GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2183.1
10/19/2021

GSA ORDER

SUBJECT: Enterprise Identity, Credential, and Access Management (ICAM) Policy

1. Purpose. In accordance with Office of Management and Budget (OMB) Memorandum M-19-17: Enabling Mission Delivery through Improved Identity, Credential, and Access Management, Federal Information Technology Acquisition Reform Act (FITARA), and the Federal Information Security Modernization Act (FISMA) this order sets forth the General Services Administration's (GSA) enterprise-wide ICAM policy, process, and provides a framework for a GSA enterprise ICAM technology solution roadmap and strategy. This order is consistent with agency authorities and operational mission needs. This order incorporates applicable Federal policies, standards, playbooks, and guidelines, and includes roles and responsibilities. New challenges have emerged along with these advances. Identity and access management has become even more critical to GSA's successful delivery of services.

2. Cancellation. This Order cancels and supersedes Instructional Letter CIO IL-20-01 Enterprise Identity, Credential, and Access Management (ICAM) Policy, dated November 17, 2020.

3. Explanation of Changes.

a. Removed deprecated policy references;

b. Updated links throughout;

c. Updated applicability section to include information about the Civilian Board of Contract Appeals (CBCA);

d. Updated divisions for roles and responsibilities;

e. Updated definition for public identity and federal enterprise identity;

f. Removed references to operational procedures; and

g. Removed references to Continuous Diagnostic and Mitigation (CDM) tools for clarification and consistency purposes.

4. Objectives. The Enterprise ICAM Policy provides a single source for identifying applicable ICAM policies and processes. It consolidates existing ICAM guidance and provides a framework for an enterprise-wide ICAM strategy. Advances in technology enable more digital and business transactions, and provide the opportunity to improve service delivery. GSA continues to modernize and consolidate Information Technology (IT) infrastructure and services to save costs, improve efficiency, effectiveness, security, and customer experience.

To ensure secure and efficient operations, GSA must identify, credential, monitor, and manage identities that access federal resources. These resources include data, information systems, and facilities. GSA must establish enterprise-wide digital identities, and adopt sound processes for authentication and access control. This significantly affects the security, privacy, and delivery of the GSA mission; and enhances the trust and safety of digital transactions with the American public. The Enterprise ICAM Policy is part of larger government-wide mandates to implement identity, authentication, and access control security disciplines. This will enable the right identity to access the right resources, at the right time, for the right reasons. ICAM requires an enterprise-wide approach; to harmonize governance, technology, and acquisition; and to ensure efficient and effective execution in support of our mission and business objectives.

5. Scope and Applicability.

a. This policy applies to all GSA Federal employees, contractors, and vendors of GSA, who manage, maintain, operate, or protect GSA systems or data, all GSA IT systems, and any GSA data contained on or processed by IT systems owned and operated by or on the behalf of any of the Services or Staff Offices. In addition, it also applies to physical access to GSA owned or leased facilities for GSA Federal employees, contractors, and vendors of GSA.

b. The provisions of this Order shall not be construed to interfere with, or impede, the legal authorities or independence of the Office of Inspector General or the CBCA.

c. This Order refers to “identity” in two contexts:

(1) Federal Enterprise Identity (or simply Enterprise Identity). Refers to the unique, GSA-managed representation of: GSA personnel as an enterprise user; a

device; or a technology. In the context of the federal enterprise, federal enterprise identity may refer to other federal executive branch agency civilian or defense personnel that are managed by the other federal agency, and

(2) Public Identity. Refers to the unique representation of: a person as a member of the populace; or persons affiliated with businesses and acting on behalf of the business entity and / or on the legal authority for the business entity.

6. Policy.

a. An ICAM Portfolio was established to meet the requirements of OMB M-19-17 and to serve as the ICAM governance structure (e.g., team, council, office) to effectively govern and enforce ICAM efforts for GSA enterprise. The ICAM Portfolio is led by the CISO and includes representatives from GSA IT divisions, and Staff and Service Offices. This group meets OMB M 19-17 requirements to establish an ICAM CIO Governance Board.

b. Policies implementing HSPD-12 and governing the use of GSA issued Personal Identity Verification (PIV) cards are established as follows:

(1) GSA Order ADM 2181.1, “Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors”;

(2) GSA Order ADM 5400.2, “General Services Administration Heads of Services and Staff Offices’ and Requesting Officials’ Roles and Responsibilities to Implement Homeland Security Presidential Directive-12”;

(3) GSA Order ADM 7640.3, “Termination Process and Oversight of General Services Administration (GSA) Issued Facility Access Cards in GSA Controlled Space in Both Owned and Leased Facilities”; and

(4) GSA Order ADM 5900.1, “Physical Access Control Systems in U.S. General Services Administration Controlled Space”.

c. Supporting ICAM governance and operational procedures will be defined and maintained in the following GSA IT Security Policy and supporting procedural guides:

(1) GSA Order CIO 2100.1, “GSA Information Technology (IT) Security Policy," identifies specific settings for ICAM security controls.

