From AI to Access: Identity and Security Reshape the Federal Workforce

A shift in digital environments demands rethinking the on/off-boarding process for skills-based requirements and access.

With the ever-present reality of the $80 billion federal legacy debt[1], agencies are challenged to transform their systems, workforce and cultures to enhance mission agility. Success or failure in this transformation will depend on the ability to attract and retain exceptional human technologists and securely deploy the next generation of AI autonomous agents.

Eliminating the Onboarding Tax

Federal hiring is a technical bottleneck, not just a human resources challenge. The government's ability to compete for the nation's best technologists depends on providing a modern, friction-free onboarding experience that mirrors the private sector. Currently, federal user provisioning can take up to three days because IT must manually create accounts in five or more legacy and cloud systems.[2]

This "onboarding tax" can erode morale from day one and contribute to early churn among top talent. To win the war for technical talent, federal leaders need an identity security fabric that eliminates these manual, brittle processes.

Facilitating a Mobile Workforce

National security demands fully embracing elasticity between agencies, task forces and research centers. Federal hiring initiatives like the U.S. Tech Force, for example, enable software engineers to work on a Department of War modernization project on Monday and a Department of Veterans Affairs digital health project on Wednesday.

However, traditional agency identity silos treat every move as a new-hire event. This mobility gap frustrates subject-matter experts moving between tours of duty or interagency coordination bodies. There is an urgent need to replace static, agency-specific access with a centralized identity security fabric. Access should follow the person and their verified skills, not the building they are in. That requires a move to modern identity systems that can verify competencies, clearance levels and employment history from diverse sources in real time, enabling dynamic, policy-based access at mission speed.

Securing the Autonomous AI Workforce

The modern workforce now includes the deployment of AI agents and non-human identities. Federal AI use cases nearly doubled in 2024[3], yet many remain in pilot phases due to security risks. For chief AI officers looking to move from concept to deployment, managing these autonomous agents is a critical priority.

"We must move toward a future where we are credentialing both our human federal workers and our AI agents with the same level of rigor and trust … Ensuring both have verifiable identities and validated skills is the only way to maintain the integrity of our digital government," said the White House's former science and technology advisor Arati Prabhakar.[4]

Agencies must treat AI agents as first-class identities with the same lifecycle management, governance and security oversight as human engineers. Securely scaling government's 1,100+ AI use cases it has outlined in the federal AI use case inventory requires an identity infrastructure that manages how human users access AI and how AI agents access data simultaneously.

The Solution: An Identity Security Fabric

The technology to move from fragmented, manual silos to an enterprise authorization-as-a-service model is available today. It is easy-to-deploy and fully compliant with NIST 800-63 and zero-trust compliance requirements as well as frameworks such as the National Cyber Strategy.

Federal agencies can adopt a centralized identity security fabric. The Okta Identity Platform provides a digital control plane that secures AI and every other identity, from machine to human manages who a person or AI agent is and what they are allowed to do across the entire agency. Whether managing propulsion engineers for NASA Force or interdisciplinary teams at National Science Foundation (NSF) Tech Labs, a unified identity layer must federate identities and scope access to shared resources while maintaining compliance.

Identity is not just a security pillar; it is the foundation for an agile, secure and modern federal workforce. By modernizing the identity of every human and AI agent across its full lifecycle, agencies can ensure they remain a magnet for the talent required for national security.

By adopting Okta Workforce Identity, agencies can pivot from manual, siloed maintenance to mission agility. Key functions of this platform include:

- **Single sign-on (SSO):** Allows employees and contractors to use one secure account to access all necessary tools.
- **Adaptive multi-factor authentication (AMFA):** Provides a layer of security, such as a code on a phone or a biometric scan, that adapts based on risk factors like location or device.
- **Automated lifecycle management (ALM):** Automatically creates accounts during hiring and revokes them the moment a person leaves, ensuring no ghost accounts remain as security risks.
- **Okta Identity Governance:** Acts as a bridge to protect older on-premises systems that were not originally built for the cloud.
- **Okta Universal Directory:** Secures all types of identities including employees, customers, partners and AI agents within a neutral and extensible identity security fabric. A core component of the Okta Identity Platform, it helps organizations centralize identity management at the heart of their technology stack to improve security and efficiency.

"Granting access to secure enclaves remains one of our most significant hurdles in the Zero Trust journey. Between legacy PIV card requirements and the push for modern phishing-resistant MFA, the identity silos we've built over decades make it nearly impossible to provide a seamless 'day one' access experience for the workforce. We are essentially fighting our own infrastructure to let our people in." —Eric Mill, Executive Director for Cloud Strategy, General Services Administration (GSA)

[1] Deborah Collier, August 2025, "GAO Reconfirms Federal IT Must Be Modernized." Citizens Against Government Waste; [2] GAO-25-107653 July 2025 "Artificial Intelligence: Generative AI Use and Management at Federal Agencies; [3] "Assessing the state of AI adoption across the federal government,"" Brookings Institution, April 15, 2026; [4] White House OSTP Briefing on AI Workforce Integrity, January 15, 2025.