U.S. DEPARTMENT OF COMMERCE

UNITED STATES DEPARTMENT OF COMMERCE
Identity, Credential and Access Management (ICAM) Policy

May 2021

Table of Contents

1. PURPOSE

a. This Departmental Policy establishes the Department of Commerce (DOC) policy for Identity, Credential, and Access Management (ICAM) for unclassified systems and institutes the authority for ICAM governance, policy, procedure, and technology.

b. This policy complies with the requirements of:

(1) Office of Management and Budget (OMB) Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*;

(2) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63 Rev 3, *Digital Identity Guidelines*;

(3) NIST SP 800-157;

(4) Federal Information Processing Standards Publication (FIPS) FIPS 201-2;

(5) NIST SP 800-53 Rev 4;

(6) *The Electronic Signatures in Global and National Commerce Act*, Public Law 106-229;

(7) The Uniform Electronic Transaction Act (UETA), 1999; and

(8) FIPS PUB 186-4, *Digital Signature Standard (DSS)*.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

Nothing in this policy will alter the requirements for the protection of information associated with national security systems such as those identified in the *Federal Information Security Modernization Act* (FISMA), 44 United States Code § 3551, or the policies, directives, instructions, or standards issued by the Committee on National Security Systems (CNSS) or the intelligence community.

3. SCOPE

a. The policies, roles, and responsibilities described herein are applicable to all DOC Mission Areas, Operating Units (OU), and staff offices, employees, appointees, contractors, and others who work for, or on behalf of, DOC.

b. This policy extends to the processes, procedures, and technology for any Information Technology (IT) system that requires the management or authentication of an "identity."

i. For the purposes of this policy, "identity" refers to the unique representation of a subject including a person, a device, a Non-Person Entity (NPE), or an automated technology such as Robotic Process Automation (RPA), that is engaged in a transaction involving at least one Federal subject or a Federal resource, including data, information systems, or facilities.

ii. This policy refers to identity in two contexts: 1) Federal enterprise identity and 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 (collectively referred to as staff). Public identity refers to the unique representation of a subject that a Federal Agency interacts with, but does not directly manage, 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.

c. Detailed supporting processes, procedures, and requirements will be described in associated ICAM Service Catalog.

4. BACKGROUND

Advances in technology have enabled more digital interactions and business transactions, offering the Federal Government an opportunity for improved service delivery. Accordingly, DOC continues to modernize and consolidate its IT infrastructure and services to improve efficiency, effectiveness, security, and customer experience. However, with these opportunities new challenges have emerged. As information about individuals, including Personally Identifiable Information (PII) and passwords, are exposed through data breaches, identity management has become even more critical to the Federal Government's successful delivery of services to the American public.

To ensure secure and efficient operations, DOC must be able to identify, credential, monitor, and manage identities that access Federal resources, including information, information systems, facilities, and secured areas across their respective enterprises. How the DOC will conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access control significantly affects the security, privacy, and delivery of the DOC mission as well as the trust and safety of digital transactions with the American public.

DOC's ICAM program is a part of a larger government-wide mandate to address implementation of ICAM security disciplines that enable the right individual to access the right resources, at the right time, for the right reasons. DOC's ICAM program comprises the policy, processes, technologies, and supporting personnel used to identify, credential, monitor, and manage user access to information and information systems throughout the DOC enterprise.

5. POLICY

a. ICAM Governance

i. ICAM requires an enterprise-wide approach to harmonize governance and ensure efficient and effective implementation. Therefore, DOC will establish and maintain an ICAM Advisory Council (IAC). The IAC will govern the DOC ICAM program by setting policy and approving budgets related to ICAM. The IAC structure, functions, roles, and responsibilities are described in greater detail in the ICAM Advisory Council Charter.

ii. DOC will establish an enterprise-level ICAM Program Office (IPO) to manage and administer the program, including management, maintenance, and continual improvements to meet Department and regulatory requirements.

iii. To ensure ICAM processes, procedures, and technology solutions meet agency requirements for mission delivery, DOC must establish and maintain an ICAM Working Group (IWG). The IWG structure, functions, roles, and responsibilities will be described in an associated IWG Charter.

