Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 07| 2025

Research Article **Received:** 05-06-2025| **Accepted:** 28-06-2025 | **Published:** 17-07-2025

Deconstructing Government-Grade Access Management Systems in the Cloud

Naveen Parameshwarappa
Cornell University, Ithaca, New York, USA

Abstract: The challenge that government agencies face in terms of security and everyday functionality falls on a tight line between having an ironclad security requirement and the flexibility required on a day-to-day basis in other operations. Access management has morphed dramatically as cloud solutions penetrate deeper into federal infrastructure backbones. This article dissects how modern identity frameworks—with particular focus on Salesforce implementations—have upended traditional security approaches while threading the compliance needle. Readers discover the nuts-and-bolts mechanisms enabling HSPD-12 adherence, personnel vetting integration, and multi-tiered access provisioning across sprawling user populations. Security practitioners once juggled disconnected systems requiring cumbersome manual coordination; contemporary architectures eliminate these friction points through hardened API connections between background check databases, personnel systems, and permission controls. Gone too are one-size-fits-all approaches, replaced by nuanced configurations including inheritance-capable role structures, context-aware attribute controls, time-bounded privileged access, and federated administration patterns. The roadmap extends toward never-trust architectures, always-on identity confirmation, risk-calibrated security challenges, and pattern-recognition safeguards spotting anomalous behaviors. The article illuminates how federal security teams harness cloud platforms to both strengthen protective measures and unlock cross-agency capabilities that remained frustratingly out of reach under legacy paradigms.

Keywords: Federal Identity Management, Cloud Security Compliance, Zero Trust Architecture, Personnel Vetting Integration, Tiered Access Control.

INTRODUCTION

The federal landscape presents a curious paradox - agencies must simultaneously lock down sensitive assets while remaining nimble enough to fulfill diverse missions. Access management architectures have undergone seismic shifts, particularly as cloud technologies entrench themselves across government infrastructure. This transformation runs deeper than mere technology replacement; it represents a fundamental rethinking of security design principles throughout federal environments.

Scale creates its own peculiar challenges—federal entities must authenticate millions of employees, contractors, and partners accessing thousands of sensitive systems. Traditional approaches centered around perimeter defenses and static permissions flounder when confronted with contemporary operational demands and increasingly sophisticated attackers targeting credential weaknesses. Research published in Complex Adaptive Systems Modeling exposes how these conventional approaches lack the necessary flexibility to counter emerging threats across large, distributed ecosystems (Habiba, U. *et al.*, 2014).

Cloud-driven identity frameworks offer compelling alternatives to legacy approaches, delivering elasticity, durability, and adaptability beyond what on-premises solutions can provide. These platforms establish cohesive identity governance across departmental boundaries while enforcing stringent controls mandated by federal directives. Complex Adaptive Systems research validates how distributed security architectures demonstrate exceptional resilience against evolving threats while preserving operational functionality during disruptive events, critical for government functions demanding uninterrupted availability (Habiba, U. *et al.*, 2014). This resilience proves particularly crucial for systems maintaining FedRAMP compliance while supporting essential operations spanning multiple agencies (Google Cloud).

This analysis explores how cloud-based identity and access frameworks—particularly implementations on FedRAMP-authorized platforms like Salesforce—transform federal security operations while satisfying critical mandates, including HSPD-12. The FedRAMP authorization process establishes standardized security assessment methodology, authorization protocols, and continuous monitoring requirements for cloud offerings, enabling federal entities to adopt cloud technologies with appropriate safeguards (Google Cloud). Through examination of architectural patterns, migration approaches, and operational considerations, this exploration illuminates how government agencies navigate transitions toward more robust, adaptable access management systems while addressing unique federal requirements.

