Whitepaper

Deploying Modern Identity for National Security

Accelerate missions with modern, Zero Trust Identity

okta

Identity is an investment in military readiness

For the Department of Defense (DoD), and the federal government in general, two initiatives are especially critical at this moment: the modernization of infrastructure and service delivery, and enterprise resilience against increasingly severe and complex cyber threats.

Modernization necessitates adopting new digital tools to enable the DoD and enhance its capabilities as it serves the nation and its citizens. Good security requires implementing robust solutions and skills by design. The result: a collective defense that can take the maximum advantage with and through cyber.

Modernization and cyber resiliency are deeply intertwined. The common thread that binds them is Identity, a pillar on which Okta builds its Identity-as-a-service (IDaaS) products to make technology safe for all users. We know it's necessary for the DoD to provide information security protections across its primary workforce, extended workforce of contractors, allies, veteran population, and beneficiaries. Recognizing the unique challenges the Department faces in doing so, we have designed a solution.

Okta for US Military is our new Identity platform designed specifically for the Department of Defense and approved mission partners. It includes tailor-made features and security operations that integrate with DoD infrastructure. This next-generation security architecture provides centralized, secure access to mission-relevant resources for approved users—anywhere, anytime.

Secure, critical infrastructure

DoD Zero Trust pillars

1. User
2. Device
3. Application & Workload
4. Data
5. Network & Environment
6. Automation & Orchestration
7. Visibility & Analytics

Identity is the first pillar of the Cybersecurity and Infrastructure Security Agency (CISA)'s Zero Trust Maturity Model, which was developed to answer a requirement of the Executive Order on Improving the Nation's Cybersecurity. Within the Department, it is also a key driver behind the DoD Zero Trust Reference Architecture and the Identity, Credential, and Access Management (ICAM) Strategy. Additionally, the DoD Zero Trust Strategy includes users—the unique individuals requesting access to and privileges within systems—among its seven pillars and their enablers to ensure standardization of execution.

This increasing focus on Identity reflects the continuous evolution of not only the DoD, but the potential threats it must contend with:

- Cyber crime has become part of the military vernacular, with sophisticated attacks on government systems being deployed by both individual bad actors and adversarial nation states.
- Government Identity platforms are targeted because they offer a way into apps and the sensitive data they hold.

In short, Identity data is a strategic asset, and secure Identity platforms are critical infrastructure. Given the wealth of highly sensitive information that the DoD holds, any changes to the confidentiality, integrity, and availability of this infrastructure could have serious implications for national security.

Executive Order on Improving the Nation's Cybersecurity

Department of Defense Zero Trust Reference Architecture

Department of Defense Identity, Credential, and Access Management Strategy

Cybersecurity and Infrastructure Security Agency Zero Trust Maturity Model

Department of Defense Zero Trust Strategy

Secure, critical infrastructure

Identity is also critical to achieving the vision of the Joint All-Domain Command and Control (JADC2) in joint warfighting with international mission partners. Identity federation between organizations and mission partners can be the difference between success and failure. So, to continue to drive mission excellence in a landscape where cyber security is a moving target—and Identity infrastructure is becoming increasingly essential—it's imperative to embrace a culture of Zero Trust underpinned by increased collaboration and proper resourcing.

It's clear from ongoing efforts, agendas, and policies that the DoD is already engaged in vital cyber security initiatives. For example:

- Moving to the cloud
- Consolidating information technology (IT) infrastructure
- Addressing technical debt
- Implementing modern, secure Identity and access policies
- Acting urgently to maintain a competitive advantage against sophisticated threat actors

The next step is to build out capabilities and partnerships that advance these initiatives. One opportunity in particular is a cloud-native, vendor-neutral Identity ecosystem that aligns the DoD with the latest industry and military best practices.

Joint All-Domain Command and Control

Improved user experiences

Identity has a role to play beyond security. Used strategically and with a human-centered design approach, it can enhance the experiences of stakeholders that interact with the DoD. In fact, Identity has been deemed a common standard in delivering improved citizen experiences, as reflected in the Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government. The DoD Strategic Management Plan also prioritizes digital transformation by supporting the future force with the right technology investments—ones that maximize IT efficiencies, reduce IT costs, and help the Department leverage data strategically to improve the capabilities of its Total Force.