iv. To ensure regular coordination among the DOC Mission Areas to implement, manage, and maintain ICAM capabilities, each DOC Mission Area must designate an ICAM liaison to serve on the IWG. The IWG is responsible for planning, coordinating, and implementing OU-specific ICAM initiatives, directives, and activities in coordination with the ICAM Program Office and communicating processes and procedures to its user population.

v. The DOC IPO will be the lead in ICAM implementation and will be responsible for the implementation and governance of the processes and technology solutions required to deliver enterprise identity, credential, and access management capabilities to all DOC. Additionally, the ICAM Program Office is responsible for daily operations, maintenance, and integration support of enterprise-level ICAM shared services.

vi. The DOC ICAM Program Office will work with the DOC ICAM Working Group to ensure solutions support the needs of the Department.

vii. The DOC ICAM Program Office will propose ICAM budgets and changes in DOC ICAM policy to the ICAM Advisory Council as required.

viii. DOC must outline enterprise-wide performance expectations for ICAM capabilities, including security and privacy risk management throughout the identity lifecycle. These performance expectations must support the President's Management Agenda (PMA) Cross Agency Priority (CAP) goals.

ix. The DOC ICAM Program Office will propose enterprise-wide performance expectations to the ICAM Advisory Council for acceptance.

x. Agencies must incorporate Digital Identity Risk Management into existing processes as outlined in NIST SP 800-63, including the selection of assurance levels commensurate with the risk to their digital service offerings.

b. ICAM Architecture

i. The ICAM Program Office must establish authoritative enterprise-wide solutions for ICAM services and maintain a technology solution roadmap. Enterprise-wide ICAM solutions must:

1. Align with the governmentwide Federal Identity, Credential, and Access Management (FICAM) Architecture;

2. Align with Continuous Diagnostic and Mitigation (CDM) requirements;

3. Incorporate applicable Federal policies, solutions, standards, playbooks, and guidelines;

4. Support integration of Mission Area solutions where practical; and

5. Be published in the ICAM service catalog.

ii. Mission Areas, agencies, and staff offices must use enterprise ICAM shared services to fulfil their ICAM requirements and rationalize existing ICAM capabilities that they will integrate, replace, retire, or consolidate.

iii. Mission Areas, agencies, and staff offices must use enterprise ICAM shared services or approved federal solutions for credentialing and identity proofing (when required) public consumers who require access to DOC public facing digital services.

iv. Mission Areas, agencies, and staff offices must use the authoritative ICAM shared services to manage the digital identity lifecycle of all DOC person identities, to include employees, appointees, contractors, and others who work for, or on behalf of, DOC as well as public citizens who require access to DOC online services.

v. Mission Areas, agencies, and staff offices must use the authoritative ICAM shared service to manage the digital identity lifecycle of devices, NPEs, and automated technologies such as RPA tools and Artificial Intelligence (AI), to ensure the digital identity is distinguishable, auditable, and consistently managed. This includes processes to bind, update, revoke, and destroy credentials for the device or automated technology.

vi. All DOC systems or applications that store, maintain, or consume user accounts must:

1. Integrate with the authoritative ICAM Enterprise Identity Management Services (EIMS) to manage the digital identity lifecycle and to enable compliance auditing and reporting; and

2. Establish processes to manage access control, including the ability to revoke access privileges when no longer authorized and to revoke or destroy credentials in a timely manner to prevent unauthorized access to information systems.

vii. Mission Areas, agencies, and staff offices must require Homeland Security Presidential Directive (HSPD)-12 compliant credentials, including but not limited to Personal Identity Verification Credential (PIV), Personal Identity Verification Interoperable Credential (PIV-I), and Derived PIV (where applicable in accordance with Office of Personnel Management (OPM) requirements) as the primary means of identification and authentication to Federal information systems, Federally controlled facilities, and other secured areas by Federal employees and contractors.

1. As technology evolves, the DOC ICAM Program will, in cooperation with the DOC Chief Information Security Officer (CISO), review or approve OU - specific implementation of additional credential solutions (e.g., different authenticators) that meet the intent of HSPD-12 and align to NIST guidelines and governmentwide ICAM requirements such as mobile and cloud identity.

