

Public sector mandate update: FICAM v2.0

Benefits

Our identity and access management software can help you comply with FICAM and enhance security and efficiency. For more information, visit: www.oneidentity.com.

About FICAM

The Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance document was first published in 2009, and the Office of Management and Budget's Memorandum 11-11 requires that agencies align their processes with the guidance document.

However, the first version of the guidance document does not specify a fully-defined set of regulations to follow. Instead, it defines an architectural framework comprising five key elements (credential management, identity management, access management, federation, and auditing & reporting), and offers 11 associated real-world scenarios. Guidance into how agencies should implement FICAM processes and services is largely missing.

What's new in v2.0

With Version 2.0, released in December 2011, the Roadmap and Implementation Guidance document has grown from 220 to 478 pages – and half of that content is specific advice on how to build agency level initiatives and deploy ICAM services. The new version includes the following details:

- **How to plan for ICAM implementations:** This includes program organization and management, with specific guidance on implementing a formal governance structure. Also discussed is how to incorporate ICAM into existing agency processes, along with privacy considerations and the application of Fair Information Practice Principles (FIPPs).
- **How to streamline the collection and sharing of digital identity data:** This includes how to collect and share data for digital identities, attributes, and unique identifiers; how to integrate digital identities into business processes; and how to secure electronic sharing of attributes.
- **How to fully leverage PIV and PIV-I credentials:** This section covers PIV and PIV-I basics, authentication mechanisms, challenges related to HSPD-12, federation across agency boundaries, and uses above and beyond the mandated physical and logical access requirements.
- **How to manage physical and logical access control convergence:** This is guidance on processes and technologies common to both physical and logical controls.

- **How to modernize physical and logical access infrastructures:** This includes implementation planning, architecture and design, technical implementation, and the physical concerns of local facility and visitor access.
- **How to implement identity federation:** In this section, a summary of the reasons to federate and an overview of federation trust topologies, which leads into a discussion of the Federal Trust Framework. Provisioning external (non-Federal-government) users and federation using third-party credentials is also discussed.

The How of Implementing FICAM

Version 2.0 of the FICAM Roadmap and Implementation Guidance document provides – for the first time – significant actual guidance in how agencies can implement FICAM processes and services.

The guidance is complex, but with that guidance, along with the appropriate software solutions, agencies can conform to the FICAM framework, and in doing so, move toward developing the security and efficiencies that were the original stated intent of FICAM.

Version 2.0 of the FICAM Roadmap and Implementation Guidance document can be [found here](#).

FICAM element	One Identity solution	
Credential management	<ul style="list-style-type: none"> • Defender • Enterprise Single Sign-on • One Identity Safeguard for Privileged Sessions 	<ul style="list-style-type: none"> • Password Manager • Privileged Access Suite for Unix • Starling Two-factor Authentication
Identity management	<ul style="list-style-type: none"> • One Identity Safeguard for Privileged Passwords • Identity Manager • Active Roles • Authentication Services 	<ul style="list-style-type: none"> • Active Administrator • Cloud Access Manager • Enterprise Single Sign-on • Password Manager
Access management	<ul style="list-style-type: none"> • Active Roles • Cloud Access Manager • Identity Manager 	<ul style="list-style-type: none"> • Identity Manager – Active Directory Edition • Identity Manager – Data Governance Edition • Starling Connect
Federation	<ul style="list-style-type: none"> • Cloud Access Manager 	
Auditing and reporting	<ul style="list-style-type: none"> • Active Roles • Change Auditor for Logon Activity • Change Auditor for Windows File Servers • Change Auditor for NetApp • Change Auditor for Active Directory • Change Auditor for SharePoint • Change Auditor for EMC • Change Auditor for SQL Server 	<ul style="list-style-type: none"> • Change Auditor for Exchange • Change Auditor for VMware vCenter • Cloud Access Manager • InTrust • Identity Manager • Starling Identity Analytics & Risk Intelligence • Enterprise Reporter

About One Identity

One Identity, a business unit of Quest Software, helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at [OneIdentity.com](https://www.oneidentity.com)

© 2018 One Identity LLC ALL RIGHTS RESERVED. One Identity, and the One Identity logo are trademarks and registered trademarks of One Identity LLC in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.oneidentity.com/legal. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.
 Datasheet_2018_PublicSector-mandate-update-ficam-v2_US_RS_36749