Ping Identity

The Path to Zero Trust Starts with Identity

EXECUTIVE BRIEF

Large-scale cyberattacks have rocked both the public and private sector in recent years, causing everything from data loss to a fuel shortage along the Eastern seaboard – and they aren't letting up. No industry is immune to the hackers' relentless quest to disrupt business operations that keep daily life in America moving forward – and safe. With our critical infrastructure — including healthcare, energy, and education systems — and government agencies in hackers' crosshairs, cybersecurity has been elevated to a national security issue.

To better protect critical operations against attacks, President Biden issued the Executive Order (EO) on Improving the Nation's Cybersecurity[1] , which outlines actions that Federal agencies must take to fortify our nation's digital infrastructure. A central element of the EO is a mandate to adopt a Zero Trust architecture.

Traditional cybersecurity is based on a strong perimeter. Once users get past the perimeter, they are free – or trusted – to move about the network. In contrast, Zero Trust views everyone inside and outside of the network as potentially hostile. With a Zero Trust architecture, identity is at the center of security. Identities are constantly verified to ensure users are who they say they are and have the necessary credentials to access network resources at various access points.

Agencies must reexamine and up-level identity, credential, and access management (ICAM) capabilities to move forward with a Zero Trust architecture and achieve the mandates in the EO. The General Services Administration and Federal CIO Council define ICAM as "the set of tools, policies, and systems that an agency uses to enable the right individual to access the right resources, at the right time, for the right reason."[2] The Federal ICAM (FICAM) program offers guidance on identity standards, architectures, and implementations to help Federal agencies build ICAM into their environments. The goal of FICAM is to enable the work of government employees and contractors while ensuring that access to applications and assets on government networks is secured and authorized.[3]

OVERCOMING IDENTITY CHALLENGES WITH ICAM

Federal agencies have worked for a long time to enhance, standardize, and secure the identities of their employees and contractors who access Federal networks. While they have made many ICAM improvements, agency environments are rife with legacy identity technologies, which lead to common identity challenges. These challenges can make it difficult to implement Zero Trust. Below, we review these challenges and ways to overcome them by modernizing existing identity infrastructure.

COMMON IDENTITY CHALLENGES INCLUDE:

Legacy identity management tools are not equipped for a distributed workforce.

Today's Federal workforce, mission partners, and contractors are spread between agency headquarters offices, satellite locations, and remote offices, and all need secure access to resources located in both on-premises data centers and cloud environments.

Incompatible identity systems across agencies hinder interoperability.

Agency systems to prove identity are frequently incompatible with each other. As a result, interagency teams can't always access the systems or relevant data needed to collaborate with their colleagues.

Fragmented identity landscapes complicate resource access.

Historical identity authentication protocols have led to siloed identity environments, and disparate authentication systems have made it challenging for many agencies to offer dependable access to resources.

Legacy identity infrastructure components don't support modern technology needs.

Legacy ICAM tools aren't designed to handle cross-domain, hybrid environments that cover on-premises data centers, public and private clouds, and virtualized environments. This legacy technology also lacks security features that can withstand sophisticated cyberattacks.

While these challenges may seem daunting, it is possible to address them quickly and cost effectively. Federal agencies facing identity challenges can up-level their ICAM infrastructures to align with FICAM guidance and achieve the mandates outlined in the EO. This can be accomplished with modern, standards-based identity components that integrate into existing architectures.

MODERNIZING FEDERAL ICAM WITH PING IDENTITY

Ping Identity helps agencies modernize their ICAM infrastructure by breaking down the silos that exist in fragmented identity environments and building upon the existing capabilities supported by legacy identity and access management (IAM) technology.

With standards-based identity solutions that plug into existing architectures, agencies don't have to start from scratch to establish a strong ICAM foundation and achieve Zero Trust. Ping's solutions for government can be used across the enterprise or can plug into only those areas of the infrastructure that need to be improved.

Ping's solutions for government directly support the following ICAM components:

Federation

Ping's federation server easily integrates with any application across an agency, third-party authentication sources, diverse user directories, and existing identity access management systems. Its support for X.509 adapters expands the reach of existing identity management tools — including PKI, PIV, and CAC authenticators.

By integrating silos of identities and applications inside the agency, across partners, and in the cloud, Ping's federation server enables:

- Agency-wide single sign-on (SSO) between any user and resource
- The extension of existing authenticators to apply multi-factor authentication (MFA) to any resource
- Identity federation for improved interoperability

Identity management

Ping's identity management component modernizes legacy identity infrastructure by providing a fast, scalable directory that stores identity and rich profile data that can be used by SaaS, cloud, and on-premises applications. It secures credentials, application data, and profiles in a flexible directory that technology teams control. The directory can encrypt data at rest, in motion, and in use to avoid costly data breaches and help ensure regulatory compliance.

Ping's identity management component scales to hundreds of millions of profiles with billions of attributes without losing access to critical resources. It allows agencies to:

- Expose unified profiles to all channels and devices
- Centralize user attributes across all data stores – whether in the cloud or on-premises
- Manage all identities within their environment, including employee and partner identities

Access management

Ping's access management component is a centralized access security solution with a comprehensive policy engine. It employs risk-aware authorization and centralized session management for both internal and external users, providing secure access to applications and APIs down to the URL level.

It also continuously validates authentication tokens from Ping's federation component in predetermined time intervals, so if there's a change in user context — or if a single logout process terminates a user's authentication session — all application sessions will immediately be terminated.

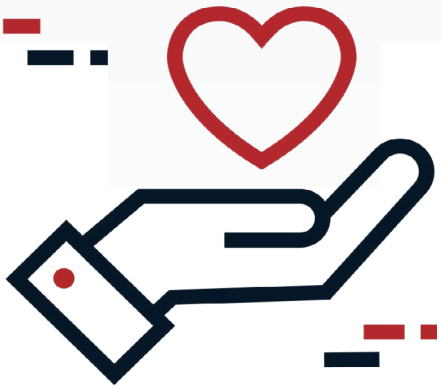
Ping's access management component allows agencies to:

- Centrally manage sessions and access policies for any application
- Continuously enforce authorized user access to the right resources
- Audit all access correlated by identity and context

REALIZING ZERO TRUST WITH PING IDENTITY

As a result of the EO mandate to implement Zero Trust, agencies need to review their Federal ICAM architectures quickly and take action to up-level their capabilities. To support this effort, agencies should look to modern, standards-based identity solutions that enable them to strategically and efficiently enhance existing capabilities in order to advance their Zero Trust journeys.

Ping's solutions for government not only helps agencies accomplish this, but also allow agencies to do so while avoiding significant IT operational costs. Ping's solutions can be deployed as DOD IL5 certified, FedRAMP High in-process SaaS, or in hybrid, DDIL, air-gapped, or on-premises environments so agencies can be assured that their sensitive data and assets will be protected in compliance with Federal standards.



Learn more about Ping's solutions for government and how it supports the path to Zero Trust.

1 Executive Order on Improving the Nation's Cybersecurity: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
2 Federal ICAM Architecture Introduction, FICAM Playbooks: https://playbooks.idmanagement.gov/arch/
3 Identity, Credential, and Access Management: https://www.gsa.gov/policy-regulations/policy/informationintegrity-and-access/identity-credential-and-access-management

#3617 | 05.23 | V02