Whitepaper

Federal Zero Trust Strategy: OMB M-22-09 sets new goals

Okta helps you accelerate the top-priority Identity actions.

Shared baseline of Zero Trust maturity

Executive Order (EO 14028), *Improving the Nation's Cybersecurity*, demanded bold and swift action on cyber modernization, not just incremental improvements. It directed NIST, CISA, OMB, and others to develop clear guidance that enables agencies to adopt a Zero Trust architecture.

OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, is another important step. Since agencies are at different levels of Zero Trust maturity, the memorandum aims to "reduce uncertainty and outline a common path" by establishing clear goals for all to achieve by September 2024. It requires agencies to update their Zero Trust adoption plans and incorporate these goals.

OMB goals align with CISA

Fortunately, OMB's goals readily align with the CISA Zero Trust Maturity Model, also developed to support the Executive Order. The maturity model (pre-decisional draft) defines the five pillars of Zero Trust as Identity, device, network/environment, application workload, and data.

For each pillar, CISA outlines what it takes to move from the "traditional" or perimeter-based approach through "advanced" to "optimal" Zero Trust maturity.

Consider the first pillar, Identity.

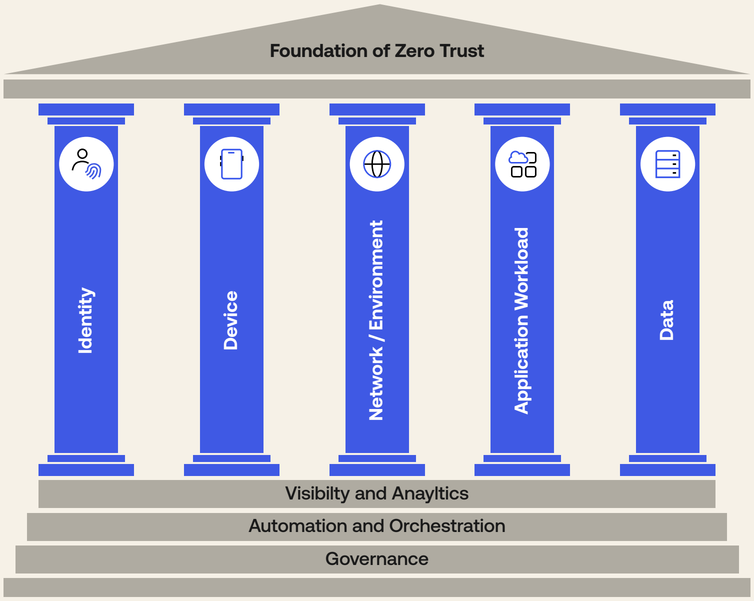

Figure 1: Foundation of Zero Trust

CISA explains that authentication must evolve from a mix of passwords and some multi-factor authentication (traditional) through agency-wide MFA (advanced) to continuous Identity verification (optimal). It provides similar advice for the other functions of Identity — Identity stores and risk assessment — as well as the three cross-pillar considerations (visibility and analytics; automation and orchestration; and governance).

Identity is the first strategic goal

CISA established Identity as the first pillar of Zero Trust for good reason: it's impossible to assess and enforce least-privilege access without it. NIST also explains that the first step in every Zero Trust transition is to "Identify actors on the enterprise."

Therefore it's not surprise that OMB M-22-09 addresses Identity first. The vision is: "Agency staff use enterprise-managed Identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks."

To accomplish this, M-22-09 requires every agency to:

1. Employ and integrate centralized Identity management with applications and platforms
2. Use strong, phishing-resistant MFA at the application layer
3. Consider at least one device-level signal alongside Identity information for resource access

Okta has Identity covered

At Okta, we're the clear leader in modern, cloud-based Identity and Access Management. Without covering everything we do, let's focus on your new M-22-09 related actions.

1. Employ and integrate centralized Identity management with applications and platforms

Okta Universal Directory delivers centralized Identity management, a single view of all your users, groups, and devices. Even if your agency has multiple Identity sources today, we provide that all-important single view and access policy decision point. We integrate with Active Directory and LDAP sources, and integrate with out-of-the-box connections with modern HR systems like Workday, SaaS apps like G Suite, and third-party Identity providers.

2. Use strong, phishing-resistant MFA at the application layer

Skim that quickly, and you conclude that if you've got MFA, then all's OK. But let's look closer.

First, the easy part: MFA at the application layer. They're drawing an important distinction between *application-layer* access and *network-layer* access. Recall that in Zero Trust, we must assume that attackers are already on our networks, so network layer access control doesn't cut it. Okta MFA provides adaptive, context-based Zero Trust access at the application layer with an added bonus: Less friction for users.

Next, the harder part: *Phishing-resistant* MFA. MFA methods are not created equal, and OMB is saying that agencies must stop supporting weaker MFA approaches like registering phone numbers for SMS or voice calls, one-time codes, and simple push notifications because they're susceptible to phishing attacks. But Okta MFA is different. We already support the phishing-resistant, government-recommended methods like PIV and WebAuthn. For example, WebAuthn combines second-factor push notifications with biometrics like FaceID to counter phishing attacks.

3. Consider at least one device-level signal alongside Identity information for resource access

End user devices are often stepping stones for cyberattackers. They exploit insecure configurations, unauthorized software, or vulnerabilities to plant malware. Sometimes they trick users through tactics like phishing to let them in. And once the device is compromised, attackers move laterally and breach your agency's critical resources.

Therefore, you must assess device risk before granting access. Device-level risk signals include detected malware, open vulnerabilities, non-compliant configurations, or unauthorized software. By combining device-level risk signals with Identity information, you can dramatically reduce threats by restricting access from compromised devices.

At Okta, we partner with EDR solutions like Crowdstrike to build external risk signals into our access policy decisions. For example, we'll decline an authentication request from a device that exceeds a certain risk score — effectively preventing that device from exposing your enterprise resources to new threats. It's part of our extensive Okta Integration Network that provides deep, pre-built integrations to securely connect everything.

Let us help you implement your Zero Trust plan

At Okta, we've been helping agencies modernize cybersecurity and adopt Zero Trust long before the Cyber Executive Order. And today we're working with the NIST Cybersecurity Center of Excellence (NCCoE) to develop its 1800-series practice guide to help implement Zero Trust. We're lending our time, talent, and technology to make the path easier for everyone.

Knowing the path and walking it are two different things, and the lack of funding often impedes progress. OMB M-22-09 reminds you that you're on your own for the next two years. So if you can't accomplish your Zero Trust goals with existing funding sources, let us help you write and submit a Zero Trust project proposal to the Technology Modernization Fund (TMF).

Implement your Zero Trust plan — talk to us today.

About Okta
Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.