Today's technology users constantly engage with digital services from major consumer companies like Amazon, Netflix, and Uber. They're accustomed to streamlined Identity-based features that allow them to accomplish tasks securely and efficiently:

- Single Sign-On (SSO) enabling navigation through application ecosystems using a single Identity
- Quick, intuitive authentication based on secure factors such as device, location, and biometric data
- Centralized, role-based access to all the resources they need

These features are secure by design, with automated security controls built into IT infrastructure and management practices as part of a continuous risk management lifecycle. Security by design mitigates risks by minimizing the credentials and access points that bad actors target.

> With Identity, ease of use and security are two sides of the same coin.

As such, Identity can address implementation challenges with the DoD Common Access Card (CAC). The CAC grants physical and digital access to cardholders based on user permissions, but only provides a common authenticator, not the federation of Identities, and doesn't cover the use case of non-cardholders or scenarios when the CAC is temporarily unavailable but a service member still needs to work on vital mission applications.

Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government

Department of Defense Strategic Management Plan

Improved user experiences

Recruits

The DoD Strategic Management Plan reflects the Department's priority of recruiting, training, and retaining its Total Force as part of the President's Management Agenda (PMA) of making every federal job a good job. With Identity data, the DoD can be more effective in its recruitment efforts in several ways:

- Building joint influencer campaigns to reach new recruits
- Improving the overall experience for recruits with one-click access to information, resources, and support
- Providing a seamless transition of recruits' Identities when evolving from active duty to veteran status

Total Force

To make the Total Force as effective as possible, risk-based access to approved resources and protected services should have these attributes:

- Seamless
- Secure
- Auditable
- Available at any time, from anywhere

With a clear understanding of Identity-based threats and vulnerabilities, drawn from the continuous monitoring capabilities of an integrated Identity platform, the DoD can better mitigate risk and restore competitive advantage to its warfighters.

President's Management Agenda

Improved user experiences

Beneficiaries and contractors

For military spouses, dependent children of active-duty military personnel, and veterans, unclassified DoD networks and applications are their connections to vital services:

- Healthcare
- Education
- Human resources (HR)

Without CACs, these populations experience significant barriers. They must either rely on their cardholding relatives or create and manage multiple user Identities for various independent systems.

Similarly, international mission partners and contractors without CAC sponsorship fall outside the scope of the CAC program, yet their work may require timely access to potentially sensitive information. Information-sharing workarounds to bypass permissions issues pose great risk. So does the potential for human error when provisioning and deprovisioning temporary user Identities: inactive accounts are prime targets of bad actors.

With an enterprise-wide Identity solution, the Department could fill the gaps that the CAC doesn't cover:

- Enable role-based and time-based access to all DoD systems, networks, and applications
- Allow granular control of permissions from a central pane
- Provide a consolidated view of all user activity
- Prevent the need for shadow IT and information-sharing workarounds due to legacy Identity systems

Improved user experiences

GOTS definition

The term government-off-the shelf (GOTS) describes software developed exclusively for government use. It can be compared to commercial-off-the shelf (COTS) software, which is licensed commercially, but may also be sold to the government.

Okta supports the CAC today, and it can also support non-cardholders and federate Identities as needed. Our solution solves and scales unclassified or internet-connected Identity use cases for the DoD to enable streamlined, secure authentication, and improved user experiences. Although there's still a long way to go to support Secure Internet Protocol Router Network (SIRPNet), Joint Worldwide Intelligence Communications System (JWICS), and air-gapped enclaves with SaaS, that is primarily due to cloud feature parity for those environments.

While solution parity may be desired across networks, avoiding government-off-the-shelf (GOTS) Identity software for unclassified networks brings tremendous value. Leveraging commercial services decreases government burdens that limit the agility and responsiveness of the Total Force when accomplishing critical work. A poor user experience can also disrupt or impact mission success through increased friction and unnecessary additional strain on IT staff caused by support requests. Lastly, GOTS software prevents DoD from leveraging pre-built integrations such as the Okta Integration Network (OIN) that seamlessly integrates with leading Zero Trust vendors such as Palo Alto, Splunk, Zscaler, Crowdstrike, ServiceNow, Salesforce, GovSlack, O365, and more.

