Standard PR.AC: Identity, Credential, and Access Management

February 2nd, 2021

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

APPROVAL

Steven Hernandez Digitally signed by Steven Hernandez
Date: 2021.02.09 11:50:53 -05'00'

Steven Hernandez **Date**

Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Draft Date	Summary of Changes
1.0	11/19/2020	Initial draft

Table of Contents

APPROVAL ii

1 INTRODUCTION 1

1.1 Purpose 1

1.2 Background 1

1.3 Scope 2

1.4 Risk Acceptance/Policy Exceptions 2

2 STANDARDS 2

2.1 Governance 2

2.2 Architecture 4

2.3 Acquisition 5

3 APPENDIX A: ACRONYMS 7

4 APPENDIX B: AUTHORIZING REFERENCES 8

1 INTRODUCTION

This document establishes Department of Education (ED) standards for Identity, Credential, and Access Management (ICAM).

This Standard complies with Office of Management and Budget (OMB) Directive M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management:

> *Each agency shall define and maintain a single comprehensive ICAM policy, process, and technology solution roadmap, consistent with agency authorities and operational mission needs.*

OMB M-19-17 also states:

> *To ignite adoption of this new mindset around ICAM capability deployment across the Federal Government, each agency must harmonize its enterprise-wide approach to governance, architecture, and acquisition.*

1.1 Purpose

This document sets the ED standards needed for ED to comply with the above requirements for governance, architecture, and acquisition. In doing so, it supersedes any prior documentation establishing such standards.

1.2 Background

The National Institute of Standards and Technology (NIST) defines ICAM as the following:

> *Programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-person entities (NPEs), bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources.*

According to OMB M-19-17:

> *Agencies shall establish capabilities aligned to Federal ICAM Architecture and Continuous Diagnostics and Mitigation (CDM) requirements that enable the continuous vetting and evaluation of fitness of personnel subject to HSPD-12.*

Advances in technology enable more digital and business transactions which provide the opportunity to improve service delivery. ED continues to modernize and consolidate Information Technology (IT) infrastructure and services to improve efficiency, effectiveness, security, and customer experiences. New challenges have emerged along

with these advances, such as data breaches exposing controlled unclassified information (CUI); e.g., passwords and Personally Identifiable Information (PII), in particular. Identity management has become even more critical to ED's successful delivery of services.

To ensure secure and efficient operations, ED must be able to identify, credential, monitor, and manage identities that access federal resources, such as data, information systems, facilities, and secured areas. ED must conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access control. The implementation of these processes significantly affects the security, privacy, and delivery of the ED mission; and enhances the trust and safety of digital transactions with the American public.

The ED Enterprise ICAM (referred to as ED ICAM) transformation is part of a larger government wide mandate to implement ICAM security disciplines. This will enable the right individual to access the right resources, at the right time, for the right reasons. The ED ICAM program includes policy, processes, technologies, and personnel. Together, they identify, credential, monitor, and manage user access to information and information systems for ED.

1.3 Scope

The standards established in this document apply to all employees, contractors, and users authorized to access ED information systems.

1.4 Risk Acceptance/Policy Exceptions

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

2 STANDARDS

ED complies with the requirements for governance, architecture, and acquisition by adherence to the following standards.

2.1 Governance

ICAM requires an enterprise-wide approach to harmonize governance, architecture, and acquisition and to ensure an efficient and effective implementation. To accomplish this; ED established an ICAM Program Office for the enterprise, as described below.

- Manage, administer, maintain, and continually improve the program to meet regulatory requirements.
- Lead and synchronize ICAM implementation activities for all of ED.
- Define, implement, and govern; the policy, processes, and technology solutions; to deliver enterprise ICAM capabilities to all of ED.
- Be responsible for daily operations, maintenance, and integration support; of ICAM shared services for managing digital identities, credentials, and access; to ED systems and applications.

ACS Departmental Directive OCIO: 3-112 describes the governance structure the Secretary of ED delegates to ensure full compliance with the Federal IT Acquisition Reform Act (FITARA). The ED ICAM Program Office complies with this mandate as described below.

1. The ICAM Stakeholder Group gathers technical requirements
    a. Includes IT Principal Office Coordinators (IT POC), Information System Owners (ISO) and Information System Security Officers (ISSO); to coordinate implementation, management, and maintenance of ICAM capabilities.
    b. Ensures ICAM processes, procedures, and technology solutions meet agency requirements for delivery.
2. Planning and Investment Review Working Group (PIRWG), described in *ED IT Investment Management Process Guide,* settles issues submitted by the ICAM Stakeholder Group
3. FITARA Implementation Working Group (FIWG), described in *FITARA Implementation Working Group (FIWG) Charter*, further settles issues, if needed

The ED ICAM Program Office will outline performance expectations; including security and privacy risk management; throughout the identity lifecycle for the enterprise. These performance expectations must support the President's Management Agenda (PMA) Cross Agency Priority goals and align with the Government-wide Federal Identity, Credential, and Access Management (FICAM) Architecture and Continuous Diagnostics and Mitigation (CDM) requirements.

