2022 FCW ICAM Workshop

FICAM and Zero Trust

Ken Myers
Director, Identity Assurance and Trusted Access Division
August 2022

Presenter

Ken Myers
Director
Identity Assurance and Trusted Access Division
Office of Government-wide Policy
kenneth.myers@gsa.gov

What We Do

We're here to help: *https://playbooks.idmanagement.gov/*

Guides
(various articles on a topic)

- FICAM Architecture
- ICAM Program Management
- Federal Public Key Infrastructure
- Personal Identity Verification
- Physical Access Control Systems

Playbooks
(procedural recommendations)

- Digital Identity Risk Assessment
- Identity Lifecycle Management
- Single Sign On
- Cloud Identity
- Privileged Identity (Coming Soon)

Does FICAM change with Zero Trust?

Zero Trust Digital Identity

5

OMB Memo 22-09

Moving the U.S. Government Toward Zero Trust

The goal of this strategy is to accelerate agencies toward a **shared baseline of early zero trust maturity**.

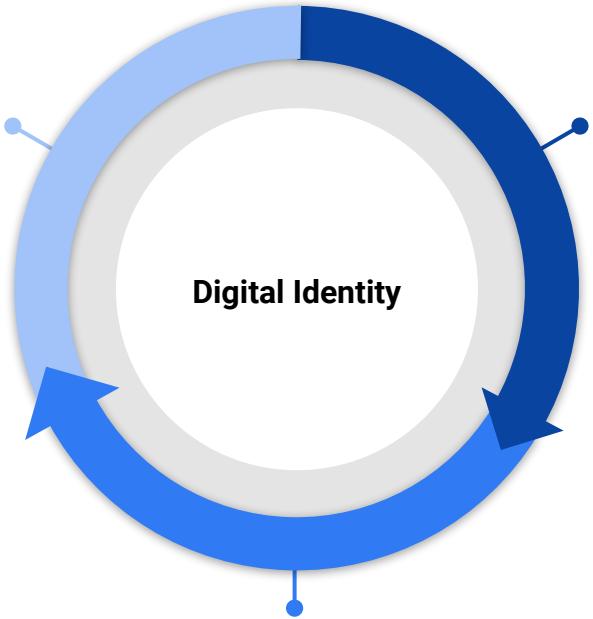
- Moving to a zero trust architecture will be a multi-year journey for agencies.
- The federal government will learn and adjust as new technologies and practices emerge.

This strategy places significant emphasis on **stronger enterprise identity** and **access controls**, including phishing-resistant multi-factor authentication (MFA).

Digital Identity Strategic Goals

Enterprise-wide Identity System

Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.



User Authorization

When authorizing users to access resources, agencies must consider at least one device-level signal alongside identity information about the authenticated user.

Multi-factor Authentication

Agencies must use strong MFA throughout their enterprise. Within one year, provide option for phishing-resistant authenticators for public users.

It’s Cloud or Nothing

Most agencies that utilize an IDaaS are operating in a hybrid configuration.

Baseline ICAM Capabilities

10

Achieve Zero Trust

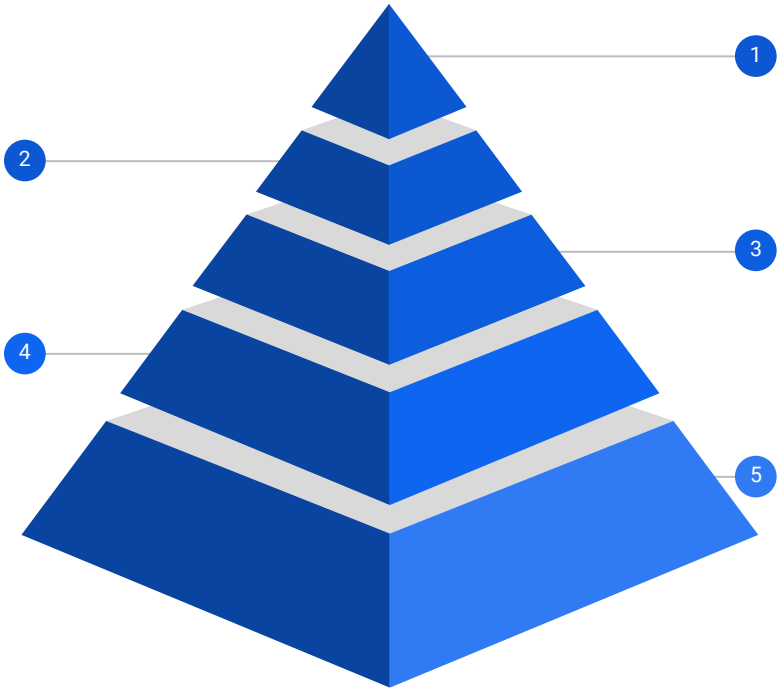
Align Zero Trust Priorities to ICAM Capabilities

Multiple MFA Options (Coming Soon)

Agencies should deploy multiple phishing-resistant MFA options when a PIV smart card is not available. FIDO2 is the optimal secondary option.

Fine-Grained Authorization (Cloud Identity Playbook

Most IDaaS support device-level signals or other risk attributes as part of an authorization decision.



Create a Master User Record (Lifecycle Playbook)

A master user record is a single identity which may link to multiple accounts, credentials, or personas. Includes both people and non-person entities. Supports fine-grained authorization models.

Use Single Sign-On (Single Sign-On Playbook)

Centralize access for your workforce and public users.

Manage Privilege Users (Coming Soon)

Privilege users include anyone that can impact a privileged account.