Improved user experiences

A tailored solution for the DoD

It is uniquely challenging to provide advanced and secure Identity capabilities to both the workforce and the public—so how can the DoD achieve the Enterprise Identity, Credential, and Access Management (ICAM) Reference Design?

> "A secure, trusted environment where people and non-person entities can securely access all authorized resources based on mission need, and where we know who and what is on our networks at any time."
>
> DoD Enterprise Identity, Credential, and Access Management Reference Design

Okta for US Military can help. The platform includes workforce and customer Identity solutions that achieve Zero Trust requirements and modern ICAM adoption. It can integrate with existing cloud and legacy infrastructure to support enterprise-wide Identity management, security, and modernization at scale.

Department of Defense Enterprise Identity, Credential, and Access Management Reference Design

Improved user experiences

For the workforce

The DoD's globally rotating employee base complicates managing access credentials, policies, and permissions. As users rotate between duty stations, they may spend weeks getting assigned to new applications, often leaving orphaned accounts behind once they move on. Within Okta's Workforce Identity Cloud, application rules, user groups, and Okta Lifecycle Management can mitigate these kinds of discrepancies.

Okta can streamline access control decisions by providing a centralized source of truth, enabling the DoD to perform workforce HR management, contractor management, mission partner collaboration, and security approvals.

Beyond the workforce

Okta for US Military is designed as an Identity solution for enterprise and component-level objectives. For instance:

- Okta provides a toolkit for creating infrastructure that meets the demands of the global scale of the Department, balancing the diverse needs of both centralization and management delegation.
- Okta can address CAC-holding users and those without a CAC, as well as user situations where the CAC is temporarily unavailable or not the best 2FA form factor, such as mobile or development environments and biometric identification scenarios.
- Okta has a history of supporting the largest, most complex organizations—ones that need enterprise visibility and shared services delivered at scale—and the Federal Solutions Architect team applies lessons from this work directly to supporting the DoD.

The call for a modern approach to security

Flexible, secure infrastructure

The DoD Digital Modernization Strategy articulates an enterprise view of the future where more common foundational technology is delivered across the DoD components. In other words, the DoD should be as equipped as any other organization—public or private—to leverage foundational technologies and deliver technology solutions to its stakeholders.

However, as the DoD increasingly engages in information sharing with external partners as part of joint cyber operations, its attack surface expands. This is also true of any partnerships with private sector organizations, such as technology vendors. There are pressing needs:

- Increase visibility into network traffic
- Strengthen access controls across the Department
- Ensure that there is no unauthorized access to sensitive resources

---

Department of Defense Digital Modernization Strategy

The call for a modern approach to security

End-to-end Identity, credential, and access management

While ICAM capabilities have been deployed on the individual system level within the DoD, they don't inherently serve the risk profile of the Department as a whole. In addition, inconsistencies between systems bring friction to access experiences, causing user Identity and password management frustrations that invite human error, increasing the potential threat landscape. The strategic digital modernization objective of shifting from component-centric to enterprise-wide operations and defense requires architectural transformation and an end-to-end ICAM infrastructure—one that monitors user activity and facilitates collaboration.