***Corresponding Author:** Naveen Parameshwarappa

DOI- https://doi.org/10.5281/zenodo.16032619

Leveraging authorized cloud platforms unlocks novel capabilities for cross-organizational collaboration, real-time security monitoring, and adaptive authentication previously unattainable under legacy paradigms. Complex Adaptive Systems research suggests interconnected security frameworks continuously evolve, responding to emerging threats, making them particularly suited for high-security environments with dynamic operational demands (Habiba, U. *et al.*, 2014). These capabilities help agencies fulfill missions more effectively while maintaining rigorous security postures required for government operations. Subsequent sections examine these capabilities in depth, providing comprehensive insights into how cloud-based access management reshapes federal security architecture while maintaining compliance with programs like FedRAMP, establishing security benchmarks for cloud providers serving government clients (Google Cloud).

THE EVOLUTION OF FEDERAL ACCESS MANAGEMENT

Traditional federal access management was comprised of separated islands utilizing manual identity checks and other permission-granting procedures. The unsynchronised strategies led to inefficiencies in process, user experiences, and security vulnerabilities. Government IT architecture research reveals how these splintered systems created dangerous security gaps, particularly where multiple interconnected systems meet. NIST Special Publication 800-204 highlights critical weaknesses in legacy approaches—inconsistent security policy enforcement across system boundaries, creating exploitable vulnerabilities at integration points between separate identity domains (Chandramouli, R. 2019). These architectural flaws prove especially problematic for access management systems that must preserve security integrity across diverse application landscapes.

Federal access management history reveals progression through multiple architectural eras, from mainframe centricity through client-server deployments, arriving now at cloud-native paradigms. Each transition addressed specific limitations while introducing novel capabilities. Pre-cloud implementations typically featured on-premises directory services alongside separate provisioning mechanisms, authentication services, and governance tools—an approach creating substantial integration hurdles and inconsistent security enforcement. NIST architectural guidance pinpoints how monolithic security implementations struggle to scale in modern distributed environments, recommending instead composable security services that adapt to changing requirements while maintaining consistent policy enforcement (Chandramouli, R. 2019). This guidance proves particularly relevant for federal agencies transitioning from legacy identity infrastructure toward more flexible cloud-based implementations.

The federal modernization push has elevated cloud-based solutions as viable alternatives addressing persistent challenges. The Cloud Smart strategy, supplanting the earlier Cloud First policy, prioritized security and governance considerations over migration speed alone. This strategic pivot proved particularly significant for identity and access management, serving as foundational security infrastructure underpinning all other systems. FedRAMP represents a crucial enabler for this transformation, establishing standardized assessment frameworks for authorizing cloud services for government deployment. This approach reduces duplicative evaluation efforts across agencies while ensuring cloud providers maintain appropriate security controls aligned with federal mandates (Risk, F. 2012). The rigorous assessment methodology includes comprehensive documentation reviews, security testing, and continuous monitoring, validating ongoing compliance with federal standards.

Federal agencies are using cloud platforms to build single access management environments that support tens of thousands of users across various departments. These systems comply with high security and provide fluid experiences to administrators as well as end users. Newer implementations provide flexibility in authentication mechanisms, contextual policies of access control, and automated architectures of provisioning services that adjust to changes in the organization in near-real time. NIST architectural recommendations for distributed systems emphasize centralized policy management with distributed enforcement—a model perfectly aligned with cloud-based access management implementations (Chandramouli, R. 2019). This approach enables consistent security control across diverse environments while providing flexibility, adapting to varying operational requirements across different federal agencies.

Publisher: SARC Publisher

The transition toward cloud-based access management unlocks cross-agency collaboration capabilities previously impractical under traditional approaches. These platforms have federated authentication paradigms that enable agencies to establish trusting relationships that help them share information in a controlled manner and maintain governance boundaries. This is a valuable ability when it comes to sharing tasks with another performing body, coordinating a disaster response, or dealing with situations that require quick inter-organizational cooperation. The FedRAMP certification process creates trust in agencies that cloud services can support their federal security requirements, so it is possible to use such services to support sensitive activities, taking due risk considerations (Risk, F. 2012). This standardized security framework proves instrumental in establishing cross-agency trust necessary for effective identity federation in high-security environments, enabling collaborative capabilities previously unattainable with isolated security implementations.

