Office of Management and Budget (OMB) M-19-17

Summary Gap Analysis

Template

**Table of Contents**

[1. Purpose 3](#_30j0zll)

[2. Summary 3](#_1fob9te)

[3. I. Contextualizing Identity in the Federal Government 4](#_tyjcwt)

[4. II. Managing Identities, Credentials, and Access in Modern Government 5](#_3dy6vkm)

[5. III. Adapting the Government’s Approach to Homeland Security Presidential Directive 12 (HSPD-12) 6](#_4d34og8)

[6. IV. Shifting the Operating Model Beyond the Perimeter 7](#_2s8eyo1)

[6.1. Governance 7](#_17dp8vu)

[6.2. Architecture 8](#_3rdcrjn)

[6.3. Acquisition 8](#_26in1rg)

[7. V. Improving Digital Interactions with the American Public 9](#_lnxbz9)

[8. VI. Enumerating Government-wide Responsibilities 10](#_35nkun2)

[8.1. NIST is responsible for: 10](#_1ksv4uv)

[Changes Between the Final and Draft Versions 11](#_44sinio)

[Appendix A - References and Associated Content 11](#_2jxsxqh)

# Purpose

The Office of Management and Budget (OMB) released the federal government’s Identity, Credential, and Access Management (ICAM) Memorandum M-19-17 on May 21, 2019. This document is an overview of what was released by the OMB with SAMPLE associated gaps and recommendations that are applicable to an agency landscape. This will facilitate creation of a comprehensive ICAM strategic roadmap and vision to fulfill the requirements presented in the [memorandum.](https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf)

# Summary

The OMB released a new memorandum setting the Federal Government’s ICAM policy for providing a greater level of identity assurance and privacy as it relates to entities interacting with Federal information systems and facilities. The memo notes:

* Agencies shall **implement flexible and scalable identity solutions** that can be utilized across agencies, such as **commercially available products and shared services**.
* In addition, agencies must develop an office and appropriate personnel to provide guidance and support regarding specific access controls to authorize or revoke privileges as necessary.
	+ In addition, the Chief Operating Officer (COO) or agency equivalent is responsible for ensuring coordination for implementation, management, and maintenance of the agency’s ICAM policies, processes, and technologies.
	+ Agencies must leverage National Institute of Standards and Technology (NIST) standards and Continuous Diagnostics and Mitigation (CDM) requirements as they implement policies, procedures, and technologies.

| **Gap Analysis** | **Recommendations** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
| *SAMPLE:* Lack of enterprise governance to successfully strategize and execute the core ICAM services and functions. Governance, for the purpose of this services framework, does not refer to the governance or management of an entire enterprise but of those capabilities necessary to ensure successful ICAM operations.  | *SAMPLE:* Implement governance functions that enable organizations to make programmatic decisions, manage enterprise policies, and promote the efficiency of the ICAM program.Update Charter to clearly reflect governance structure, roles and responsibilities, and enterprise buy-in for an enterprise approach.  |

# I. Contextualizing Identity in the Federal Government

* “Identity” is defined as a unique representation of a subject (person, device, non-person entity, or automated technology) engaged with at least one Federal subject or protected resource and may be referred to in two contexts:
	+ Federal enterprise identity – An employee, a contractor, an enterprise user, a device, or technology that is managed by a Federal agency.
	+ Public identity – A subject that a Federal agency interacts with but does not directly manage.

| **Gap Analysis** | **Recommendations** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
| *SAMPLE:* Lack of authoritative sources for Trainees, Volunteers, and Affiliates Identities | *SAMPLE:* Develop authoritative sources across the enterprise for digital identity |

# II. Managing Identities, Credentials, and Access in Modern Government

* The Federal Government is refreshing its digital infrastructure focused on cybersecurity, procurement and management of a workforce capable of operating cloud-based environments.
* Increased focus on adoption of policies and procedures to enhance privacy and storage.
* Agencies must update their ICAM policies that previously provided an insufficient level of assurance and align to NIST Special Publication (SP) 800-63 guidelines, and other standards/guidance released by NIST, the Office of Personnel Management (OPM), and the Department of Homeland Security (DHS) to form a comprehensive approach to identity management.

| **Gap Analysis** | **Recommendations** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# III. Adapting the Government’s Approach to Homeland Security Presidential Directive 12 (HSPD-12)

* Although HSPD-12 and Personal Identity Verification (PIV) remains the government-wide standard, agencies must adapt to the changing technology and offer flexible solutions.
	+ Agencies shall use PIV credentials as the primary means of identification and authentication for access to Federal systems and facilities.
	+ Agencies shall use PIV credentials for physical access to facilities in accordance with NIST SP 800-116 R1.
	+ Agencies shall implement access control processes to authorize and revoke privileges in a timely manner.
* Agencies must support cross-government identity federation and interoperability by remediating obstacles to accepting other agencies’ PIV credentials.
* Agencies must establish capabilities aligned to the Federal ICAM Architecture and CDM requirements.
* Agencies must require and implement PIV credential digital signature capability, and should use PIV credentials to encrypt information in transit

| **Gap Analysis** | **Recommendations** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# IV. Shifting the Operating Model beyond the Perimeter

