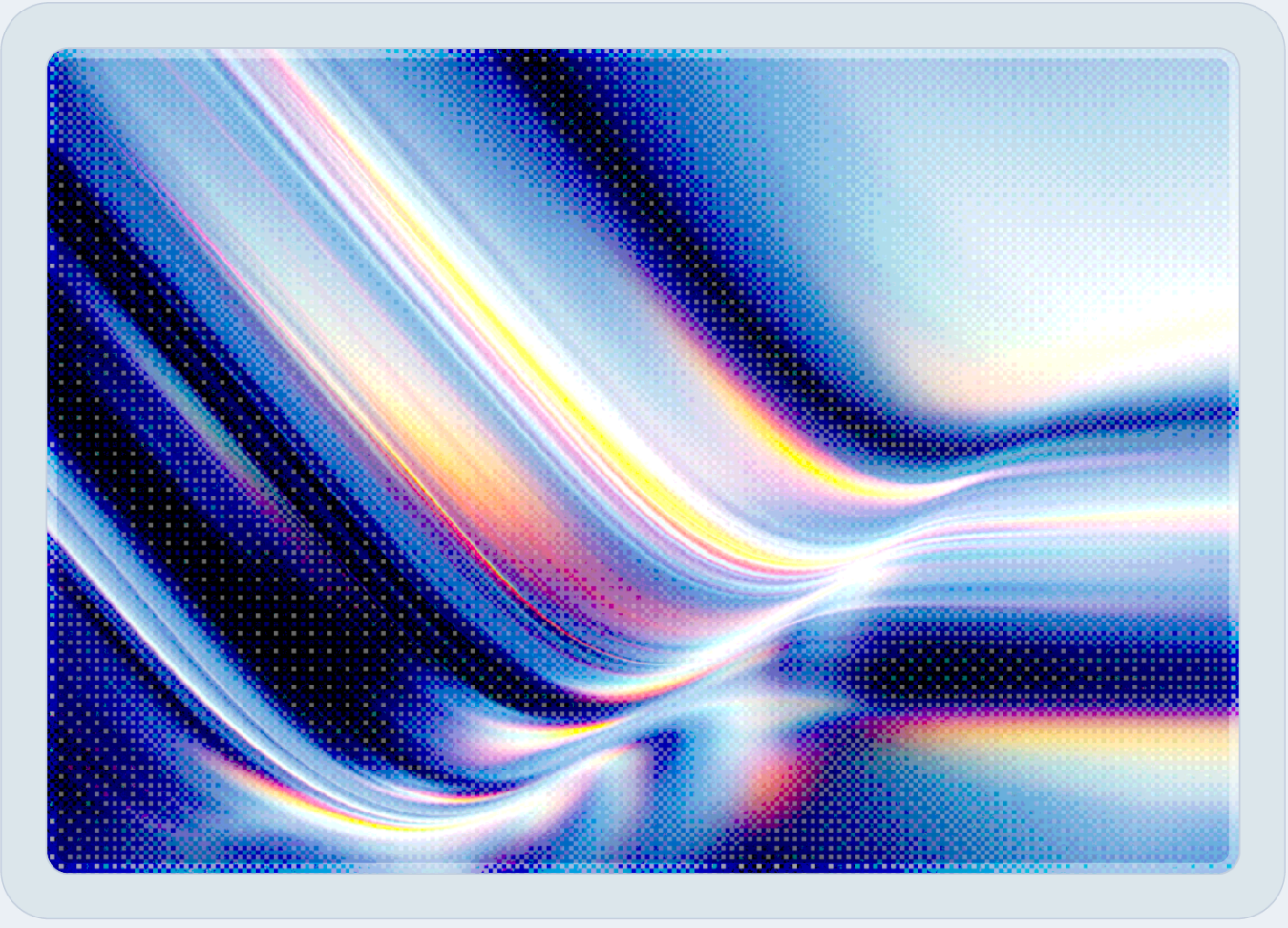
CSAI Foundation | Cloud Security Alliance