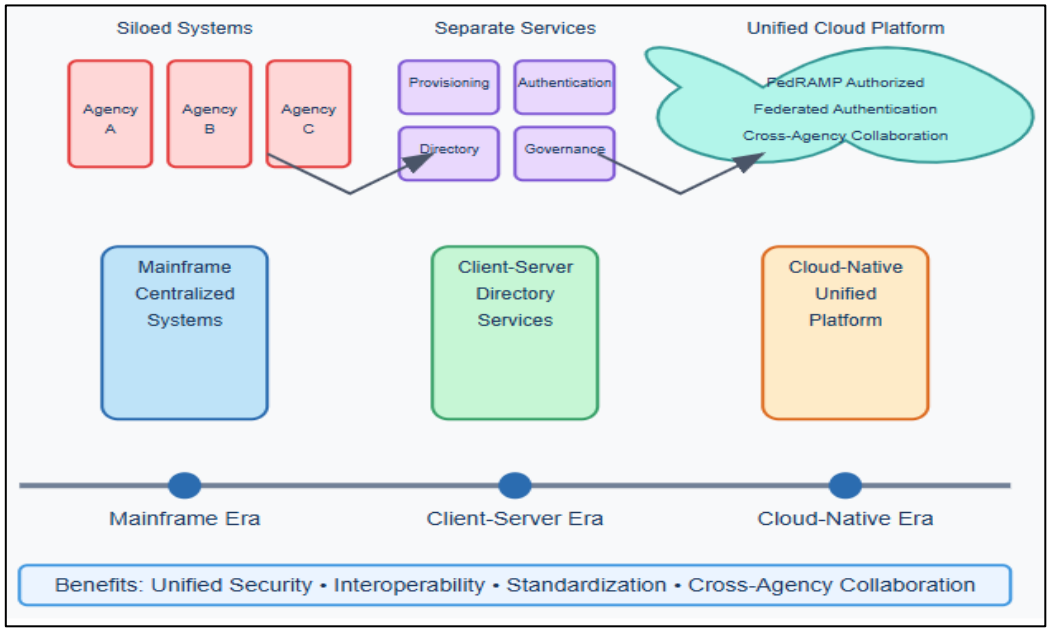

Figure 1: The Evolution of Federal Access Management (Chandramouli, R. 2019; Risk, F. 2012)

COMPLIANCE WITH HSPD-12 AND FEDERAL STANDARDS

Homeland Security Presidential Directive 12 turned federal identification upside down, mandating uniform credentials verifiable across agency lines. Gone were the days when each department crafted unique ID systems; HSPD-12 birthed standardized PIV cards for civilian agencies and CAC cards throughout the Defense. This watershed directive forever altered how federal workers prove identity and gain system access. The FICAM Architecture delivers nuts-and-bolts guidance for implementing these requirements, spotlighting standardized processes that balance security with practical access needs (ID Management, 2023). The framework tackles thorny questions around cloud-based verification—how distributed systems can check credentials against central authorities without punching holes in security perimeters.

Cloud access systems tackle HSPD-12 demands through real-time credential checks against the Federal PKI infrastructure. When employees tap cards against readers, these systems ping certificate authorities instantly, rejecting expired or revoked credentials on the spot. Cryptographic validation must satisfy FIPS 201-2 standards—no small feat given the complexity of certificate chains and revocation processes. Cloud environments face unique validation hurdles: maintaining unbroken trust chains across distributed systems while handling certificate revocation lists efficiently. FICAM guidance digs into these technical weeds, mapping implementation paths that satisfy security mandates without drowning agencies in operational quicksand (ID Management, 2023). This roadmap proves invaluable when navigating the maze of PKI integration in elastic computing environments.

Publisher: SARC Publisher

Fingerprints and facial recognition add crucial HSPD-12 compliance layers in high-risk scenarios. Modern credentials carry embedded biometric data, demanding cloud systems support matching capabilities without compromising sensitive biometric markers. These systems walk a tightrope: enabling verification while keeping actual biometric data away from cloud providers' storage. Clever implementations build secure API bridges to agency-operated matching services, maintaining appropriate data boundaries. CISA's Zero Trust model charts pathways incorporating these biometric checks into authentication flows as agencies climb the zero trust ladder, boosting security without frustrating legitimate users (Cybersecurity & Infrastructure Security Agency, 2023). The guidance emphasizes calibrating verification intensity—applying fingerprint checks where warranted by sensitivity, bypassing them where excessive friction damages productivity.

