Datasheet

July 2026

Identity security: The must-have checklist for government agency attack readiness

14 questions to help protect your agency from identity-based cyber attacks.

Nation-state actors and cybercriminals targeting government agencies do not care about your legacy firewalls; they are hunting for credentials to breach critical infrastructure and public services. While agencies struggle with modernizing siloed systems and defending against automated fraud, attackers are actively exploiting session tokens, bypassing weak MFA via AiTM proxies, and weaponizing Non-Human Identities (NHIs) like dormant service accounts to pivot undetected across sensitive networks.

Use this checklist to audit your agency’s defense capabilities against the modern threat landscape and ensure you are meeting critical security mandates.

Please note that this checklist is intended only as a component of your agency's overall security and compliance program.

Datasheet

July 2026

PRE-ATTACK

Proactive identity governance

This section focuses on eliminating excess access and reducing the identity attack surface within your authorized boundary, before an attack compromises mission-critical data.

1. Do you register AI agents as first-class identities in your directory, with a unique identity and an accountable human owner assigned at the point of onboarding?
2. Can you automatically enforce least privilege access controls and validate that there are no MFA bypasses threatening your compliance posture?
3. Do you have a structured process to identify stale or partially off-boarded contractor or employee accounts that still retain active access to government systems?
4. Do you run structured, recurring access certifications for both human personnel and AI agent identities operating inside your authorized environment?
5. Is there a system in place to certify, adjust, or revoke excessive permissions to minimize the potential blast radius of a compromised identity on public services?
6. Do you use an "identity lens" to get a holistic view of which personnel or contractors have access to what agency resources and how they authenticate, covering gaps left by traditional CSPM and SSPM tools?

Okta for AI agents

Continuously discover, register, and govern AI agent identities within a single secure control plane.

Datasheet

July 2026

DURING ATTACK

Continuous threat detection and response

This section covers the mission-critical capabilities needed to detect and respond to cyber threats in real-time as they happen.

1. Have you implemented phishing-resistant authentication (e.g., Okta FastPass) to protect agency workforce and public users against sophisticated phishing attacks?
2. Do you continuously monitor session activity and user behavior after initial authentication to detect anomalies, prevent fraud, and stop potential lateral movement across government networks?
3. Can you automate inline responses to contain cyber incidents, such as performing a universal logout across all agency apps and devices, enforcing step-up MFA, or triggering custom security workflows?
4. Do you have AI-driven bot protection that can detect and mitigate automated attacks—such as massive, automated benefits fraud—without requiring high-friction user input like traditional CAPTCHA?
5. Does your system continuously assess risk levels alongside user and device context to dynamically evaluate and enforce stringent public sector security policies throughout a session?

Identity Threat Protection

Automatically detect and respond to identity-based threats against government systems in real time.

Okta Device Access

Secure device login that hardens protection and simplifies access to agency resources.

Okta FastPass

Gain Zero Trust security with public-sector-ready, phishing-resistant, passwordless authentication.

Datasheet

July 2026

POST-ATTACK

Strengthen identity resilience

This section focuses on improving agency security posture and incident response capabilities after a breach attempt has occurred.

1. Do you have tools for incident observability and forensics that can uncover the complete identity attack path to satisfy rigorous government reporting requirements?
2. Is there a system to improve incident handling by using identity event correlation and shared threat intelligence across your agency's security tools?
3. Can you provide strict compliance assurance by mapping your identity controls directly to required government frameworks (e.g., NIST)?
4. Do you have a continuous feedback loop to analyze security events and fine-tune responses over time to maintain public trust?

Datasheet

July 2026

Okta makes it possible

Regardless of where your agency sits on the spectrum of attack readiness, Okta provides the end-to-end visibility and real-time response capabilities necessary to secure your critical infrastructure before, during, and after an incident.

With visibility into 10 billion global logins and 2 billion blocked threats monthly, Okta sees the TTPs (Tactics, Techniques, and Procedures) others miss, protecting the integrity of public services. By unifying signals across your entire agency ecosystem, Okta enables you to move from reactive defense to proactive resilience—eliminating misconfigurations, stopping phishing in its tracks, and automating inline responses to contain threats instantly.

Learn how to turn your agency's identity layer into your strongest security asset. Then take the next step by assessing your AI security architecture. Use our interactive AI Blueprint tool to map your agent environment, simulate real attack scenarios, and expose critical security gaps.

Okta for AI Agents

Core Helps Federal Agencies Who Need to Govern AI. For more information See Okta's Public Sector Support Page.

Read more here

About Okta

Okta, Inc. is The World's Identity Company™. We secure Identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of Identity to drive security, efficiencies, and success — all while protecting their users, employees, and partners. Learn why the world's leading brands trust Okta for authentication, authorization, and more at okta.com.