ForgeRock

INDUSTRY BRIEF

Zero Trust IAM: What Federal Agencies Need to Know

These days, it's rare to read about a cybersecurity incident that doesn't link to user identity — ForgeRock's 2021 Consumer Identity Breach Report found that attacks involving usernames and passwords increased a staggering 450 percent over 2019, translating into more than one billion compromised records in the U.S. alone. Given that user identity remains a primary threat vector exploited by bad actors, it comes as no surprise that we see identity and access management (IAM) playing a leading role in national cybersecurity policy and guidance.

When the Biden Administration issued Executive Order (EO) 14028 on Improving the Nation's Cybersecurity in May 2021, it brought a reinvigorated focus to cybersecurity, setting into motion a series of actions by federal agencies, including the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the Department of Homeland Security's Cyber and Infrastructure Security Agency (CISA).

In January 2022 Office of Management and Budget (OMB) acting director Shalanda Young issued the finalized strategy that requires federal agencies to submit their plans within 60 days for how they will meet these cybersecurity standards by the end of fiscal year (FY) 2024. The OMB acknowledges that this will be a journey with "learning and adjustments along the way as agencies and policies adapt to new practices and technologies."

A significant recommendation in the EO is to advance toward a zero trust architecture. So, to facilitate your zero trust journey, we've broken down what you need to know about zero trust policy, and the key ways that IAM factors into such a strategy.

> "This will be a journey for the Federal Government, and there will be learning and adjustments along the way as agencies and policies adapt to new practices and technologies."
>
> **OMB Draft Zero Trust Strategy**

What is Zero Trust?

Before we dive into the federal guidance, let's explore the term zero trust. What is it? How does the zero trust model relate to identity, and how does zero trust IAM differ from what agency admins have been doing all along? Is it a true security architecture, or is it just another marketing scheme to rebrand identity? Simply put, zero trust is a security framework that removes implied trust. In the past, once an entity (end-user, workload, app, or device) was inside the secure network perimeter, that entity was assumed to be trusted. But in the era of digital transformation, the traditional network perimeter has given way as apps and services have moved to the cloud and end-users are increasingly working off the network or connecting through VPNs using unmanaged devices.

First defined by Forrester Research, the zero trust framework removes that implicit trust and focuses instead on evaluating each connection or activity in near-real time based on access policies. It uses an "adaptive" approach to trust, meaning that access permissions are continually reassessed as any context (device, geo-location, etc.) changes.

NIST defines zero trust as, "moving defenses from static, network-based perimeters to focus on users, assets, and resources." This shift from network security to a more dynamic approach effectively makes identity the new network perimeter.

The buzz around zero trust might make it seem like an entirely new IT security concept; however, as noted in NIST Special Publication 800-207, "Federal agencies have been urged to move to security based on zero trust principles for more than a decade, building capabilities and policies such as the Federal Information Security Modernization Act (FISMA) followed by the Risk Management Framework (RMF); Federal Identity, Credential, and Access Management (FICAM); Trusted Internet Connections (TIC); and Continuous Diagnostics and Mitigation (CDM) programs."

Moreover, much of what the draft federal guidance covers emphasizes existing NIST guidance, in particular Special Publication 800-63-3, Digital Identity Guidelines.

Federal Guidance on the Identity Pillar

EO 14028 mandates agency adoption of both multifactor authentication (MFA) and the implementation of a zero trust architecture with more detailed requirements contained in the Federal Zero Trust Strategy and Zero Trust Maturity Model released in draft for public comment on September 7, 2021, by OMB and CISA, respectively. Given that identity & access management (IAM) plays a foundational role in zero trust implementation, it appears prominently in this draft guidance as one of five "pillars." OMB's draft Federal zero trust strategy sets the fiscal year (FY) 2024 identity goal as follows: "Agency staff use an enterprise-wide identity to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks." The strategy outlines agency requirements in the following three areas: 1) enterprise-wide identity, 2) multifactor authentication, and 3) strong password policies.

Enterprise-Wide Identity

Agencies put themselves in a vulnerable position when weak or inconsistent access controls are in place, particularly with the increase in remote work and the use of multiple endpoints, and the problem is exacerbated by the use of too many identity systems. The draft guidance notes that the "simplest way for a Federal agency to address these challenges is to support a single, well-designed authentication system, and to integrate it with as many applications as possible."

By FY 2024, agency security teams must employ an identity provider or IAM solution and enterprise-wide single sign-on (SSO) service for agency users that can be integrated into applications and common platforms, including SaaS platforms, and begin decommissioning other identity systems. The guidance directs agencies to leverage open standards such as SAML or OpenID Connect with an eye toward API integration in cloud and hybrid environments — those that host apps in both cloud environments and on-premises. This is no small task for large organizations with multiple agency segments that may be using many different IAM solutions across their ecosystems—to the extent that an agency segment that can justify the continued need for a separate identity system federation must be supported.

