Modernizing IT in Government: Facilitating the Public Sector's Move to the Cloud

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

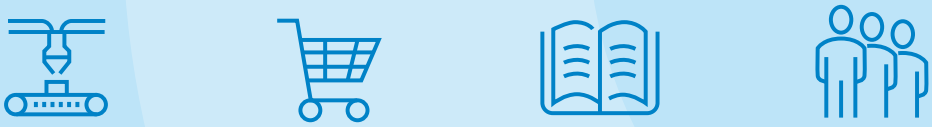
Modernizing IT in Government: Facilitating Secure Information Sharing

Government Agencies: New Demands, New Technology Needs

From the smallest town agencies to the largest federal departments, new software solutions typically provide convenience and brand-new challenges in equal measure. Finding a mix of solutions that satisfy employee needs, meet public demands, and work well together is a challenge IT stakeholders run up against on a daily basis.

This is particularly important because government agencies are adopting new IT systems and upgrading current ones at a faster rate than ever before, which has created an environment where modern solutions—especially cloud-based ones—need to be compatible with legacy systems that have often been in place for years. Moreover, with robust security and data protection being absolutely essential in the public sector, IT teams are left trying to manage different users across different systems and applications in a way that will not put the organization at risk.

Data breaches according to Verizon's 2018 Data Breach Investigations Report (DBIR)



	Manufacturing	Retail	Education	Public
Breaches	71	169	101	**304**
Incidents	536	317	292	**22,788**

Source: Verizon 2018 Data Breach Investigations Report. For the public sector, ensuring easy access and information sharing while keeping data secure is an ongoing challenge.

Two major expectations have pushed the issue, forcing agencies to rethink the breadth, depth, and overall shape of their digital footprints:

- **Changing customer demands.** As a rule, customers are more time-strapped and less accepting of bureaucratic inefficiency than ever. Because they are immersed in a day-to-day world where convenience trumps all, they have come to expect a smooth experience from public agencies at the local, state, and federal level. Long wait times are unacceptable, as is downtime due to upgrades or confusing interfaces. People want self-service and around-the-clock access—the sort of user experience they get from a large consumer site like Amazon—and this is true of both internal and external users.
- **The standard government "do more with less" ethos.** When they work as prescribed, newer cloud-based solutions have real potential to provide greater efficiency and productivity in any workplace, including government offices. Here lies the challenge for many institutions, though. The pressure is on to make smart use of their limited budgets to adopt new solutions and migrate to the cloud, all the while working within government mandates and keeping legitimate security concerns in mind.

In total, these demands have led to a public sector that is more invested in new technologies than ever before. US federal agencies alone are estimated to have spent $6.5 billion on cloud technology in 2018, 32% more than cloud spending in 2017. It's a brave new world for government IT; one that comes with difficulties unique to the vertical.

A Shifting Govtech Landscape

Government agencies traditionally rely on an IT footprint that's very different from that of a private business. Budgets, regulations, security concerns, scale, and the nature of the user base all contribute to the diverse needs government IT personnel must consider.

Then there are the substantial differences between old and new. While a perceived lack of need ("If it ain't broke, don't fix it") or the desire for security-through-obscurity has left many agencies to function around legacy systems as long as possible, it is fair to say friction between older, on-premises tools and newer cloud options has finally come to a head in many offices. Certain critical processes may run through a newer cloud-based system, while others may be processed through solutions built or acquired years in the past. Increasingly, these systems must be able to share data, a degree of interplay that may require specialized knowledge and upskilling on IT's part.

Cloud adoption in government agencies

Roughly **50%** of federal organizations "actively use" cloud services.

$1.2 billion: Increase in federal cloud spending from 2017 to 2018.

9%: Percentage of federal tech spending dedicated to provisioned, cloud-based services.

79% of federal IT managers say they would trust cloud vendors with data.

69% of decision-makers say they need cloud access to do their work.

78% of IT managers who have moved to the cloud say it helped them achieve reliability goals.

Sources: Understanding Cloud Adoption in Government, Nextgov, Debunking Government Cloud Myths

In this sense, the challenge surrounding government technology is not so much about the age of the systems as the *age difference* between different solutions. Because the average government footprint is sprawling, and because upgrades tend to take place on an ad-hoc basis, it can be difficult to integrate a collection of solutions to resemble a unifying system. And though baseline functionality represents one large and distinct aspect of this challenge, the complexity truly comes through in an area government agencies have struggled with for years: centrally managing users and related authentication practices across the collection of systems an organization has come to rely on over the years.

Access and Security Challenges at the Core of Government IT Overhaul

Scale is a problem that often sets government IT challenges apart from similar issues in the private sector. That's true of general architecture and doubly true of access and identity management. When a single agency oversees IT systems that serve thousands upon thousands of employees and customers, finding a solution that provides user trust through smart policies, strong security, and ease of use may seem almost impossible.

