U.S. Department of Labor ICAM Implementation Plan - Status February 2024

Objective/References: Office of Management and Budget Memorandum (M-19-17) dated May 21, 2019 "Enabling Mission Delivery through Improved Identity, Credential, and Access Management"

Purpose: Contextualizing Identity in the Federal Government

For the purposes of this policy, "identity" refers to the unique representation of a subject, for example, a person, a device, a non-person entity (NPE), or an automated technology, that is engaged in a transaction involving at least one Federal subject or a Federal resource, for example, Federal information, a Federal information system, or a Federal facility or secured area. This policy may refer to identity in two contexts: (1) Federal enterprise identity or (2) public identity. Federal enterprise identity, or, simply, enterprise identity, refers to the unique representation of an employee, a contractor, an enterprise user, such as a mission or business partner, a device, or a technology that a Federal agency manages to achieve its mission and business objectives. Public identity refers to the unique representation of a subject that a Federal agency interacts with, but does not directly manage, in order to achieve its mission and business objectives. Public identity may also refer to a mechanism of trust used to render services to the American public.

	M-19-17 Agency Objectives	Responsible Party	Status	Schedule
III.2	Agencies shall require PIV credentials (where applicable in accordance with OPM requirements) as the primary means of identification and authentication to Federal information systems and federally controlled facilities and secured areas by Federal employees and contractors.	Security Center & OCIO	In Place	Q2 FY2020
III.2(1)	Agencies shall use Derived PIV Credentials for Federal employees, contractors, and other enterprise users (where applicable in accordance with OPM requirements) and enable the acceptance of Derived PIV Credentials by applications and devices.	OCIO	Partial	Q2FY2025 As permitted in OMB M-22-09, DOL is adopting FIDO-2 compliant methods rather than derived PIV to accomplish this purpose
III.2(2)	Agencies shall work with the Federal CIO Council, the Federal Privacy Council, and NIST to pilot additional solutions (e.g., different authenticators) that meet the intent of HSPD-12 and advance the technical approach to managing identities. The output of these pilots will drive improvements to NIST guidelines and Government-wide ICAM requirements including areas such as mobile and cloud identity.	OCIO	In Place	Q3 FY2021
III.3(1)	Implementing processes for the electronic verification of PIV identity assertions from other agencies.	Security Center & OCIO	In Place	Q2 FY2022
III.3(2)	Accepting and leveraging existing, valid PIV credentials, including those issued by other agencies and electronically verified, rather than issuing new ones. This is equally applicable for logical and physical access (where authorized).	Security Center & OCIO	In Place	Q4 FY2022
IV.1(1)	***Governance*** . Each agency shall designate an integrated agency-wide ICAM office, team, or other governance structure in support of its Enterprise Risk Management capability to effectively govern and enforce ICAM efforts.	OASAM, OCFO, SOL	In Place	Q1 FY2020
IV.1(1)(2)	Chief Operating Officers or the agency equivalent role shall ensure that there is regular coordination among agency leaders and mission owners to implement, manage, and maintain the agency's ICAM policies, processes, and technologies.	Deputy Secretary	In Place	Q2 FY2020
IV.1(1)(3)	While the agency governance structure described above will facilitate oversight of the implementation of Government-wide and agency enterprise-specific requirements, all bureaus, components, and other organizations at the sub-enterprise level must support efforts to harmonize ICAM across their respective agency by adhering to requirements and fostering accountability at all levels of the organization.	DOL	In Place	Q4 FY2020
IV.1(2)	Each agency shall define and maintain a single comprehensive ICAM policy, process, and technology solution roadmap, consistent with agency authorities and operational mission needs. These items should encompass the agency's entire enterprise, align with the Government-wide Federal Identity, Credential, and Access Management (FICAM) Architecture and CDM requirements, incorporate applicable Federal policies, standards, playbooks, and guidelines, and include roles and responsibilities for all users.	DOL_ICAM_Gov	In Place	Q2 FY2022
IV.1(3)	Each agency shall outline agency-wide performance expectations for security and privacy risk management throughout the identity lifecycle. These performance expectations shall support Government-wide management requirements, such as the President's Management Agenda (PMA) Cross Agency Priority (CAP) goals.	DOL_ICAM_Gov	In Place	Q2 FY2020
IV.1(3)(1)	Agencies shall incorporate objectives for improving ICAM into their strategic plans and review their progress with OMB as part of their strategic reviews.	DOL_ICAM_Gov	In Place	Q2 FY2020
IV.1(4)	Each agency shall incorporate Digital Identity Risk Management into existing Federal processes as outlined in NIST SP 800-63, including the selection of assurance levels commensurate with the risk to their digital service offerings.	DOL_ICAM_Gov	In Place	Q4 FY2021
IV.1(4)(1)	Agencies shall use these levels to make risk-informed decisions when selecting and using processes and technologies implemented across the ICAM environment.	DOL_ICAM_Gov	In Place	Q4 FY2022