Identity proofing forms the bedrock of HSPD-12 implementation—establishing who belongs before issuing credentials. These types of verification processes can be executed on a cloud access platform by utilizing orchestration engines that can be configured to ensure the separation of requester, approver, and issuer is adequate. A detailed audit record will record all verification procedures which will meet security and compliance requirements. These procedures follow National Institute of Standards and Technology 800-63A standards of identity confirmation completeness and accuracy. Federal agencies configure these workflow engines to match agency-specific procedures while maintaining standards compliance. FICAM offers practical blueprints for these workflows, stressing consistent processes safeguarding every identity lifecycle stage (ID Management, 2023). These templates prove priceless when agencies abandon paper-shuffling for digital workflows that boost security while cutting processing delays from weeks to days.

Table 1: HSPD-12 Compliance Components in Cloud-Based Federal Access Management (ID Management, 2023; Cybersecurity & Infrastructure Security Agency, 2023)

Compliance Component	Key Capability	Implementation Challenge	Federal Standard	Security Benefit
Digital Credential Validation	Real-time PKI verification	Trust chain maintenance	FIPS 201-2	Immediate credential revocation
Biometric Verification	Fingerprint/facial recognition	Data boundary protection	NIST 800-76	Enhanced authentication in high-risk scenarios
Identity Proofing	Configurable orchestration	Separation of duties	NIST 800-63A	Verified Identity Foundation
Workflow Automation	Digital approval processes	Cross-agency standardization	FICAM	Reduced processing time

PERSONNEL VETTING AND ONBOARDING INTEGRATION

The cloud platforms have transformed personnel vetting operations through the development of a smooth integration channel between the background investigation systems, the HR systems, and the access control systems. There were times when individual organizational fiefdoms would manage security clearances manually by email chain and on paper. The Defense Counterintelligence and Security Agency's personnel security guidance underscores how critical timely information exchange between vetting authorities and access systems has become—decisions must reflect current trustworthiness assessments, not outdated investigations (Defense Counterintelligence & Security Agency). This guidance particularly addresses how modern integration capabilities support the shift away from periodic reinvestigations toward continuous vetting models, enabling risk management through live information flows between previously disconnected systems.

Automated provisioning based on background investigation status eliminates dangerous security gaps between clearance decisions and system access adjustments. Direct digital connections now link security clearance platforms with access management systems, ensuring permissions perfectly mirror current vetting status. Cloud implementations accomplish this through hardened API integrations with authoritative vetting systems, establishing automated workflows that translate investigation results into access decisions while preserving appropriate separation between personnel security functions and access management. DCSA guidance specifically tackles

Publisher: SARC Publisher

how these connections implement the "whole-person concept" in access determinations, weighing all relevant factors when granting access to sensitive information (Defense Counterintelligence & Security Agency). This comprehensive approach demands sophisticated integration capabilities, synthesizing data from multiple authoritative sources to produce accurate, timely access decisions.

Real-time HR system synchronization ensures access permissions accurately mirror current organizational roles, not positions employees held months ago. This synchronization forms the backbone of least privilege enforcement, granting access exclusively to resources required for current positions. Cloud platforms establish this synchronization through secure data channels between HR systems and access platforms. These integrations leverage event-driven architectures to propagate personnel changes immediately, eliminating dangerous delays typical in batch-oriented approaches. NIST Special Publication 800-63-3 tackles authoritative source requirements, emphasizing that "digital identity creation requires identity proofing, the process by which a CSP collects, validates, and verifies information about a person" (Grassi, P. A. *et al.*, 2017). This guidance specifically addresses how authoritative connections support security principles by ensuring identity information remains current across connected systems.