2. Mission Areas, OU, and staff offices must follow the standard PIV exemption process approved by the ICAM Program Office and CISO.

viii. Mission Areas, agencies, and staff offices must require and implement the use of the PIV credential digital signature capability for internal business. When signature transactions include individuals that fall outside the scope of PIV applicability, Mission Areas, agencies, and staff offices should define and use alternative digital or electronic signature mechanisms commensurate with the risk of the transaction.

ix. Mission Areas, agencies, and staff offices must ensure that use of the PIV credential for physical access to Federal facilities and secured areas is implemented in accordance with *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (or any successive version) and NIST Special Publication (SP) 800-116 Revision l, *Guidelines for the Use of PIV Credentials in Facility Access* (or any successive version).

c. Acquisition of ICAM Capabilities and Services

i. IT products and tools procured that require user authentication must support PIV or other HSPD-12 compliant credentials or must be able to integrate with ICAM

shared services that enable HSPD-12 compliant authentication through commercially available open standards.

ii. All contracts requiring contractors to have access to Federally-controlled facilities or access to Federally-controlled information systems must include a requirement to comply with HSPD-12 and FIPS 201-2 for affected contractor personnel based on OPM requirements and the Federal Acquisition Regulation (FAR), 48 Code of FR § 4.13 .

iii. The Department of Homeland Security (DHS) CDM Program will be leveraged to accelerate procurement and deployment of tools related to the ICAM capabilities of CDM (formerly known as CDM Phase 2).

iv. Products and services acquired to further HSPD-12 and ICAM implementations must be compliant with OMB policy, NIST standards, and when applicable the General Services Administration (GSA) GSA approved products list (APL) and CDM Approved Products List.

d. In carrying out responsibilities under this policy, all Department officers, employees, and contractor personnel must comply with agency policies and practices concerning confidentiality and whistleblower protections and all applicable provisions under the Privacy Act, 5 U.S.C. § 552a, the Whistleblower Protection Act, 5 U.S.C. § 2302, and any other related law, regulation, or policy.

6. ROLES AND RESPONSIBILITIES

a. The DOC Chief Information Officer (CIO), will:

(1) Ensure there is regular coordination among the CIO, OU CIO and Mission Area, OU, and staff office leaders to implement, manage, and maintain the DOC's ICAM policies, processes, and technologies; and

(2) Ensure establishment of the ICAM Advisory Council, chartered under the current DOC CIO Council, that will maintain the charter for management of DOC ICAM program.

(3) Ensure the coordination, implementation, and management of federal ICAM requirements;

(4) Designate National Oceanic and Atmospheric Administration (NOAA) CIO as enterprise ICAM Program Office to manage and administer the DOC ICAM Program in accordance with federal governmentwide policies and regulations;

(5) Provide oversight of Mission Area, agency, and staff office acquisition of ICAM technology solutions to eliminate duplication with enterprise shared service capabilities;

(6) Publish and maintain an ICAM service catalog.

b. The DOC Chief Information Security Officer (CISO) must:

(1) Provide oversight to the assessment and accreditation of Mission Area, OU, and staff office systems to ensure compliance with this policy.

(2) Incorporate Digital Identity Risk Management assessment as outlined in NIST SP 800-63 into the existing Risk Management Framework (RMF) process, including the selection of assurance levels commensurate with the risk to systems and applications; and

(3) Ensure continued coordination between the DOC CDM Program and the DOC ICAM Program.

c. The DOC ICAM Program Manager must:

(1) Provide enterprise-level ICAM shared service platforms to support managing identities, credentials, and access to DOC and Mission Area, OU, and staff office applications, systems, and services in accordance with the Federal ICAM Architecture and CDM Requirements;

(2) Evaluate and recommend federal shared ICAM offering for use within the enterprise ICAM solution;

(3) Publish and maintain the ICAM guidance, or handbooks, which will provide detailed information and guidance about the use of systems and processes to meet the requirements in this ICAM policy; and

(4) Operate enterprise ICAM systems in compliance with DOC security requirements, and be responsible for assessment, authorization, and monitoring efforts.

d. DOC OU CIOs will:

(1) Comply with this policy, and governmentwide ICAM related mandates, regulations, and guidance;

(2) Participate in the DOC ICAM Advisory Council process and designate an ICAM Liaison to coordinate activities with the ICAM Program Office;