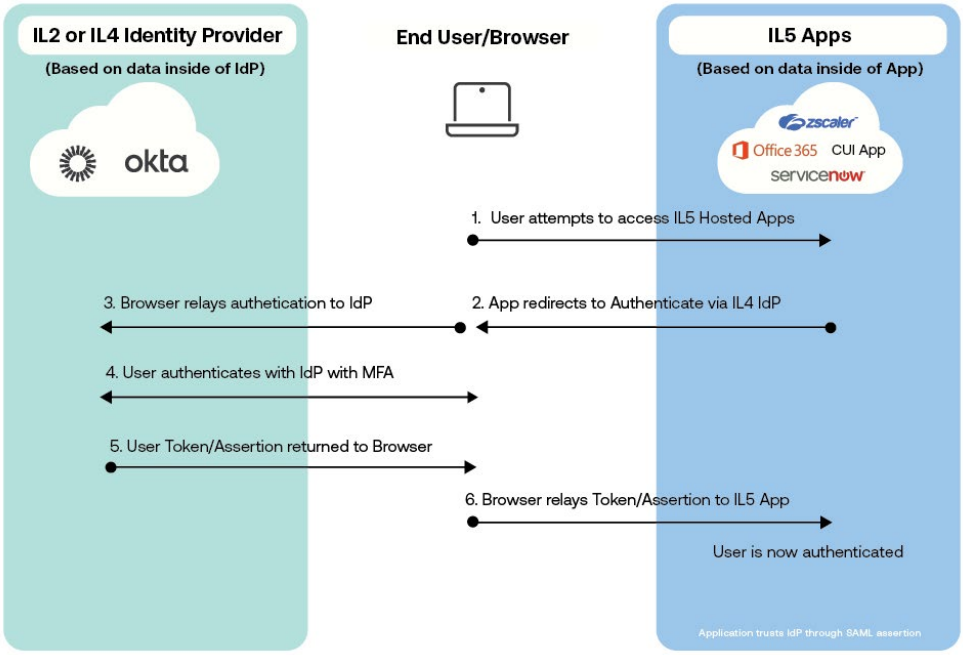
To align with the mindset "Cyber First, Cyber Always," this ICAM infrastructure must be secure by design. At the core of Okta's Identity solutions is the principle of Zero Trust, which itself relies on the premise of never trusting and always verifying. In other words, Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location, or based on asset ownership. It also relies on continuous authentication: ensuring that each user is authenticated often in order to verify that they are still the right user with the right level of access to the right resources.

The call for a modern approach to security

Additional layers of security

Okta has invested in providing higher levels of assurance within the public sector. More specifically, Okta for US Military achieved an Impact Level 4 (IL4) conditional Provisional Authorization (PA) to ensure we are abiding by DoD's additional security and compliance requirements. This means the solution has the following security features:

- Is hosted on a secure .mil web domain and network traffic is Defense Information Systems Agency (DISA)-approved
- Meets DoD security requirements for system registration and risk management
- Is built on the AWS GovCloud
- Peers with the internet and NIPRNet from a Boundary Cloud Access Point (BCAP) connection
- Includes an eMASS package that allows for inheritance



Okta for US Military is easy to deploy and manage, and it's ready to integrate into modern DoD apps with IL4 and IL5 authorizations (such as AWS, Box, Crowdstrike, O365, Salesforce, ServiceNow, VMware, Zoom, and Zscaler).

.mil
A .mil domain is a sponsored top-level domain for the United States Department of Defense and its subsidiary or affiliated organizations.

Streamlined user Identity and access management

Common Access Card internal users

1.3M

active duty personnel

780K

civilian personnel

800K

National Guard and Reserve forces

The DoD has one of the largest IT systems in the world, which includes public and private networks, applications, and security capabilities. Unifying it under a consolidated strategy means integrating approximately 10,000 operational systems. As part of this work, the Department intends to leverage SaaS to reduce IT infrastructure, cyber security operations, and maintenance costs. Okta for US Military is ready to integrate with over 7,000 commercially available applications and is designed to facilitate integration into cloud and on-prem applications.

Taking this consolidated approach also means managing Identity and access for the DoD's 1.3 million active duty military personnel, 780,000 civilian personnel, and 800,000 National Guard and Reserve forces. That's about 3.8 million internal CAC users in addition to the contractor workforce. Okta for US Military is well equipped to support and consolidate high volumes of users across disparate systems, providing risk-based Identity and access experiences that are appropriate to the varied interactions, credentialing, and environments across the DoD subscriber base.

Department of Defense Strategic Management Plan

Streamlined user Identity and access management

The Department also has other access needs that must be incorporated. Across the US, nearly 24 million people are involved in military, public, and national service at the local, state, and federal levels but fall outside of the CAC program and cannot access the services they need. This includes:

- US citizens in the recruiting pipeline
- An estimated 710,000 spouses of active-duty military personnel
- The dependent children of active-duty military personnel
- 19 million military veterans
- International mission partners
- Maintenance and warehouse workers
- Operational Technology/Facilities Related Controls Systems workforce
- Personnel working in non-appropriated funds positions, such as retail, food service, and hospitality workers

These populations have cumbersome experiences whenever they attempt to access DoD services. While the Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government does not call out these specific populations, it requires government organizations to repair gaps in access to government services. The order recognizes that everyone should be able to reach the services they need—and Okta for US Military is designed to help fulfill that mandate.