(2) Implementation of procedural guides in the ICAM family of controls is required by the GSA IT Security Policy, including CIO IT Security 01-07, “Access Control Procedural Guide” and CIO IT Security 01-01, “Identification and Authentication”.

d. Digital Identity Risk Management[1] has been incorporated into the GSA selection of assurance levels commensurate with the risk to the GSA digital service offerings as outlined in the established processes.

e. Systems containing Personally Identifiable Information (PII) must be designated with an Authentication Assurance Level (AAL) of 2 or higher.[2]

f. All new or modernizing GSA applications must have their ICAM capabilities evaluated by the ICAM Portfolio.

g. Any new request for inclusion with IT Standards related to an ICAM solution must be evaluated by the ICAM Portfolio.

h. Procurements of ICAM solutions or components by GSA Service or Staff offices, for use in GSA, must be reviewed by the ICAM Portfolio prior to fulfillment.

i. As technology evolves, the GSA ICAM Portfolio will develop enterprise roadmaps for agency-specific implementation of additional authentication solutions (e.g. different authenticators) for the enterprise. These must meet the intent of HSPD-12; and align with NIST guidelines and government wide ICAM requirements; such as mobile and cloud identity.

j. Procurements for services and products involving physical access control must be in accordance with GSA Order ADM 5900.1, Physical Access Control Systems in U.S. General Services Administration Controlled Space.

7. Responsibilities. ICAM roles and responsibilities are distributed across GSA as follows:

a. The ICAM Shared Services Portfolio. The ICAM Shared Services Portfolio (ICAM Portfolio), led by the Chief Information Security Officer (CISO), collaborates across IT and business lines to:

[1] Required by OMB Memorandum M-19-17, “Enabling Mission Delivery through Improved Identity, Credential, and Access Management,” May 21, 2019.
[2] Required by EO 13861, “Improving the Security of Customer Financial Transactions," October 17, 2014.

(1) Develop ICAM strategies to define requirements, eliminate duplicative efforts, identify technology standards, and align ICAM shared service capabilities across the agency.

(2) Implement ICAM strategies across GSA organizations.

(3) Review the existing ICAM environment to understand capability gaps and recommend improvement opportunities for IT Advisory Board (ITAB) consideration

(4) Evaluate business requirements to chart the future enterprise-wide ICAM environment of GSA.

(5) Develop and maintain a GSA enterprise-wide ICAM technology solution roadmap.

(6) Collaborate with the Identity, Credentialing and Access Management Sub-Committee (ICAMSC) of the Federal CISO Council to ensure Federal mandates and policies are reviewed and implemented.

b. Director, ICAM Shared Services Division, Office of the CISO (OCISO). Establish and manages an ICAM Program for service to GSA IT for:

(1) ICAM governance via a Program Management Office (PMO), including to develop the policy and program frameworks needed. The ICAM PMO provides dotted line support to solutions and enterprise shared ICAM services that are managed outside of the OCISO.

(2) Research and identify solutions for inclusion in an enterprise-wide ICAM technology solution roadmap from a technical perspective.

c. Chief Technology Officer (CTO). Manages the GSA IT Standards function. ICAM responsibilities include approving requests for new or updated software solutions (including ICAM) to be added to the GSA IT Standards.

d. Senior Agency Official for Privacy (SAOP). Responsible for the privacy program at GSA. ICAM responsibilities to include:

(1) Decide when it is appropriate to notify potentially affected persons of a breach of personally identifiable information (PII).

(2) Develop or revise documentation such as Systems of Record Notices (SORN), Privacy Impact Assessments (PIA), or privacy policies (e.g. Privacy Act Statements, agreements, policies).