Dynamic clearance-based access adjustments enable security teams to implement nuanced controls to respond to personnel trustworthiness changes. When clearance levels shift, access rights automatically adjust accordingly—no manual intervention required. Cloud platforms support these dynamic adjustments through policy-based access controls, incorporating clearance status as authorization decision factors. DCSA guidance tackles how these dynamic adjustments support risk management principles in personnel security, ensuring that "any doubt is resolved in favor of national security" while avoiding unnecessary restrictions hampering mission execution (Defense Counterintelligence & Security Agency). This balanced approach demands sophisticated access mechanisms implementing nuanced security policies that adapt to changing risk profiles.

Automated personnel onboard and offboard eliminate hazardous security loopholes as personnel are changed. In cases where contractors need to be changed or where employees need to be moved, the work is done easily through orchestrated workflows across systems to provision the access and, where necessary, revoke it. Cloud platforms coordinate these complex processes, ensuring all necessary steps are executed in the proper sequence with appropriate approvals. NIST Special Publication 800-63-3 specifically addresses identity lifecycle management, emphasizing proper "binding, updating, renewing, and terminating identity proofing, credentials, and authenticators" (Grassi, P. A. *et al.*, 2017). This guidance shapes how federal agencies handle identity processes in cloud environments, particularly ensuring identity information remains synchronized throughout the entire identity lifecycle.

Cloud architecture enables these integrations through standardized APIs and hardened data exchange protocols, replacing manual handoffs that previously created security vulnerabilities. Distributed cloud platforms establish secure connections between systems operated by different organizations residing in separate environments. These technical capabilities, combined with standardized interfaces, create integrated vetting ecosystems spanning organizational boundaries. DCSA guidance emphasizes information sharing in effective personnel security, stressing "timely transmission of relevant information" between stakeholders involved in clearance processes (Defense Counterintelligence & Security Agency). NIST digital identity guidelines establish secure protocols for identity information exchange between federated systems (Grassi, P. A. *et al.*, 2017). Together, these frameworks guide agencies implementing integrated personnel security capabilities, enhancing protection while streamlining operations.

Table 2: Personnel Vetting and Onboarding Integration in Federal Cloud Environments (Defense Counterintelligence & Security Agency; Grassi, P. A. *et al.*, 2017)

Integration Component	Function	Key Benefit	Technical Implementation
Background Investigation Integration	Links security clearance data with access systems	Eliminates gaps between clearance decisions and access rights	Hardened API connections with authoritative vetting systems

Publisher: SARC Publisher

HR System Synchronization	Keeps access permissions aligned with current roles	Ensures least privilege enforcement in real-time	Event-driven architecture with secure data channels
Dynamic Access Adjustment	Automatically updates permissions when clearance changes	Maintains security without manual intervention	Policy-based access controls with clearance attributes
Lifecycle Workflow Management	Streamlines onboarding and offboarding processes	Prevents security vulnerabilities during transitions	Orchestrated workflows with proper sequencing

TIERED ACCESS MANAGEMENT FOR LARGE-SCALE DEPLOYMENTS

Federal environments with 80,000+ users present daunting management challenges that cloud platforms address through layered security architectures. Mass user populations, tangled organizational structures, and diverse mission requirements create access complexities that break traditional approaches. Enterprise-scale federal deployments typically encompass hundreds of applications with varying security requirements distributed across multiple physical locations. CISA's Continuous Diagnostics and Mitigation program tackles these challenges head-on, focusing intensely on identity management across sprawling federal enterprises (Cybersecurity & Infrastructure Security Agency). CDM recognizes identity verification and access control as foundational security pillars, which are particularly crucial as tens of thousands of users access hundreds of applications spanning organizational boundaries.