(3) Use enterprise ICAM shared services for the creation and maintenance of identity and credential information for all persons accessing DOC Logical Access Control Systems (LACS);

(4) Ensure that all persons accessing Departmental systems have a DOC accepted identity and enforce the PIV card usage to meet Federal requirements;

(5) Request extensions and/or exceptions in accordance with Departmental guidance for systems or processes that cannot be aligned to the ICAM program directives;

(6) Waivers or request for deviations of the approved ICAM program requirements are still required to meet all Federal ICAM requirements; and

(7) Work with the DOC ICAM Program and DOC Continuous Diagnostic Mitigation (CDM) Program to understand requirements and identify future CDM phase capabilities that support ICAM goals.

e. OU ICAM Liaisons will:

(1) Work directly with the ICAM Program Office on all ICAM program activities;

(2) Assist the DOC CIO with implementing ICAM in the Department and provide all details when any service or systems will be integrated with DOC ICAM system;

(3) Serve as the primary coordinator for all ICAM-related activities in the Department, and prioritize ICAM implementations as directed by DOC leadership, organizational leadership, and business needs; and

(4) Provide reports and data on the OU ICAM implementation activities and progress as requested by the ICAM Program Office or as required by Federal directive.

f. DOC Federal and Non-Federal Employees will:

(1) Notify their PIV credential sponsor and/or human resources point of contact of any changes in identity information, such as legal name or citizenship status;

(2) Use their PIV or other HSPD-12 compliant credential for accessing information systems and facilities, and follow the set procedures when PIV enforcement is not available;

(3) Not share their credentials and/or secret keys with another person; and

a. Secure their credentials and secret keys in a way that reduces the likelihood that others will use them.

2. POLICY EXCEPTIONS

(1) To request an exception to this policy, the application/system owner must contact the ICAM Program Office for the current security exception process.

(2) To be considered for an exception, an application/system must meet one of the following requirements:

a. A technical constraint that inhibits the use of or integration with the DOC enterprise ICAM services.

b. A transition plan is provided detailing when the asset will be retired or integrated with the enterprise ICAM service.

c. The extension request is for an individual system or application. No blanket or group extension requests will be accepted or approved.

d. All granted waivers must have a time limit and an expiration date of no more than 2 years and must not include an automatic extension clause. If the exception requires more time, a new extension request must be submitted and approved before the expiration date of the original extension. The extension request must be approved by the DOC CIO.

e. Alternative solutions must adhere to the Federal ICAM Architecture, NIST regulations for digital identity (including NIST SP 800-63 Rev 3), and CDM requirements. This information must be documented and will be reviewed by the ICAM Program Office before an extension is granted.

7. INQUIRIES
All inquiries pertaining to the contents of this policy can be submitted to ICAM@DOC.GOV

Effective Date: May 20, 2021

Approved By:

ANDRE MENDES

Digitally signed by ANDRE MENDES
Date: 2021.05.21 08:46:57 -05'00'

André V. Mendes
Chief Information Officer
U.S. Department of Commerce

–END–

APPENDIX A

ACRONYMS AND ABBREVIATIONS

AAL	Authentication Assurance Level
AI	Artificial Intelligence
API	Application Programming Interface
APL	Approved Products List
CDM	Continuous Diagnostic Mitigation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
DHS	Department of Homeland Security
DSS	Digital Signature Standard
EIMS	Enterprise Identity Management Services
FAL	Federation Assurance Level
FAR	Federal Acquisition Regulation
FICAM	Federal Identity Credential Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
IAL	Identity Assurance Level
ICAM	Identity, Credential, and Access Management
IT	Information Technology
NIST	National Institute of Standards and Technologies
NOAA	National Oceanic and Atmospheric Administration
NPE	Non-Person Entities
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	Personally Identifiable Information
PIV	Personal Identity Verification Credential
PIV-I	PIV-Interoperable Credential
PIV-D	Derived PIV Credential
PKI	Public Key Infrastructure
RMF	Risk Management Framework
RPA	Robotic Process Automation
UETA	Uniform Electronic Transaction Act

APPENDIX B

DEFINITIONS

a. Authoritative system – system designated by the Department's enterprise ICAM program to be the official primary source for identity-related records, data, or attributes; such a system may or may not be a system of record.

