okta

Identity is the Core of Federal Zero Trust Environments

Look to Okta to help your agency comply with the Executive Order on Cybersecurity.

President Biden's **Executive Order on Cybersecurity** (EO) is a solid step toward creating a resilient cyber infrastructure for our nation. Yet implementing the EO requirements within the given timelines may be challenging for some agencies, especially if they haven't effectively addressed identity management. Adding to the challenge, agencies must also secure a blend of applications across a hybrid infrastructure. Okta, the market leader in identity and access management, gives agencies the edge in meeting the EO mandates. With Okta, agencies can accelerate the adoption of modern identity management or build out a scalable Zero Trust framework — without overhauling their architectures.

The perimeter has changed

Distributed workforces and evolving attack vectors have changed how we secure applications and data. The perimeter no longer exists in the way we've thought about it previously. The new attack surfaces are more personal and direct.

Okta can help agencies meet cybersecurity EO mandates with:

- Zero Trust architecture that aligns to FedRAMP, NIST, and other standards
- Vendor neutral approach that enables MFA and identity management across endpoints, workflows, and supply chains
- Ability to leverage legacy authentication, like PIV/CAC or a FIPS-validated alternative
- Adaptive MFA to create flexible policies
- A unified single platform that simplifies identity management
- Full compliance and audit reporting

Accordingly, identity has become the most crucial aspect of a Zero Trust (ZT) architecture. A ZT architecture that incorporates identity-based access management ensures strong authentication, visibility, and control across devices, apps, and services—regardless of their location.

Identity-first cybersecurity that scales

Okta can help agencies integrate a modern, vendor-agnostic ZT identity management foundation that easily integrates across the agency ecosystem—in the cloud or on-premises. This foundation helps agencies meet the EO requirements and consolidate identity management across infrastructures, platforms, applications, and devices while delivering scale and performance on demand.

Speed adoption of Multi-Factor Authentication and Zero Trust architectures

The EO mandates that agencies adopt multi-factor authentication (MFA) within 180 days after the EO was issued. It also mandates strong endpoint detection and response capabilities. Okta's vendor-neutral approach allows delivery of MFA across almost any application, platform, or environment quickly and easily. Additionally, Okta's platforms meet critical NIST, FedRAMP, and DoD security and access standards. Okta's Adaptive MFA lets you create contextual access policies that assess risk factors such as device, network, location, travel, IP, and more, at each step of the authentication process. Okta enables safe and secure connections between users and data, wherever it's stored, with dynamic security policies.

Deploy CAC/PIV - in-the-cloud capability, even in hybrid environments

The EO promotes the move to the cloud as part of an effective ZT architecture. Okta accelerates movement to secure cloud services with over 7,000 pre-built integrations that quickly and easily allow agencies to

> Okta is collaborating with the National Cybersecurity Center of Excellence (NCCoE) in the Zero Trust Cybersecurity: Implementing a Zero Trust Architecture Building Block Consortium to develop practical, interoperable cybersecurity approaches that address the real-world needs of complex Information Technology (IT) systems. NIST does not evaluate commercial products under this Consortium and does not endorse any product or service used. Additional information on this Consortium can be found at: https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture."

securely connect to all types of applications – on-premises or in the cloud. Additionally, agencies can leverage different authentication schemas, like CAC/PIV or a FIPS-validated alternative. Plus, Okta's Advanced Server Access can extend secure access management to all on-premises and cloud resources.

Improve detection of vulnerabilities and incidents, monitor and report with ease

Slow or inconsistent deployment of basic cybersecurity tools and practices exposes agencies to adversaries. With Okta, agencies can easily create and implement the best security practices, policies, and methodologies that automatically connect the right apps to the right users and revoke access based on triggers from HR systems and IT resources. Agencies can also create pre-authentication policies that are evaluated before the password to prevent account lockout and help to reduce password reliance. In addition, Okta enables agencies to monitor organization configurations continuously and receive tailored recommendations that improve security posture.

The Okta Identity Platform leverages machine learning to help agencies establish policies to evaluate context that identifies and blocks large-scale identity attacks, such as password spray and brute force, in real-time. This allows admins to block access attempts from these IPs. With powerful, automated security incident response workflows, 3rd-party apps can be triggered to create tickets and notify SecOps teams. Okta also offers compliance and audit reporting to enable agencies to collaborate with other agencies to identify and stop breaches.

Extend and enhance security for supply chains and endpoints

The EO emphasizes the need for a secure supply chain, and Okta delivers here as well. Built on the AWS GovCloud, Okta provides a single, unified platform that has security built-in from the start and delivers powerful downstream effects. With Okta, identity management is simplified, even in complex vendor environments.

Summary

For agencies who need to meet the Executive Order on Cybersecurity requirements, the Okta Identity Platform delivers the security, automation, scalability, and integrations necessary to implement an identity-centric Zero Trust foundation quickly and effectively, without a heavy lift. It's easy to configure, simple to deploy, and doesn't introduce friction to daily workflows.

Contact your Okta representative today to learn how your agency can quickly and cost-effectively meet the EO mandate requirements with Okta.

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. We provide simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. To learn more, visit **okta.com**.