Role-based access frameworks with inheritance capabilities form the foundation of scalable federal access management. These frameworks group related permissions into defined roles aligned with organizational functions, dramatically reducing entitlement sprawl. Cloud implementations leverage inheritance capabilities, enabling hierarchical permission models that cascade through organizational structures. This architecture proves particularly valuable in federal environments with clearly defined reporting structures influencing access requirements. NIST Special Publication 800-53 Revision 5 explicitly addresses role-based access control, directing organizations to "establish and administer privileged user accounts in accordance with role-based schemes organizing allowed system access and privileges into roles" (Force, N. J. T. 2020). This guidance emphasizes structured role design matching organizational functions while maintaining granular control, creating scalable access management for massive federal deployments.

Attribute-based access control transcends static role limitations, enabling context-aware decisions factoring user characteristics, resource sensitivity, requested actions, and environmental conditions. This approach implements nuanced security policies, adapting to changing circumstances without manual intervention. Cloud platforms excel at ABAC implementation, processing complex authorization rules instantly across distributed environments. CDM emphasizes dynamic security capabilities focused on continuous monitoring rather than point-in-time compliance checks (Cybersecurity & Infrastructure Security Agency). This continuous assessment enables federal agencies to implement adaptive access controls to respond to changing risk conditions, leverage cloud capabilities, and balance security with operational flexibility across vast enterprises.

Just-in-time privileged access eliminates standing admin rights—the crown jewels attackers target relentlessly. Instead, administrative capabilities become available only when needed through time-bound authorizations requiring explicit approval. When maintenance completes, elevated permissions automatically expire, minimizing exposure windows. Cloud platforms enable sophisticated workflow automation, ensuring consistent implementation of approval requirements while capturing comprehensive audit trails. NIST SP 800-53 Revision 5 tackles this approach directly in control AC-6(2), mandating that organizations "employ least privilege principles, allowing only authorized accesses necessary to accomplish assigned tasks according to organizational missions" (Force, N. J. T. 2020). The control specifically demands time-limited privileged access, directing organizations to "automate mechanisms temporarily disabling inactive accounts and automatically terminating temporary accounts after defined periods."

Delegated administration distributes management responsibilities while maintaining central oversight—the only practical governance approach at enterprise scale. This model pushes access

Publisher: SARC Publisher

decisions to appropriate organizational levels where business requirements receive proper context. Cloud platforms support these models through administrative hierarchies enforcing separation of duties while preserving centralized visibility. CDM specifically addresses distributed management capabilities, enabling "effective security control implementation across complex federal enterprises while maintaining governance oversight" (Cybersecurity & Infrastructure Security Agency). This balanced approach enables operational efficiency while preserving security controls, addressing critical challenges in federal environments with diverse mission requirements spanning organizational boundaries.

This layered approach ensures precisely calibrated access—nothing more, nothing less—while enabling governance at enterprise scale. Complementary access models enable sophisticated security policies balancing protection with usability, adapting to specific requirements across varied systems. Cloud platforms provide distributed processing capabilities, advanced policy engines, and comprehensive monitoring, enabling effective oversight across vast user populations. NIST SP 800-53 Revision 5 provides implementation guidance through integrated controls in the Access Control family, acknowledging that "organizations may implement combinations of access policies and mechanisms based on security requirements" (Force, N. J. T. 2020). This flexible approach, combined with CDM's continuous monitoring emphasis, gives federal agencies frameworks for implementing effective access management at scale while maintaining appropriate security controls across complex environments.