Multifactor Authentication (MFA)

Federal guidance reflects an administration that is fully "signed-on" to MFA — and not just any MFA will do. It needs to be phishing resistant, or what the NIST Digital Identity Guidelines call "verifier impersonation resistant." NIST sent this signal over four years ago in SP 800-63B by requiring phishing-resistant authenticators at Authentication Assurance Level 3 (AAL3) and, generally, by designating authenticators leveraging the public switched telephone network, including phone and SMS-based one-time passcodes (OTP) as restricted.

Agencies must bolster their baseline defenses to match the increased sophistication of hackers, as MFA that leverages OTP will become insufficient to guard against increasingly sophisticated attacks. Accordingly, beyond the EO requirement for agencies to implement MFA to the maximum extent feasible by mid-November 2021, OMB's guidance takes secure access a step further, requiring agencies to enforce MFA at the application level using enterprise SSO. For enterprise users, phishing-resistant methods are required, and for external citizen-facing use cases, phishing-resistant MFA must be an option.

Agencies already have tools available to address phishing-resistant requirements through Personal Identity Verification (PIV) or derived PIV. However, six years post the Office of Personnel Management data breach and the push for mandatory PIV demonstrates that PIV cannot solve all use cases; fortunately, there are modern risk-based authentication approaches that can be leveraged to meet phishing-resistant requirements through WebAuthN and other authentication protocols that meet NIST requirements, including FIDO.

Strong Password Policies

There is a lot of buzz in the IAM industry encouraging organizations to go passwordless in part for a better user experience. While this is a path the government can also pursue, the draft federal guidance is focused on the adoption of secure password policies. This guidance puts more prominently into policy what NIST already recommends in its digital identity guidance (see 800-63B Appendix A- Strength of Memorize Secrets), including checking passwords against known-breached data. CISA is required to make one or more services that can accomplish this task available to agencies.

Zero Trust Maturity Model

While CISA's draft Zero Trust Maturity Model is not quite mature enough to meet the definition of Capability Maturity Model Integration (CMMI), a program used by many agencies to guide process improvement, it does offer a relative scale that includes "traditional, advanced, and optimal" categories with some basic descriptors for each level. CISA's draft model more closely resembles the tier concept (which is not considered a maturity model) from the NIST Cybersecurity and Privacy Frameworks, and is a good starting point; through interagency inputs, we'll be able to see more clearly defined criteria and examples of what a traditional, advanced, and optimal zero trust architecture should look like.

It's Time to Anchor Identity with Privacy

The EO is clear that the government must take steps to modernize cybersecurity while "protecting privacy and civil liberties." Digital authentication supports privacy protection by mitigating risks of unauthorized access to individuals' information. At the same time, because authentication and some of the more advanced behavioral authentication mechanisms involve the processing of individuals' information, they can also create privacy risks.

While the OMB zero trust security model doesn't explicitly call out specific privacy requirements, it is important for agencies to implement zero trust plans that are anchored in privacy. For example, as agencies begin implementing more behavioral authentication techniques, they should consult with their privacy counterparts to conduct a privacy risk assessment and implement mitigations (e.g., informing users, obtaining consent, educating enterprise users, etc.). Note that privacy requirements are already embedded into the NIST Digital Identity guidelines and remain relevant in zero trust implementations. Other useful tools available to assess and mitigate privacy risks can be found in the NIST Privacy Framework and NIST Internal Report 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems and an accompanying privacy risk assessment methodology.

> "Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."
>
> **OMB Draft Zero Trust Strategy**

What's Next in Zero Trust?

EO 14028 required agencies to develop zero trust implementation plans; upon release of the final Federal Zero Trust Strategy, agencies will need to, within 30 days, designate and identify a zero trust architecture implementation lead and, within 60 days, update their individual plans by incorporating requirements in the strategy and and submitting an implementation plan for FY 22-24 along with a budget estimate for FY 23-24. Agencies are to re-prioritize funding in FY 22 to achieve zero trust goals or seek funding from alternate sources, such as the Technology Modernization Fund.

Federal agencies have a lot to accomplish by FY 24, and achieving an "optimal" zero trust architecture is not something that can be achieved overnight. Agencies will need people, process, and technology to carry out the actions identified in federal guidance. As agencies look to consolidate disparate identity systems, they should also keep an eye on interagency interoperability since it is highly likely that different agencies will select different solutions. Agencies can leverage reference architectures as they build their own, including the Department of Defense Zero Trust Reference Architecture and CISA's Cloud Security Technical Reference Architecture. In addition, the NIST Cybersecurity Center of Excellence has an "Implementing Zero Trust Architecture" initiative with industry leaders to apply concepts in SP 800-207. Taken together, these reference architectures and NIST guidance should help improve the likelihood of successful implementation.