IV.1(4)(2)	Agencies shall update legacy e-Authentication risk assessments to shift away from the obsolete Levels Of Assurance model.	DOL_ICAM_Gov	In Place	Q2 FY2022
IV.1(4)(3)	Agencies shall coordinate with state, local, and tribal governments, other entities, and individuals to provide identity verification and access control appropriate to the risk level and performance of the business function in cases where information sharing or collection is required for business and mission functions.	DOL_ICAM_Gov	In Place	Q2 FY2022
IV.1(4)(4)	Agencies shall share feedback on their implementation of the Digital Identity Risk Management process with the Federal CIO Council, Federal Privacy Council, and NIST to drive improvements to NIST SP 800-63.	DOL_ICAM_Gov	In Place	Q2 FY2020
IV.2(1)	***Architecture*** **.** Agencies shall establish authoritative solutions for their ICAM services by rationalizing the ICAM capabilities that they will keep, replace, retire, or consolidate. Agencies are encouraged to promote flexible and scalable solutions that can work across the agency and change as mission needs evolve.	DOL_ICAM_Gov	In Place	Q2 FY2021
IV.2(2)	Agencies shall ensure that deployed ICAM capabilities are interchangeable, use commercially available products, and leverage open Application Programming Interfaces (APIs) and commercial standards to enable componentized development and promote interoperability across all levels of government.	DOL_ICAM_Gov	In Place	Q2 FY2020
IV.2(3)	Agencies shall manage the digital identity lifecycle of devices, non-person entities (NPEs), and automated technologies such as Robotic Process Automation (RPA) tools and Artificial Intelligence (AI), ensuring the digital identity is distinguishable, auditable, and consistently managed across the agency. This includes establishing mechanisms to bind, update, revoke, and destroy credentials for the device or automated technology.	DOL_ICAM_Gov	In Place	Q3FY2023
IV.2(5)	Agencies shall leverage federated solutions to accept identity and authentication assertions made by mission and business partners.	DOL_ICAM_Gov	In Place	Q2 FY2020
IV.2(5)(1)	Agencies shall accept assertions by partners based on digital identity risk and associated assurance levels in accordance with NIST guidelines and Government-wide ICAM requirements.	DOL_ICAM_Gov	In Place	Q2 FY2020
IV. 2(5)(2)	Agencies shall confirm that these assertions use open commercially available standards to the extent available.	DOL_ICAM_Gov	In Place	Q2 FY2020
IV.3(4)	***Aquisition*** . Agencies shall leverage the CDM Program to accelerate their procurement and deployment of tools related to the ICAM capabilities in Phase 2 or future phases.	BOC	In Place	Q2 FY2020
V.1	Agencies shall ensure that identity proofing for Federal digital services provided to public consumers aligns with NIST guidance and Government-wide ICAM requirements.	DOL_ICAM_Gov	In Place	Q2 FY2021
V.3	Agencies shall establish processes based on digital identity risk and associated assurance levels to allow an individual to bind, update, use, and disassociate non-Government-furnished authenticators to their digital identity when accessing Federal digital services provided to public consumers.	DOL_ICAM_Gov	In Place	Q2 FY2022
V.4	Agencies shall leverage existing credentials and identity federations that meet the agency's determined acceptable risk level rather than standing up processes or capabilities to issue new credentials to users.	DOL_ICAM_Gov	In Place	Q2 FY2020
V.5	Agencies shall use Federally provided or commercially provided shared services, to the extent available, to deliver identity assurance and authentication services to the public.	DOL_ICAM_Gov	In Place	Q2 FY2020