United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

March 6, 2025

Memorandum

To: Bureau and Office Associate Chief Information Officers
Heads of the Contracting Activity

From: Megan Olsen
MEGAN OLSEN Digitally signed by MEGAN OLSEN Date: 2025.03.06 13:48:01 -05'00'
Director, Office of Acquisition and Property Management and
Senior Procurement Executive

Darren B. Ash
DARREN ASH Digitally signed by DARREN ASH Date: 2025.03.06 10:35:56 -05'00'
Chief Information Officer
Office of the Chief Information Officer

Subject: Acquisition of Information Technology Cloud Services

Purpose

This memorandum updates requirements to procure and manage cloud hosting services[1] in compliance with Office of Management and Budget (OMB) Memorandum, M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*[2] to reduce duplication of cybersecurity efforts while offering a consistent, reusable authorization framework. It also strengthens the U.S. Department of Interior's (Interior, Department) alignment with the Federal Information Technology Acquisition Reform Act of 2014 (FITARA)[3]. This policy rescinds and replaces Office of the Chief Information Officer (OCIO) Memorandum, *Acquisition of Information Technology Cloud Services/Mandatory Use of Pre-Approved Cloud Hosting Services and Contracts* policy, published August 7, 2018.

Background

Over the past several years, there has been an exponential growth in cloud acquisitions. Since 2023, Interior has spent more than $300 million adopting commercial cloud services. As a result of the growth and potential cyber security risks and pitfalls of incorporating new systems into an enterprise environment, Interior is strengthening its governance and review process. This approach aims to optimize information management and technology (IMT) resources, eliminate duplicative spending, drive modernization, and increase shared services across the Department.

Scope

This policy applies to acquisitions for all public cloud services as defined under NIST SP 800-

[1] Definition of cloud services as defined under National Institute of Standards and Technology (NIST) Special Publications (SP) 800-145, *The NIST Definition of Cloud Computing*
[2] M-24-15 Modernizing the Federal Risk and Authorization Management Program as of July 25, 2024
[3] Federal Information Technology Acquisition Reform Act (FITARA) as of December 2014

145. This includes all public cloud system investments that Interior directly manages or indirectly manages through partnerships, such as shared service applications managed by other federal agencies (i.e., Folio, USA Jobs, Xacta) and applies to cloud systems covered by both an Authority to Operate (ATO) and an Authority to Use.

This policy **does not apply** to cloud-based social media platforms, newspaper subscriptions, scientific and technical journal subscriptions, non-data hosting web tools, add-on and plug-ins, or ancillary applications that are addressed in the primary applications ATO.

OCIO Directive 2021-001, *Registration of Public Cloud Applications/Instances*[4], dated April 13, 2021, is still in effect.

Policy

In accordance with OMB M-24-15, the Department promotes the use of cloud computing products and services that meet FedRAMP security requirements and other risk-based performance requirements as determined by OMB, in consultation with the General Services Administration and the Cybersecurity and Infrastructure Security Agency. If another federal agency sponsors a cloud offering for FedRAMP, Interior will utilize that agency's approved authorization (presumption of adequacy). In other words, bureaus and offices shall not assume that a particular FedRAMP authorization path or sponsorship is unacceptable but shall leverage the other agency's security authorizations to the extent possible.

Bureaus and offices shall leverage the FedRAMP document repository for their Cloud service offerings and will adopt the use of emerging technologies offered by the FedRAMP Program Management Office when they become available. This includes adopting automated continuous monitoring processes and the utilization of associated documentation.

If a bureau or office elects to leverage a non-FedRAMP cloud solution to meet mission needs, they must gain the approval of the Associate Chief Information Officer (ACIO) and the Associate Chief Information Security Officer (ACISO). If the ACIO and ACISO would like to approve the non-FedRAMP cloud solution, they must gain concurrence from the Department Chief Information Officer (CIO) and Department Chief Information Security Officer (CISO). The CIO and CISO approval may be gained by providing Federal Information Security Modernization Act (FISMA) equivalent documented proof that all cybersecurity requirements normally inherited through the FedRAMP process are being managed by the bureau or office.

The following agency components, along with any future mandates, must be included in all cloud service contracts. Additional information about these Baseline and Service Level components as well as any future requirements can be found in the Cloud Reading Room.