## Governance

* Designate agency wide ICAM office, team or other governance structure with personnel from designated offices to maintain ICAM processes.
* Chief Operating Officer (COO) or agency equivalent is responsible for ensuring coordination for implementation, management, and maintenance of the agency’s ICAM policies, processes, and technologies.
* Agencies must define an ICAM solution roadmap aligned with the Federal ICAM and CDM requirements and outline the performance expectations for security and privacy that will support the President’s Management Agenda (PMA) and Cross Agency Priority (CAP) goals, and review progress with OMB per OMB Circular A-11.
* Agencies must incorporate Digital Identity Risk Management into existing processes as outlined in NIST SP 800-63, including the following activities:
	+ Use these risk levels for making solution decisions.
	+ Update legacy e-Authentication risk assessments.
	+ Coordinate with state, local and tribal governments to provide identity verification.
	+ Share feedback on Digital Identity Risk Management Process implementation with Federal Chief Information Officer (CIO) Council, Federal Privacy Council and NIST.

## Architecture

* Agencies shall establish authoritative solutions for their ICAM services by rationalizing the ICAM capabilities they will keep, replace, consolidate, etc., and should promote flexible, scalable, and interchangeable solutions to work across agencies including commercial systems and leverage open APIs.
* Agencies shall manage the digital identity lifecycle of devices, NPEs, and automated technologies, and control credentials.
* Agencies that are authoritative sources for attributes utilized in identity proofing events, shall establish privacy-enhanced data validation APIs for public and private sector access based on consumer consent.
* Agencies shall leverage federated solutions to accept identity and authentication assertions.

## Acquisition

* Agencies shall require all contractors that will have access to facilities or systems to comply with HSPD-12 and Federal Information Protection Services (FIPS) 201.
* Agencies shall require products and services are compliant with OMB policy, NIST and tech specs.
* Agencies shall leverage approved Tier 2 contract vehicles or federally provided shared services to procure digital certificates for identification and authentication.
* Agencies shall leverage CDM Program to accelerate their procurement and deployment of tools and to identify future ICAM capabilities.

| **Gap Analysis** | **Recommendations** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# V. Improving Digital Interactions with the American Public

* Agencies shall ensure that identity proofing for Federal digital services provided to public consumers aligns with NIST and ICAM requirements.
* Agencies shall limit the collection of personally identifiable information (PII) for establishing identity to what is legally authorized and necessary. Once collected, PII must be protected.
* Agencies shall establish processes allowing an individual to bind, update, use, and disassociate non-government furnished authenticators to their digital identity.
* Agencies shall leverage existing credentials and identity federations that meet the agency’s acceptable risk level rather than standing up processes or capabilities to issue new user credentials.
* Agencies shall use Federally provided or commercially provided shared services to deliver identity assurance and authentication services to the public, and should use shared service providers that leverage more than one solution.
* Agencies shall modify existing Privacy Act system of records when individuals consent is not available to reduce public burden.
* Agencies shall solicit direct feedback from consumers to determine demand for products and services and use shared services when possible.

| **Gap Analysis** | **Recommendations** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# VI. Enumerating Government-wide Responsibilities

## NIST is responsible for:

* Timelines and milestones for developing and updating guidance related to ICAM.
* Guidance on the use of derived credentials in accord with 800-63.
* Guidance and resources for alignment with 800-63.
* Developing criteria for accrediting 800-63 compliant products and services.
* GSA is responsible for:
* Developing, within 6 months, a roadmap for providing GSA solutions and shared services to meet the requirements of ICAM policy, NIST 800-63, and this OMB memo.
* Publishing, within 3 months, a catalog of ICAM solutions and shared services that agencies can leverage to meet the requirements of this memo.
* Identifying public or private sector capability for accrediting ICAM products using the NIST 800-63 criteria.

| **Gap Analysis** | **Recommendations** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Changes between the Final and Draft Versions

| **Responsible Party** | **New Requirement** | **Removed Requirement** |
| --- | --- | --- |
| Agency Level | Agencies are now required to share feedback on their implementation of the Digital Identity Risk Management process with the Federal Privacy Council, as well as with the Federal CIO Council and NIST. | Each agency shall develop a mechanism to streamline and automate agency-wide performance and accountability reporting. This mechanism should support existing and planned reporting and analytics structures and tools, such as the CDM dashboards and Federal Information Security Modernization Act of 2014 (FISMA 2014) reporting. |
| Agency Level | “Agencies shall leverage approved contract vehicles...to procure digital certificates for identification and authentication…” | The adjacent requirement was a “should” in the draft memo. |
| Agency Level | “Agencies shall use Federally provided or commercially provided shared services, to the extent available, to deliver identity assurance and authentication services to the public.” | The adjacent requirement was a “should” in the draft memo. |
| GSA | “Shall publish and maintain, within three months of the issuance of this policy, a consolidated catalog of existing ICAM solutions and shared services that agencies can leverage immediately to begin meeting the requirements of this memorandum.” |  |

* Additional item to note: In the draft version, OMB M-05-24 was rescinded. In the final version, M-05-24 is no longer rescinded.