(3) Evaluate the existing ICAM environment for existing information collections and recommend procedural and technological improvements that align with relevant NIST guidelines and the Fair Information Practice Principles (FIPPS) (e.g. data minimization).

(4) Evaluate GSA's PII inventory to chart the future ICAM environment of GSA.

e. Director, Infrastructure Management Division, Office of Digital Infrastructure Technologies (IDTO). Responsibilities include: Operate and maintain enterprise solutions supporting digital infrastructure including GSA enterprise IT accounts.

f. Personnel Security Division, Office of Chief Security Officer, Office Mission Assurance (OMA). The Personnel Security Division responsibilities include:

(1) Manage GSA Access Card issuance, usage and lifecycle maintenance for GSA personnel.

(2) Establish and implement the background investigation process for federal employees and contractors; managing background investigations; and determining suitability for employment for public trust positions in accordance with executive orders and Federal laws, as well as Office of Personnel Management (OPM) and Agency regulations, policies, and procedures.

g. Physical Security Division, Office of Chief Security Officer, Office of Mission Assurance (OMA). The Physical Security Division responsibilities include:

(1) Assist with the development of contracting documents (Statement of Work and Independent Government Cost Estimate) for compliant implementation of Physical Access Control Systems.

(2) Coordinate security matters in GSA facilities with the Federal Protective Service Headquarters to minimize physical access control issues.

h. Software Manager. Responsible for analyzing inventory data to ensure compliance with software license agreements, consolidate redundant applications, and identify other cost-saving opportunities.

8. ICAM Technology Solution Roadmap.

a. ICAM solutions should adhere to the following:

(1) Align with the Federal Identity, Credential, and Access Management (FICAM) architecture, as applicable.

(2) Align with Continuous Diagnostics and Mitigation (CDM) requirements, as applicable.

(3) Align to applicable federal policies, standards, playbooks, recordkeeping, and guidelines.

b. New GSA ICAM solutions or components must align with the defined GSA enterprise-wide ICAM technology solution roadmap unless the CISO deems otherwise.

c. All existing GSA applications must align to the defined GSA enterprise-wide ICAM technology solution roadmap or work with the ICAM Portfolio to develop an approved remediation plan to include projected timelines.

d. ICAM components must be documented sufficiently in the appropriate (i.e. System Security Plan) Authorization and Assessment package.

e. Robotics Process Automation (RPA) accounts must use a GSA enterprise-wide solution that ensures the digital identity is distinguishable, auditable, and consistently managed.

f. For any questions or to request further information about ICAM at GSA, please contact: icam-portfolio@gsa.gov

9. References.

a. Federal Information Technology Acquisition Reform Act (FITARA), Public Law 113-291, December 19, 2014.

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

c. OMB Memorandum M-19-17, “Enabling Mission Delivery through Improved Identity, Credential, and Access Management,” May 21, 2019.

d. GSA Order CIO 2160.1F CHGE 2, “GSA Information Technology (IT) Standards Profile,” March 31, 2017.

e. GSA Order CIO 2100.1M, “GSA Information Technology (IT) Security Policy," March 26, 2021.

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

g. GSA Order ADM 2181.1, “GSA HSPD-12 Personal Identity Verification and Credentialing," March 18, 2020.

h. FIPS 201-2, “Personal Identity Verification (PIV) of Federal Employees and Contractors," August 2013.

i. NIST SP 800-53, Revision 5, “Security and Privacy Controls for Federal Information Systems and Organizations," September 2020.

j. NIST SP 800-63-3, “Digital Identity Guidelines," June 2017 (includes updates as of 03-02-2020).

k. OMB Memorandum M-16-12, “Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing,” June 2, 2016.

l. GSA Order ADM 7640.3, “Termination Process and Oversight of General Services Administration (GSA) Issued Facility Access Cards in GSA Controlled Space in Both Owned and Leased Facilities,” September 16, 2016.

m. GSA Order ADM 5900.1, “Physical Access Control Systems in U.S. General Services Administration Controlled Space," April 14, 2017.

n. GSA Order CIO 9297.2C CHGE 1, “GSA Information Breach Notification Policy,” March 27, 2019.

o. GSA Order CIO 2108.2, “Software License Management," December 21, 2018.

p. Federal Information Security Modernization Act, Public Law 113-283, December 18, 2014.

10. Signature.

DocuSigned by:
David Shive
A3AE4284A2754F9...

DAVID SHIVE
Chief Information Officer
Office of GSA IT