b. Application Programming Interface (API) – A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality. (Source: NIST, Computer Security Resource Center, Glossary)

c. Credential – An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a subscriber. Credentials can be something a person knows (such as password or personal identification number), something they have, something they are (such as a biometric feature) or some combination of these items.

d. Derived PIV credential – A credential issued based on proof of possession and control of a PIV smart card that has been issued in accordance with FIPS 201. When applied to PIV, identity proofing, and vetting processes do not have to be repeated to issue a Derived PIV Credential. (Sources: NIST, FIPS PUB 201-2, *Personal Identity Verification of Federal Employees and Contractors*, August 2003)

e. Directory Services –A distributed database service capable of storing information, such as certificates and Certificate Revocation Lists, in various nodes or servers distributed across a network. (Source: NIST, Computer Security Resource Center, Glossary)

f. Governance – A set of processes that ensures the effective and efficient use of information technology in enabling an organization to achieve its goals.

g. Non-Person Entity (NPE) – Any type of non-human device (e.g., routers, servers, switches, firewalls, sensors) or software object. (Source: Federal Identity, Credential, and Access Management 4 (FICAM) Roadmap and Implementation Guidance, December 2, 2011)

h. PIV credential – PIV smart cards or other form factors that comply with FIPS 201-2 or superseding standards. This includes technological enhancements of LincPass Smart Cards and derived credentials. (Source: NIST, FIPS PUB 201-2, *Personal Identity Verification of Federal Employees and Contractors*, August 2003)

i. PIV-I credential – PIV interoperable smart card that complies with FIPS 201-2 or superseding standards. (Source: NIST, FIPS PUB 201-2, *Personal Identity Verification of Federal Employees and Contractors*, August 2003)

j. Sponsor – The Sponsor is the employer or agency official responsible for authorizing and individual to apply for a credential, who has undergone Sponsor training and is designated to perform Sponsor functions. In the case of a contractor employees, the Sponsor maybe the COR, COTR, or another designated program official.

k. DOC Employee – A Federal civil servant employed by, detailed, or assigned to, DOC, including guest researchers for NIST, NOAA and other OUs.

l. DOC Personnel – DOC employees, contractors, affiliates, interns, fellows, and volunteers who work for, or on behalf of, DOC, and whose work is overseen by DOC employees.

m. Non-DOC Personnel -- not members of "DOC personnel" but use or maintain information systems for, or on behalf of, DOC. For example, state or local government or citizens that are users of DOC information systems; administrators of cloud systems that are operated for, or on behalf of, DOC.

n. Mission Area – all DOC Operating Units/bureaus and program offices.

APPENDIX C

AUTHORITIES AND REFERENCES

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017

Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0, December 2, 2011

Federal Acquisition Regulation (FAR), 48 CFR § 4.13, (2018)

FIPS PUB 186-4, *Digital Signature Standard (DSS)*, September 2013.

FIPS PUB 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* August 2013

The Government Paperwork Elimination Act, Public Law 105-277, Title XVII, October 21, 1998

The Paperwork Reduction Act, as amended, 44 U.S.C § 3501 et seq.,

DHS Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2014 with updates as of January 22, 2015

NIST SP 800 63-3, *Digital Identity Guidelines,* June 2017

NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, December 2014

OMB, Circular A-11, *Preparation, Submission and Execution of the Budget*, June 29, 2019, as amended

OMB, Circular A-130, *Managing Information as a Strategic Resource,* July 28, 2016

OMB, Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,* August 5, 2005

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, November 2016/2nd Edition

OMB Memorandum, *Reciprocal Recognition of Existing Personnel Security Clearances*, December 12, 2005, and M-06-21, *Reciprocal Recognition of Existing Personnel Security Clearances*, July 17, 2006

OMB, M-19-17, *Enabling Mission Delivery through Improved Identity, Credential and Access Management*, May 21, 2019

The Electronic Communications Privacy Act of 1986, 18 United States Code (U.S.C.) § 2701 et seq., (2017)

The Electronic Signatures in Global and National Commerce Act, Public Law 106-229, June 30, 2000

The Uniform Electronic Transaction Act (UETA), 1999

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a