Private-CISA: GovCloud Leak and the Hollowing of U.S. Cyber Defense

DevSecOps Credential Exposure and Institutional Risk at America's Cyber Backstop

2026-05-26

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

- From November 13, 2025 through May 15, 2026, a public GitHub repository named "Private-CISA" — maintained by a Nightwing contractor — exposed 844 MB of CISA's internal DevSecOps infrastructure, including administrative credentials for three AWS GovCloud servers, Kubernetes manifests, GitHub Actions workflows, ArgoCD application files, Terraform code, Entra ID SAML certificates, and plaintext passwords. [1][2]
- Among the exposed files was one labeled "importantAWStokens" — a nomenclature that inverted the most basic security principle behind credential protection. The AWS keys it contained remained valid for approximately 48 hours after the repository was taken offline, creating a sustained window for exploitation after disclosure. [1][3]
- Exposed Artifactory credentials raised the possibility of software supply chain compromise: an adversary with valid credentials could have injected malicious code directly into CISA's internal software build pipeline. [4]
- The contractor had disabled GitHub's default secret-scanning push protections, and many credentials followed a predictable pattern of platform name plus current year — representing a failure of basic credential hygiene in an organization whose core mandate is to improve national cyber hygiene. [1][5]
- CISA has lost approximately one-third of its workforce since January 2025, has shuttered its Stakeholder Engagement Division, operationally suspended the Election Security Program, defunded the Multi-State Information Sharing and Analysis Center (MS-ISAC), and dissolved the Critical Infrastructure Partnership Advisory Council (CIPAC), compressing its defensive perimeter during a period of elevated nation-state cyber activity. [6][7][8][16]
- On May 19, 2026, Senator Maggie Hassan requested an urgent classified briefing from CISA's acting director, and House Homeland Democrats separately demanded answers — placing congressional oversight pressure on an agency already navigating leadership vacancies and depleted capacity. [9][10]

Background

The Cybersecurity and Infrastructure Security Agency is the federal government's primary civilian authority for defending critical infrastructure from cyber threats and for coordinating national incident response. Since its establishment under the Cybersecurity and Infrastructure Security Agency Act of 2018, CISA has served as the convening body between federal agencies, state and local governments, private sector operators, and international partners — providing vulnerability intelligence, threat assessments, incident response assistance, and security guidance to the sixteen critical infrastructure sectors defined under Presidential Policy Directive 21.

That mandate has existed in increasing tension with a sustained contraction of the agency's human and financial resources. CISA entered fiscal year 2025 with approximately 3,400 employees. By December 2025, that number had fallen to roughly 2,400 — a reduction of nearly 1,000 workers, or more than 29 percent of the total workforce. [6] The Trump administration's proposed fiscal year 2026 budget would reduce the agency's staff further to 2,324 and cut total funding by approximately $495 million. [6][11] In April 2026, the agency's cyber partnerships were described as being at a "standstill" following the elimination of CIPAC and the defunding of MS-ISAC [7][15], and in May 2026 CISA advised critical infrastructure operators to prepare for potential cyber outages [12] — a step that security analysts interpreted as a signal of reduced incident-response capacity.

It is against this backdrop of institutional contraction that the Private-CISA credential leak emerged. The controls that would have caught this exposure earlier — active secret scanning, contractor oversight, credential lifecycle management — were either disabled, deprioritized, or never enforced. Whether those specific failures were caused directly by workforce reduction or reflect longer-standing governance gaps is not established by the available record, but the pattern is consistent with the organizational conditions that sustained resource contraction can create.

Security Analysis

The Private-CISA Repository: Scope and Timeline

On May 15, 2026, Guillaume Valadon, a security researcher at GitGuardian, identified a public GitHub repository associated with a Nightwing contractor employee who held an administrative role within CISA's DevSecOps infrastructure. [1][5] The repository had been publicly accessible since at least November 13, 2025, when its initial commits were logged. Security researchers suspect the contractor

was using the repository as an informal mechanism to synchronize files between a work laptop and a home computer, effectively using a public code-hosting platform as a personal file transfer service for government materials. [1]