With this high-level issue in mind, government agencies' authentication challenges can be broken down into three main components:

1. **Large user rosters.** As noted above, government IT teams must deal with authorizing and provisioning massive numbers of users across their systems. Without appropriate tools and strategies in place, simply granting the right people access to the right systems can be a massive undertaking. The onboarding, provisioning and lifecycle management of users

becomes a full-time job that eats into the productivity of IT teams.

2. **Security, privacy, and enforcement.** Sprawling systems and the account management challenges they present create substantial security risks. As an example, personnel may employ weak passwords and reuse them across different networks and applications. Ineffective access management also results in dormant and abandoned accounts that may still technically be active—a massive security risk in and of itself. Without being able to manage credentials or having adequate command and control over accounts, the organization cannot properly protect itself. Regardless of other security measures that are in place, the entire enterprise is put at risk.
3. **Interplay.** Employees must be able to access work-critical systems in an efficient and secure manner, whether the systems they access share data or not. No matter the number of solutions and applications used, they need to operate with speed and ease to improve productivity.

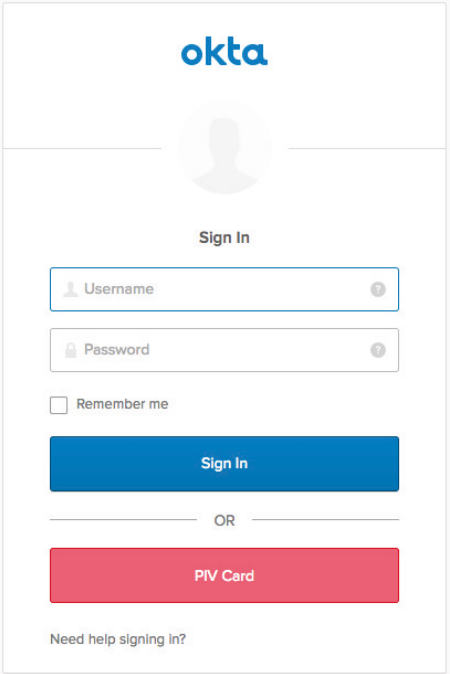
The three core challenges of secure information sharing

Balancing security and ease of access: How do we get to the cloud faster? How do we make it easy for the right people to securely access the right systems?

Scalability: How do we implement it across the breadth of our operations? Can we do this for both internal and external users?

Integrability: How do we ensure it works with all the tools we rely on, on-premises or otherwise?

Simplifying Identity and Security with Okta



Taken together, these challenges underscore the need for a new solution in the public sector: one that weaves all systems into a cohesive whole, regardless of hosting location, creator, overall function, or the information it touches and transmits. It also has to meet this goal without adversely affecting security or adding bloated cost to an agency's existing infrastructural opex/capex. Moreover, a worthwhile solution will centralize control, grant end-users useful self-service options, and automate time-consuming authentication tasks such as password reset requests and provisioning.

Finding a solution that meets this slate of identity and access management challenges may seem like a moonshot—but Okta can help your agency get there. With a collection of FedRAMP- and CAC/PIV-enabled tools that integrate with homegrown, on-premises solutions as well as the cloud-based SaaS tools government agencies rely on most (such as Box, Office 365, Google, and Salesforce), Okta brings centralized identity control and integrated security solutions to any disparate collection of cloud-based and on-premises systems.

As a result, IT stakeholders can minimize access- and identity-based challenges

as they consider their transition from legacy systems to the cloud, with tools that help them meet their goals along every step of the journey. Whether your agency is almost entirely making use of on-premises and homegrown solutions, or completing a planned cloud migration, Okta can assist.

Okta's Solutions

Single Sign-On: Simplifying access, one user at a time

Challenge: Government perimeters tend to be broad and diverse. One solution may be on-premises and custom, while the next may be cloud-based and provided by a vendor. Because of this, finding a single sign-on (SSO) offering robust and versatile enough to manage every application in a government roster has long seemed like a white whale.

Solution: Not so with Okta's Single Sign-On. End-users can utilize the same credentials across an agency's local and cloud-based applications with SSO, regardless of source. Users have a significantly easier time managing their identities, while IT can condense a pile of system-specific password reset requests into a single-point, self-service function. Throw in over 5,500 pre-built integrations to the most popular cloud solutions (Office 365, AWS, Slack, Box) and the ability to support legacy systems, and your agency has the perfect SSO solution. Okta offers the option to provide PIV authentication to SSO-based applications using PIV and CAC smartcards.