As outlined in NIST Special Publication (SP) 800-63-3, principal offices and other ED components must incorporate Digital Identity Risk Management into their existing processes when working with ICAM integrations. ED ICAM integrations require an Interconnection Security Agreement (ISA)/ Memorandum of Understanding (MOU)

document. The ISA/MOU must be completed in compliance with the requirements set forth in NIST SP 800-47.

2.2 Architecture

The ED ICAM Program Office must establish solutions for ICAM services; and maintain a technology solution roadmap for the enterprise. ED ICAM solutions must adhere to the following:

- Align with the FICAM architecture; based on the FICAM Roadmap and Implementation Guidance
- Align with CDM requirements
- Align with applicable federal policies, standards, playbooks, and guidelines
- Publish in the ICAM service catalog

All ED principal offices and other ED components must use the following:

- ED ICAM shared services to fulfill their ICAM requirements. Any exception to using ED ICAM shared services must be approved using the waiver process.
- ED ICAM shared services; for credentialing and identity proofing public consumers who require access to ED digital services.
- ED ICAM is the authoritative source for managing the digital identity lifecycle of all person identities. This includes all categories of ED personnel; as well as public citizens who require access to ED online services.
- ED ICAM is the authoritative source for managing the digital identity lifecycle of all Non-Person Entities (NPE). This includes service accounts and automated technologies, such as Robotic Process Automation tools and Artificial Intelligence. EIMS ensures the digital identity is distinguishable, auditable, and consistently managed.

All ED systems or applications that store, maintain, or consume user accounts; must do the following.

- Integrate with the ED ICAM to manage the digital identity lifecycle; and to enable compliance auditing and reporting.
- Establish processes to manage access control. Revoke access privileges when no longer authorized. Revoke or destroy credentials in a timely manner; to prevent unauthorized access to information systems.

All ED systems or applications that require authentication must use one of the approved enterprise authentication services as appropriate for the system use cases.

- Enterprise Active Directory for ED's domain for end user office automation services

- ED's privileged access system for privileged access
- ED ICAM access management services for all web and mobile application access, including internal users and public citizens
- Login.gov for externally facing (internet facing) authentication requirements.

All ED principal offices and other ED components must require the use of Homeland Security Presidential Directive (HSPD)-12 compliant credentials by all federal employees and contractors. These credentials include, but are not limited to, the following.

- Personal Identity Verification Credential (PIV).
- Personal Identity Verification Interoperable Credential (PIV-I).
- Derived PIV (PIV-D)
- Emergency PIV Alternative (PIV-A)

The HSPD-12 credentials serve as the primary means of identification and authentication to federal information systems, federally controlled facilities, and other secured areas.

As technology evolves, ED ICAM will review or approve agency specific implementation of additional credential solutions (e.g., different authenticators). These credential solutions must meet the intent of HSPD-12 and align with NIST guidelines and government wide ICAM requirements, such as mobile and cloud identity.

All ED principal offices and other ED components must require and implement the use of the PIV credential digital signature capability for internal and external business.

All ED principal offices and other ED components must ensure use of the PIV credential for physical access to federal facilities[1] and secured areas is implemented in accordance with Department Physical Security policy

2.3 Acquisition

IT products and tools procured that require user authentication must comply with one of the following.

- Support PIV or other HSPD-12 compliant credentials.
- Integrate with ED ICAM shared services that enable HSPD-12 compliant authentication through commercially available open standards.

[1] 48 CFR 2.101 (Title 48, Federal Acquisition Regulations System; Chapter 1, Federal Acquisition Regulation; Subchapter A, General; Part 2, Definitions of Words and Terms; Subpart 2.1, Definitions)

All contracts requiring contractors to have access to federally controlled facilities, or information systems, must include requirements to comply with HSPD-12 and Federal Information Processing Standards Publication (FIPS) 201-2. This standard is based on OPM requirements and the Federal Acquisition Regulation (FAR), 48 Code of FR § 4.13.

Products and services acquired to further HSPD-12 or ICAM implementations must be compliant with the following.

- OMB policy
- NIST standards
- General Services Administration (GSA) Approved Products List
- CDM Approved Products List (when applicable)

3 APPENDIX A: ACRONYMS

CISO	Chief Information Security Officer
COR	Contracting Officer's Representative
CDM	Continuous Diagnostics and Mitigation
CUI	Controlled Unclassified Information
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards Publication
FITARA	Federal IT Acquisition Reform Act
FIWG	FITARA Implementation Working Group
HSPD	Homeland Security Presidential Directive
ICAM	Identity, Credential, and Access Management
ISO	Information System Owner
ISSO	Information Systems Security Officer
NIST	National Institute of Standards and Technology
NPE	Non-person entity
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIRWG	Planning and Investment Review Working Group
POC	IT principal office coordinators

4 APPENDIX B: AUTHORIZING REFERENCES

- FAR 48 Code of FR § 4.13
- FIPS 201-2
- NIST SP 800-47
- NIST SP 800-53
- NIST SP 800-63-3
- NIST SP 800-116
- OMB M-19-17
- ED ACS Departmental Directive OCIO: 3-112
- ED IT Investment Management Process Guide
- FITARA Implementation Working Group (FIWG) Charter