The repository contained 844 MB of data spread across the working tree and Git history. [2] The exposure covered the full width of CISA's software delivery infrastructure: Kubernetes configuration manifests and secret-related YAML files that described the structure of CISA's container orchestration environment; ArgoCD application definitions that map deployed services to their source configurations; GitHub Actions workflow files detailing the CI/CD automation logic used to build, test, and deploy internal software; Terraform infrastructure-as-code files; internal documentation backups; and operational scripts. Critically, one file — titled "importantAWStokens" — contained administrative credentials for three Amazon AWS GovCloud servers. Additional material included GitHub personal access tokens, Entra ID SAML certificates, Artifactory repository credentials, and plaintext passwords that followed an easily predictable naming convention. [1][3][5]

GitGuardian contacted CISA at approximately 10:00 a.m. Eastern on May 15. The repository was taken offline by approximately 6:00 p.m. the same day. However, CISA did not immediately rotate the exposed AWS credentials. The GovCloud keys remained valid for an additional 48 hours after the repository was removed, a period during which any party who had cloned or archived the repository could have used those credentials to authenticate against CISA's most sensitive cloud infrastructure. [3]

The CI/CD Pipeline Dimension

The significance of the leaked repository extends beyond the direct credential exposure. Security researchers who analyzed the full contents noted that the files collectively describe the internal mechanics of how CISA builds and deploys software — a DevSecOps blueprint for the agency's software supply chain. [4] The Kubernetes manifests, ArgoCD files, and GitHub Actions workflows reveal pipeline topology: which repositories feed which deployment targets, how secrets are injected into CI runners, and which infrastructure components host CISA's internal tooling.

Among the most sensitive category of exposed materials were the Artifactory credentials. Artifactory is a binary artifact repository manager used to store compiled packages, container images, and build artifacts before they are promoted to production environments. An attacker with valid Artifactory credentials could, in principle, replace or poison build artifacts with modified versions containing malicious payloads — causing CISA's own software delivery pipeline to propagate compromised code into internal systems. This resembles, in structure, the software supply chain attack class described in published advisories on CI/CD security risks. [13] Whether the Artifactory credentials were valid at the time of the repository's takedown has not been publicly confirmed.

The GitHub Actions workflows themselves represent a second risk vector. Workflow files define what commands execute inside CISA's CI runners and which secrets those runners are authorized to access. An adversary who could have modified those workflows before the repository's removal — or who retained a cloned copy of the repository and discovered that the referenced secrets remained valid — would have possessed an instruction set for compromising CISA's internal automation infrastructure.

Static Secrets as Structural Vulnerability

The Private-CISA incident is a manifestation of a well-documented architectural anti-pattern: the use of long-lived static credentials that are stored alongside the infrastructure they protect. [14] Static credentials — AWS access keys, personal access tokens, SAML certificates, and API keys that do not expire on short rotation schedules — accumulate across configuration files, CI scripts, and operational runbooks over time. As they proliferate, the probability that any single copy ends up in an unauthorized location trends upward with the number of people and systems that handle them.

GitHub provides multiple default controls designed to interrupt this accumulation at the point of publication. Push protection, enabled by default in organizations with GitHub Advanced Security, scans commits for recognized secret patterns and blocks pushes that include them. Secret scanning passively monitors public and private repositories for new credential patterns after they are committed. The CISA contractor had disabled both protections, removing the automatic safety net that would have caught the "importantAWStokens" file and the embedded AWS keys before they were ever published. [1]

The password patterns exposed in the repository underscore the depth of the credential hygiene failure. Many passwords were structured as the name of the platform followed by the current year — a pattern trivially enumerable in any credential-stuffing campaign. This convention appears not to have been challenged by any automated password strength enforcement or internal security review.

The durable remedy is not procedural improvement to static credential handling but migration away from static credentials entirely. Short-lived workload identity credentials, provisioned through OIDC federation between CI systems and cloud providers, expire within minutes and are issued on demand by the cloud identity provider rather than stored anywhere a developer can retrieve them. The CISA incident illustrates, in a high-visibility context, the difference between an organization that has completed this migration and one that has not.