- FedRAMP requirements
- Service level metrics and thresholds
- Penalties or remedies for cloud service providers not meeting service level metrics
- Zero trust best practices and principles
- Federal records management (i.e., e-Discovery, Freedom of Information)

[4] OCIO Directive 2021-001_*Registration of Public Cloud Applications*_04132021

- Data Loss Prevention implementation and techniques
- Privacy Act, System of Records, and Decommissioning requirements
- Personally Identifiable Information application
- Controlled Unclassified Information handling
- Secure Software Development Framework assurance
- Continuous visibility, monitoring, and incident handling practices

Effective Date

This policy is effective immediately upon signature.

Roles and Responsibilities

Departmental bureaus and offices shall:

1. Include all cloud acquisitions in the bureau or office forecast that meet the thresholds established within the Office of Small and Disadvantaged Business Utilization's Annual Forecast of Contracting Opportunities memorandum.
2. Ensure Bureau or Office ACIO approval for all cloud acquisitions.
3. Ensure cloud registrations and acquisitions are approved by the OCIO and that the cloud asset inventory reflecting the latest activities is complete.
4. Ensure the Department CIO, CISO and Deputy CIO - Program Management have visibility and input into High Value Assets and High Impact Service Provider acquisitions.
5. Compile and provide statements of work/objectives that include service level agreements that comply with FedRAMP and/or FISMA requirements.
6. Assign (or verify existing) personnel to cover system management roles: System Owner, Authorizing Official, Information System Security Officer, and Contracting Officer's Representative.
7. Complete all necessary Privacy Act requirements.
8. Ensure contract language clearly identifies mission based FISMA security categorization (low, moderate, high) according to the Federal Information Processing Standards 199[5].
9. For FedRAMP authorized cloud offerings, complete and obtain the FedRAMP Agency Package Access Request Form to maintain and manage customer responsible controls and perform continuous monitoring functions. Once the ATO is approved, upload a copy to the Department's Governance Risk, and Compliance tool and email a copy to cloud@doi.gov.

Contracting Officers shall:

1. Comply with all Federal Acquisition Regulation requirements.
2. Use mandatory or established enterprise contracts, when available, as they already include service level, privacy, data, and monitoring. Refer to Interior Acquisition, Arts, and Asset Policy Portal - Mandatory Use Memoranda and pre-existing and approved enterprise contracts[6] for more information.
3. Adhere to the DOI-AAAP-0060 Acquisition Program Advisory Council requirement for acquisition reviews for applicable acquisitions.

[5] Federal Information Processing Standards (FIPS 199)
[6] Enterprise and Mandatory use contracts - Cloud Program SharePoint site

4. Include applicable performance metrics and service level agreements from Interior's IT Baseline Compliance Contract Guidelines.
5. Ensure cyber security and privacy contract language includes continuous monitoring/visibility of service level metrics, including penalties/remedies for not meeting metric levels for confidentiality, integrity, and availability.

OCIO Program Management Division shall:

1. Manage the Cloud Program registration, cloud asset inventory and provide outreach materials to the cloud community of practice.
2. Ensure a copy of the bureau or office ATO is in the FedRAMP repository.

Questions

For the latest OCIO Cloud Program news and process updates, visit the Cloud Reading Room. Please direct questions regarding this policy to Cloud Program Manager at cloud@doi.gov.

Authorities and References

- OMB M-24-15 *Modernizing the Federal Risk and Authorization Management Program*
- OMB M-23-16 *Update to Memorandum M-22-18, Enhancing Security of the Software Supply Chain through Secure Software Development Practices* (SECURE Technology Act)
- OMB M-22-09 *Moving U.S. Government Toward Zero Trust Cybersecurity Principles* (EO 14028)
- Interior Information Management and Technology Strategic Plan FY24-29
- Interior Information Technology Baseline Compliance Contract Guidelines
- Interior Acquisition, Arts, and Asset Policy (DOI-AAAP)
- 40 U.S.C. §§ 11302–11319, *Responsibility for Acquisitions of Information Technology*
- 44 U.S.C. § 3506, *Federal Agency Responsibilities*
- OMB Circular A-130, *Managing Information as a Strategic Asset*
- Federal Information Technology Acquisition Reform Act (FITARA)

cc: Director, Office of Small and Disadvantaged Business Utilization
Chief Information Security Officer
Bureau and Office Associate Chief Information Security Officers
Bureau and Office Deputy Associate Chief Information Officers
Bureau and Office Cloud Points of Contact
Bureau and Office Capital Planners
Bureau Procurement Executives