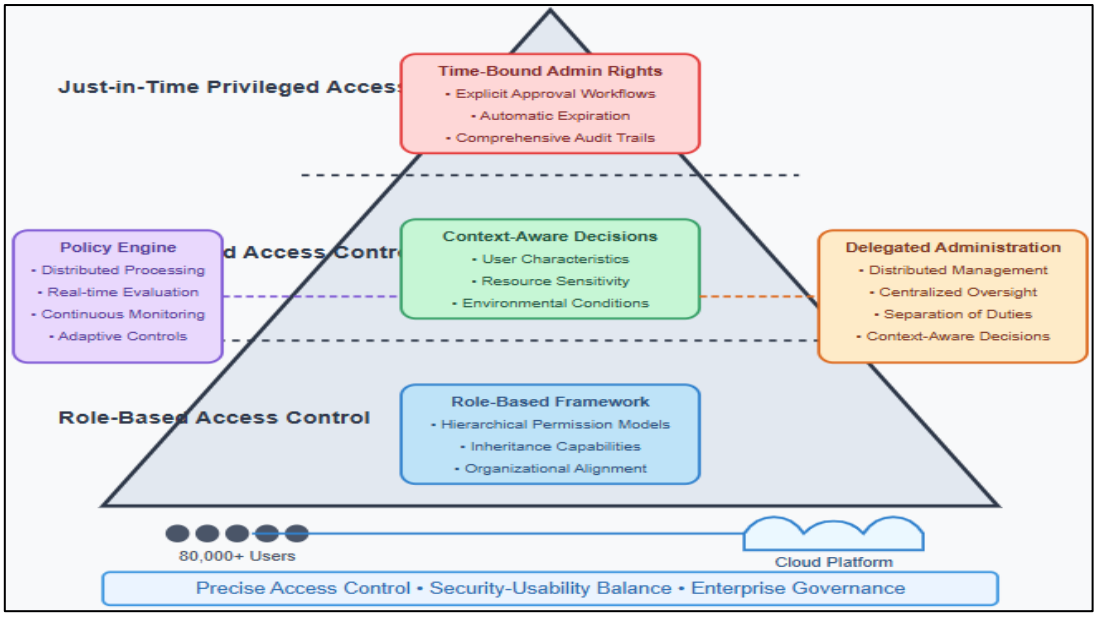

Fig 2: Tiered Access Management for Large-Scale Federal Deployments (Cybersecurity & Infrastructure Security Agency; Force, N. J. T. 2020)

THE FUTURE OF GOVERNMENT ACCESS MANAGEMENT

Federal access management sits at a crossroads while agencies overhaul aging systems amid relentless threat evolution. Tomorrow's security frameworks must bend toward operational realities, particularly supporting scattered workforces tapping sensitive assets from coffee shops, home offices, and field locations. The Cloud Strategy underscores how security models must "support staff accessing systems securely regardless of physical location," spotlighting cloud technology's role in enabling this flexibility without sacrificing protection (Federal Chief Information Officers Council). This vision demands tearing down verification orthodoxies that cling to network boundaries, pivoting toward constant validation regardless of connection origin.

Zero Trust tears up security's oldest playbook—no more assuming devices inside the firewall deserve implicit trust. This approach treats every access attempt with healthy suspicion, demanding proof before unlocking resources. The Zero Trust Strategy pulls no punches, telling agencies bluntly to "never trust, always verify" and build systems where "physical network location grants zero automatic advantage" ((Young, S. D. 2022). The

Publisher: SARC Publisher

directive plants identity verification squarely as the cornerstone, emphasizing that rigorous authentication becomes critical when network location means nothing—a radical departure from decades of perimeter-focused thinking.

Session-long authentication stretches security beyond the login screen, constantly checking user legitimacy through typing patterns, mouse movements, command sequences, and location consistency. This persistent verification catches attackers who slip past initial gateways by stealing credentials, dramatically cutting dwell time when compromise occurs. The Cloud Strategy specifically pushes implementations "continuously matching ongoing behavior against established patterns" (Federal Chief (Information Officers Council). These persistent checks represent security's evolution beyond the traditional "verify once, trust until logout" model that creates massive vulnerability windows.

Adaptive authentication dials security friction up or down based on risk signals—standard access from typical locations with expected behaviors slides through smoothly, while unusual patterns trigger additional hurdles automatically. Morning email checks face minimal obstacles, while attempts to export sensitive data from overseas hotel networks at 3 am trigger stepped-up challenges. The Zero Trust directive instructs agencies to build systems that "gauge risk dynamically for each request" and "throw additional verification barriers before high-risk operations" (Young, S. D. 2022). This approach strikes the elusive balance between protection and productivity, right-sizing friction rather than forcing everyone through maximum security regardless of context.