Institutional Capacity and the Compounding Risk

The credential leak cannot be fully analyzed in isolation from the broader institutional context in which it occurred. The contractor oversight and security controls that would have caught this exposure earlier — regular auditing of public repository activity, active enforcement of GitHub organization settings,

credential rotation policies, and supply chain security reviews — are organizational capabilities that require trained personnel to implement and sustain. The available evidence documents that these controls were absent or disabled; it does not conclusively establish that workforce reduction was the proximate cause, though the co-occurrence is analytically significant.

CISA's contraction since January 2025 has removed many of the people who would normally have exercised that oversight. Beyond raw headcount, the agency has lost entire functional divisions. The Stakeholder Engagement Division, which coordinated cybersecurity improvements with state and local governments, private sector partners, and international allies, was effectively closed in mid-2025 through the elimination of nearly all 95 employees. [7] The Election Security Program — 14 positions managing $39.6 million in annual activity — was operationally shuttered in early 2025 and proposed for complete elimination in the administration's FY2027 budget. [8] The dissolution of CIPAC removed the primary structured forum through which CISA engaged with private sector critical infrastructure operators on sensitive threat information. The defunding of MS-ISAC eliminated the organization's primary channel for sharing threat intelligence with the more than 18,000 state, local, tribal, and territorial government entities it historically served. [7]

The acting director of CISA's Cybersecurity Division, in a February 2026 town hall for division staff, advised that "there are some people in this room in programs we are going to turn off," signaling that further mission contraction was forthcoming. [12] Separately, CISA's advisory in May 2026 urging critical infrastructure operators to prepare for potential cyber outages represented a public signal that the agency's incident-response capacity had changed from prior expectations. [12] Abrupt downsizing during a period of elevated nation-state cyber activity — as documented in recent intelligence community threat assessments [16] — may produce not merely a marginal reduction in defensive coverage but a qualitatively different risk posture for federal and private-sector entities that previously relied on CISA as their primary backstop.

Congressional oversight has accelerated in response to the credential leak specifically, but the structural fragility it revealed is the product of a longer institutional trajectory. Senator Hassan's May 19, 2026 letter requesting an urgent classified briefing, and the parallel House Homeland Democratic demand for answers, reflect growing recognition that CISA's diminished capacity presents a national security concern. [9][10] Whether that recognition translates into durable resource restoration — given the competing priorities in a tight budget environment — remains to be determined.

Recommendations

Immediate Actions

Federal agencies and their contractors operating in GovCloud or FedRAMP environments should treat this incident as a trigger for immediate credential audits. Any organization using Nightwing as a contractor, or using contractors who hold administrative access to cloud environments, should audit whether contractor-managed GitHub accounts have secret scanning and push protection enabled. AWS GovCloud administrative credentials, SAML certificates, Artifactory tokens, and GitHub personal access tokens with administrative scope should be rotated on an emergency basis if there is any doubt about their exposure history. The 48-hour delay in rotating CISA's own GovCloud keys after disclosure should be treated as a cautionary data point, not a benchmark.

GitHub organization owners should audit organization security settings to confirm that secret scanning and push protection are enabled and cannot be overridden by individual repository administrators or external contributors. The ability to disable these controls at the repository level, as occurred in the Private-CISA case, reflects a permissions architecture that allows contributors to remove the safeguards protecting both themselves and the organization.

Short-Term Mitigations

The most durable correction to the static secrets problem is migration to OIDC-based workload identity credentials for all CI/CD systems interacting with cloud infrastructure. AWS GovCloud, Azure Government, and Google Cloud all support OIDC federation with GitHub Actions, GitLab, and other major CI platforms, allowing CI runners to request short-lived credentials on demand rather than consuming long-lived stored secrets. Organizations that complete this migration remove the specific risk that the Private-CISA repository represented — long-lived credentials stored in configuration files — because there are no persistent credentials to leak. Residual risks around OIDC trust configuration, token scope, and identity provider integrity require separate attention.

Terraform, Kubernetes manifests, and ArgoCD application configurations should be audited for embedded credential references. Infrastructure-as-code files are a common vector through which static credentials migrate from configuration management into version control. Secrets management platforms — HashiCorp Vault, AWS Secrets Manager, Azure Key Vault — should be the sole authoritative source for secrets, with references to those platforms injected at runtime rather than stored in configuration files.