Public service and the federal government

Lifecycle Management

Another Okta Workforce Identity Cloud solution that supports the federal mandate and the DoD's modernization goals is Lifecycle Management, which delivers automated account provisioning (AAP) capabilities. Designed to automate the control of user Identity from creation to deletion, Lifecycle Management ensures that all users are immediately provisioned to the applications and resources they require as soon as they begin or transition into a new role. That access is then revoked as soon as they transition out of that role, eliminating the security vulnerabilities that can result from improperly deprovisioned accounts.

Active military

When an enlisted member is promoted or transferred to a new base, their digital Identity can be automatically updated so that they have the right level of access to the right systems when they need them.

Veterans

Today, when a veteran leaves active service, the user Identity that followed them through their military career becomes fragmented. Okta can eliminate this Identity fragmentation, facilitating risk-based authentication across the user lifecycle beginning at recruitment, throughout active service, into a supported transition to civilian work, and after retirement.

Okta Lifecycle Management addresses the goal state for the ICAM lifecycle recorded in the DoD's ICAM strategy: "the binding of a credential to a specific individual in an auditable and consistent way. The lifecycle process then continues by providing a mechanism for systems to authenticate users using managed credentials."

Zero Trust and beyond

The Department is evolving its approach to cyber security to support its Cyber Strategy, Digital Modernization Strategy, and the federal Executive Order on Improving the Nation's Cybersecurity. As described in the DoD Zero Trust Strategy, a common thread that runs through these initiatives is Zero Trust, the gold standard model for modern, cloud-based security.

A defining feature of Zero Trust paradigms is the priority of securing access and permissions at the level of individual users, rather than physical locations or specific networks. And beyond security, Zero Trust principles lean toward consolidated architecture and automated security controls that reduce the administrative burden on IT.

> "Implementing Zero Trust requires rethinking how we utilize existing infrastructure to implement security by design in a simpler and more efficient way."
>
> DoD Zero Trust Strategy

Users, assets, and resources—rather than physical boundaries and firewalls—have become the security perimeter, and any investments in security must account for Identity.

Okta for US Military is built on Zero Trust principles. This means that it can enable the Department to develop and implement its Zero Trust strategy for multi-cloud and hybrid-cloud environments.

Zero Trust and beyond

CMMC 2.0

The Cybersecurity Maturity Model Certification (CMMC) 2.0 program evolves the DoD's original effort to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) that is shared with contractors and subcontractors of the Department through acquisition programs by ensuring they meet a baseline level of cyber security.

CMMC streamlines compliance and supports cooperation between the Department and industry partners by establishing three tiers of maturity and developing assessment and maintenance protocols for each.

Empowerment

Okta's cloud-based Identity solution can be accessed seamlessly from anywhere, so DoD mission owners can confidently perform secure, audited Identity and access management to support their evolving digital policy rules governing access to on-premises, web-based, and modern cloud-native apps. Identity enables a more agile, more mobile, cloud-supported workforce—all conducive to optimizing the Total Force.

Talent

Investments to improve the workforce user experience will contribute to recruiting and retaining talent—particularly in hard-to-fill cyber security roles, which pose additional risk to the DoD's security efforts if left open. By adopting Okta's leading technology, and the streamlined experience that it enables, the DoD can make itself more attractive to top talent. Since the technology is easy to use, it isn't burdensome on less-technical workers entering the Department.

Compliance

Okta maintains alignment with ongoing security standards laid out by the DoD and the National Institute of Standards and Technology (NIST), such as the maturity requirements of the Cybersecurity Maturity Model Certification (CMMC) and controls specified in the NIST Special Publication 800-53. A number of Okta customers have been contracted by the Department, and Okta has supported them to reach and maintain the necessary maturity level to qualify for contracts.

NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations

Building on a strong foundation

The DoD has already made significant technology investments to get to where it is today, and as a trusted partner, Okta can further the Department's progress on delivering excellent, equitable, and secure DoD services and customer experiences.

Okta for US Military has the flexibility to support the DoD's unique business and mission needs with a vendor-neutral approach that not only complements existing solutions, but will also enhance the DoD's position as it solidifies its approach to modern security.

About Okta

Okta is the leading independent Identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 16,400 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, and Teach for America, trust Okta to help protect the Identities of their workforces and customers. To learn more visit okta.com.

Whitepaper

Deploying Modern Identity for National Security

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871