Pattern recognition drives threat hunting beyond simple rule matching, spotting subtle behavioral anomalies that signal compromise. These systems learn individual user rhythms, device characteristics, and system baselines, flagging meaningful deviations while filtering normal variations. Machine learning spots sophisticated attacks slipping past traditional defenses, particularly insider threats and low-and-slow campaigns. Both strategic directives highlight these capabilities, forming the backbone of next-generation federal security operations (Federal Chief Information Officers Council; Young, S. D. 2022). These tools augment human analysts with silicon brains that constantly adapt to shifting attack methodologies.

These security advances actually reduce friction for legitimate users—the seemingly contradictory reality that better protection can mean smoother experiences when implemented thoughtfully. Each innovation builds atop existing cloud foundations rather than requiring wholesale replacement. The Zero Trust Strategy acknowledges this practical reality, advising agencies to "leverage existing investments while strategically adopting technologies enabling better security models" ((Young, S. D. 2022). This pragmatic approach recognizes federal constraints—agencies must keep operations running while evolving security postures. Cloud platforms provide the springboard for these advances, helping agencies implement controls protecting national secrets without hamstringing critical missions.

CONCLUSION

Cloud access management has fundamentally rewired federal security practices through scalable, fault-tolerant frameworks addressing long-standing government security headaches. These platforms establish consistent identity verification protocols crossing agency boundaries while satisfying rigorous federal mandates. Standardized integration capabilities eliminate dangerous security gaps and administrative bottlenecks that plagued siloed approaches, creating unified security ecosystems that adapt to shifting mission requirements. The march toward zero trust models, continuous verification, and smart security controls builds naturally upon this cloud foundation, strengthening protection while cutting friction for legitimate users. Federal digital transformation journeys increasingly position access management as a security architecture cornerstone, enabling robust protection alongside operational flexibility amid mounting threat complexity. The architectural patterns and implementation approaches explored throughout this analysis offer practical blueprints for scaling effective access management across massive federal enterprises, addressing both security imperatives and mission demands. Government security practitioners increasingly recognize cloud-based access management not merely as a technology migration but as a fundamental security transformation, enabling both enhanced protection and operational agility previously unattainable with legacy approaches.

REFERENCES

1. Habiba, U., Masood, R., Shibli, M. A., & Niazi, M. A. "Cloud identity management

Publisher: SARC Publisher

security issues & solutions: a taxonomy." *Complex Adaptive Systems Modeling* 2.1 (2014): 5.
2. Google Cloud, "FedRAMP,". https://cloud.google.com/security/compliance/fedramp
3. Chandramouli, R. "Microservices-based application systems." *NIST Special Publication* 800.204 (2019): 800-204.
4. Risk, F. "Authorization Management Program (FedRAMP),"." *Concept of Operations (CONOPS)", Version* 1 (2012).
5. ID Management, "Federal Identity, Credential, and Access Management (FICAM) Architecture," (2023): https://www.idmanagement.gov/arch/
6. Cybersecurity & Infrastructure Security Agency, "Zero Trust Maturity Model,"(2023). https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
7. Defense Counterintelligence & Security Agency, "Transforming Federal Personnel Vetting,".: https://www.cdse.edu/Portals/124/Documents/student-guides/shorts/PS008-guide.pdf
8. Grassi, P. A., Garcia, M. E., & Fenton, J. L. "Digital Identity Guidelines (翻訳版)." *NIST special publication* 800 (2017): 63-3.
9. Cybersecurity & Infrastructure Security Agency, "Continuous Diagnostics and Mitigation (CDM) Program https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program
10. Force, N. J. T. "NIST Special Publication 800-53 Revision 5–Security and Privacy Controls for Information Systems and Organizations." *Gaithersburg, MD, Sep* (2020).
11. Federal Chief Information Officers Council, "From Cloud First to Cloud Smart," *CIO Council Strategic Documents*. https://cloud.cio.gov/strategy/
12. Young, S. D. "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," M-22-09, (2022).: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Parameshwarappa, N. "Deconstructing Government-Grade Access Management Systems in the Cloud." *Sarcouncil Journal of Engineering and Computer Sciences* 4.7 (2025): pp 719-727.

Publisher: SARC Publisher