okta

Building flexible enterprise Identity

Okta's approach for public sector organizations and supporting entities

In recent years, leaders across federal organizations have faced a myriad of challenges, including a global health crisis, geopolitical conflicts, and economic uncertainty. These leaders represent a diverse group from global military operations to complex federal agencies with regional entities and seasonal teams, as well as federal systems integrators (FSIs) and the defense industrial base (DIB).

Navigating challenges requires a continuous effort to maintain an efficient, cost-effective, and flexible organizational structure. Additionally, adhering to federal cloud security standards like FedRAMP and DoD Impact Levels is crucial to help ensure a secure and compliant digital infrastructure.

For large agencies, structural change offers the potential for significant growth — but only if it can be done in an agile and sustainable manner.

Identity's role in federal organizational agility Identity is foundational to continued organizational changes because it sits at the intersection of the people, technology, and resources organizations rely on to accelerate daily missions. Identity helps to securely manage users and their access to increase productivity and efficiency when it matters — from disaster recovery efforts and 24/7 international workforces to warfighters in theater.

> "The most critical enabler for agility is a clear, inspiring mission that every member of the team identifies with and is working towards. Unfortunately, that inspiration can often get buried under the weight of unnecessarily complex processes and structures."[1]
>
> Kirk Rieckhoff, Senior Partner and leader of McKinsey's Defense practice

The challenges large or complex federal organizations face

The technology environments of larger federal organizations are complex, presenting significant challenges for securely enabling streamlined collaboration, including:

Managing identities across siloed organizations: IT teams and Mission Owners struggle to effectively and efficiently manage users as they join, move, or leave an organization, especially across multiple systems for partners, PIV/CAC, and non-smart card users and resources.

Implementing least privilege in a heterogeneous world: Autonomous federal business units, regional entities, seasonal teams, and third parties can create significant challenges to centralize and standardize Identity and access policies to deliver least privilege.

Maintaining productivity across a distributed workforce: Managing a distributed set of agency users with separate domains and IT environments inhibits organizational health and performance. Employees, contractors, and partners cannot effectively access mission-relevant resources.

[1] https://www.airandspaceforces.com/how-at-scale-agility-could-address-structural-challenges-in-the-department-of-the-air-force/

Okta can help

With Okta, agencies, FSIs, and the DIB can advance their tech ecosystem by accomplishing three major strategic outcomes:

1. **Deploy a federal-centric, adaptable management model**
   Okta's unique hub and spoke architecture enable agencies and their users to be managed separately or brought together depending on the public sector's evolving mission needs. Agencies can choose to centralize all users and resources with consolidated access controls and enable decentralized control with business units, branches, and regional offices. Or, to support different phases of mission-driven investments in the federal workforce, they can deliver a hybrid model.
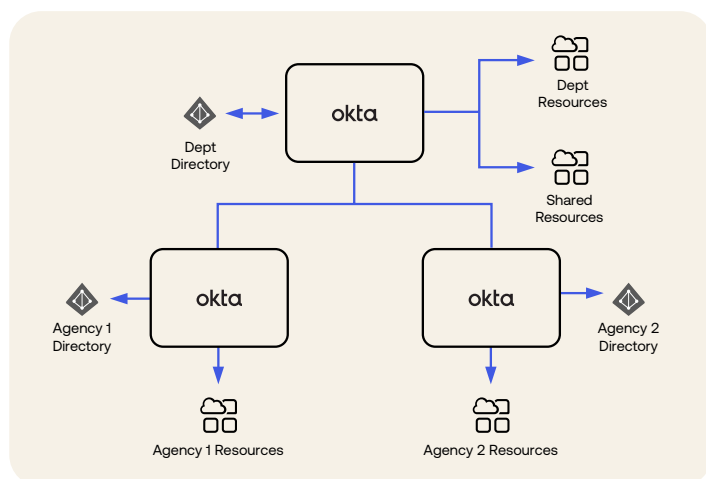
2. **Create an automation-driven single source of truth**
   With Okta, Mission Owners can integrate and manage federal users and resources into a unified Identity framework. This enables IT teams to automate and orchestrate any joiner, mover, and leaver (JML) actions to deliver operational accuracy and efficiencies across user populations. Okta's rich JML context means that users aren't just assigned or removed from applications but can be assigned specific roles or license entitlements, all from a centralized Identity solution.

3. **Centralize the federal security control plane**
   Federal security executives can drive consistent security and centralized access policies for all users and resources at every phase of evolving centralized or decentralized structures, addressing possible risk and delivering real-time reporting across the entire organization.

Building an agile Identity foundation maximizes operational strategy

By adopting an agile, flexible approach to Identity, federal agencies and government contractors' leaders can create significant value for their organizations and:

Improve public sector agility: Create a technology foundation that adapts to organizational changes quickly to maximize impact. This includes optimizing agency or organization mergers seamlessly. An Identity-first approach with Okta can eliminate the need for multiple identities and ensure neutral support for applications from all vendors, including custom-developed ones.

Improve government efficiency: Create repeatable and scalable processes through automation that foster control at the broader enterprise level while local controls are maintained at the agency, component level, or business unit.

Increase productivity: Alleviate the downtime linked to workforce UX issues by enabling multiple users under one setup. Especially for government contractors, the blend of enterprise and agency ID eradicates the necessity of managing multiple identities. This consideration simplifies access, reduces setup time, and enhances productivity.

Enhance security: Centralize and standardize policies for the most important resources within an organization, maintaining the highest thresholds of authentication.

The right Identity approach can maximize the structural change that is critical to large and complex organizations' evolution and growth. Okta can help.

Learn more at: okta.com/federal or contact our sales team at **okta.com/contact-sales**.