Adaptive Multi-Factor Authentication: Flexible, context-sensitive security

Challenge: Over 80% of breaches involve weak or stolen credentials. It's a sobering fact, and one that becomes all the more serious when one realizes how frequently government institutions are targeted for digital theft and other cyberattacks. The same broad, diverse perimeters that make government systems so challenging to manage make them extremely attractive to attackers; this is especially true when considering the amount of valuable, sensitive data these solutions store and transmit.

Solution: Okta's Adaptive Multi-Factor Authentication (MFA) has been designed to add a number of agency-selected factors to the login equation. For instance, an agency could choose to verify with the Okta Verify app or with a One-Time Password (OTP) pushed to a known mobile device. Okta can even integrate with Personal Identity Verification and Common Access Cards (PIV / CAC), and is Federal Information Processing Standards (FIPS) 140-2 certified. To reduce login friction while improving security, Adaptive MFA also allows for contextual access management, so when a user logs in from a new location, device, or network, additional authentication factors can be asked for. With the FIPS certification Okta meets NIST 800-63v3 compliance requirements for strong authentication for AAL levels.

Universal Directory: Easy to use multi-source integration

Challenge: Managing users is at the core of any identity and access management activity, but it's also a task that can quickly eat into valuable time. Too often, chasing users across a collection of systems becomes an ongoing chore for IT personnel, who may have to help with everything from password resets to provisioning issues. By the same token, a single oversight—a near certainty when dealing with so many fine details—can carry serious security implications, granting former users access to systems they should no longer be able to access.

Solution: Okta's Universal Directory aims to meet the challenge of running a single thread through multiple systems. Users, groups, and devices from across systems are combined to a single point of truth, vastly simplifying life for IT teams and providing full lifecycle support for the accounts under its banner. With the ability to seamlessly integrate with AD, LDAP, and other directory stores, Universal Directory makes user management easier than ever: Changes made on one end (an HR system, for instance) are automatically reflected on the other end.

Okta Integration Network: Deep, pre-built integrations for your critical apps

Challenge: Box. AWS. Salesforce. Office 365. Government agencies at all levels rely on apps like these, and they need to work together seamlessly. With employees needing reliable access to the systems they work on and customers having heavier user-experience expectations than ever before, a lack of interoperability is simply unacceptable. So too is sustained downtime as systems are implemented and integrated.

Solution: The Okta Integration Network makes this challenge a thing of the past. Over 5,500 pre-built integrations help government agencies avoid vendor lock-in and keep their systems fluid, no matter what needs the future may throw at them. From SSO to user profiles and security analytics, the Okta Integration Network is designed to help agencies make better use of current software solutions and free them to choose whatever applications will make most sense in the future—a far cry from the siloed systems of old.

Lifecycle Management: Automated management and better security

Challenge: In the past, huge government userbases meant huge problems with provisioning and lifecycle management, a fact that holds for both internal and external accounts. Determining precisely who gets access to which systems can become a major chore and time-sink, and that's before considering the severe security risks that can occur when accounts aren't properly—and promptly—deprovisioned.

Solution: With its automated take on provisioning and management, Lifecycle Management offers huge savings in time and money. Provisioning and deprovisioning naturally become easier under an automated system, as do access audits and hunts for rogue accounts; the tool can also be highly beneficial in reducing instances of shadow IT, another phenomenon with real potential to introduce security problems. Okta Lifecycle Management can even be extended to provision your custom apps using SCIM.

Conclusion: An Easier Transition

Government agencies exist in a unique space in terms of technical needs and ongoing evolution. Critical legacy systems must be logically and functionally linked to newer, cloud-based solutions with tools that support the transition from the former to the latter as they happen.

Recognizing the need is only the first step, however. Certain solutions—SSO, for instance—have proven especially difficult to "weave around" vast government digital footprints, leaving technological stakeholders to throw up their hands and assume it simply cannot be done. The same assumption can ultimately harm efficiency and productivity as well. Provisioning, access auditing, and lifecycle management may seem like massive time expenditures, but when no other option is apparent, what is an organization to do?

With Okta's suite of FedRAMP-authorized and CAC/PIV-enabled tools, agencies can realize a higher degree of speed, ease, and efficiency no matter which solutions they employ, where they're housed, or who created them. This assists government agencies with their current host of cloud-based and on-premises solutions, then helps further as agencies continue to migrate from legacy systems to modernized cloud-based tools.

Putting it all together, Okta offers government agencies at the state, federal, and local levels an easy, cost-effective way to meet today's demands and make the best choices for tomorrow. If identity, access management, or related security concerns are preventing your agency from modernizing its IT infrastructure, reach out to Okta.

Okta solutions are FedRAMP-authorized and CAC/PIV-enabled.

Visit the Okta for Government page for more information on our best-in-class identity and access management tools.