Contractor access governance requires explicit attention at federal agencies. Contractors with administrative access to cloud environments should be subject to continuous GitHub activity monitoring, organization-level enforcement of security controls they cannot override, and periodic access reviews that include audit of repository visibility settings.

Strategic Considerations

CISA's institutional capacity to fulfill its statutory mandate — defending federal civilian agency networks, coordinating critical infrastructure security, and leading national cyber incident response — has been materially degraded by sustained workforce reduction, program elimination, and the dissolution of long-established partnership mechanisms. Congress should evaluate the relationship between CISA's current resource posture and the threat landscape it is expected to address, recognizing that restoring defunded programs like MS-ISAC and CIPAC requires rebuilding organizational trust and relationships that took years to establish, not merely appropriating funds.

The Private-CISA incident also surfaces a governance question about contractor security accountability. CISA's contractors operate with privileged access to the same systems CISA is charged with defending. Contractor security hygiene, credential management practices, and repository access controls should be subject to the same standards — and the same enforcement — as those applied to federal employees. The current incident suggests a gap between those standards.

More broadly, the incident demonstrates that the same organizational conditions that enable government to defend others — trained personnel, enforced tooling standards, active oversight, and functional partnerships — are themselves security properties that require sustained investment. When institutional capacity erodes, the controls that prevent the next credential leak erode with it.

CSA Resource Alignment

This incident connects to several areas of CSA's published guidance and ongoing work.

CSA's **AI Controls Matrix (AICM)** and the underlying **Cloud Controls Matrix (CCM)** address credential management, access control, and supply chain risk governance. CCM domain IAM-09 covers identity and access management policies that apply to contractor access; CCM SEF-01 addresses security policy enforcement. The failure to enforce GitHub organization-level secret scanning controls reflects a gap in the IAM and change-management controls domains.

CSA's research on **workload identity federation** provides a technical migration path away from the static credential architecture that made the Private-CISA repository so damaging. The transition from long-lived API keys to OIDC-based ephemeral credentials applies directly to government and contractor CI/CD environments operating in GovCloud.

The **STAR (Security Trust Assurance and Risk)** program's third-party attestation model is relevant to the contractor oversight dimension of this incident. Requiring contractors with privileged access to federal cloud environments to complete STAR attestation — demonstrating specific controls around credential management, code repository governance, and access reviews — would establish a documented baseline for what is currently an informal and apparently under-audited relationship.

CSA's **Zero Trust guidance** provides a conceptual framework for the access architecture that should govern contractor cloud credentials: no persistent privilege, just-in-time access requests, and continuous verification rather than long-lived administrative keys. The "importantAWStokens" file is the precise anti-pattern that Zero Trust architecture is designed to eliminate.

References

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

[2] CyberNews. "US cybersecurity agency CISA exposed passwords and AWS credentials on public GitHub repository." CyberNews, May 2026.

[3] SOCFortress. "CISA Under Fire Following Major GovCloud Credential Leak." Medium, May 2026.

[4] Axis Intelligence. "CISA GitHub Data Leak 2026: Full Technical Breakdown (AWS Keys + Supply Chain Risk)." Axis Intelligence, May 2026.

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

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

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

[8] Infosecurity Magazine. "Trump Budget Plan to Cut Nearly 1000 Jobs at Cyber Agency CISA." Infosecurity Magazine, 2025.

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

[10] Nextgov/FCW. "House Homeland Dems request CISA briefing amid report of leaked agency credentials." Nextgov, May 2026.

[11] Defense One. "2026 budget proposal would axe one-third of CISA workforce." Defense One, June 2025.

[12] Cybersecurity Dive. "CISA will shutter some missions to prioritize others." Cybersecurity Dive, 2026.

[13] CISA. "Defending Continuous Integration/Continuous Delivery (CI/CD) Environments." CISA, June 2023.

[14] Akeyless. "CISA's GitHub Leak Exposed a Static Secrets Problem." Akeyless Blog, May 2026.

[15] Federal News Network. "CISA cyber partnerships face 'standstill' amid cuts." Federal News Network, April 2026.

[16] Office of the Director of National Intelligence. "Annual Threat Assessment of the U.S. Intelligence Community." ODNI, April 2025.