U.S. DEPARTMENT OF ENERGY

# Department of Energy (DOE) Modernizing the FedRAMP Program Amplification Guidance

# Document Revision History

| Date | Version | Page(s) | Description | Author |
|---|---|---|---|---|
| 01/16/2025 | V1.0 | All | Initial Publication | OCIO, IM-32 |

## Overview

Congress enacted the Federal Risk and Authorization Management Program (FedRAMP) Authorization Act in December 2022 to establish the Federal Risk and Authorization Management Program (FedRAMP). The purpose of FedRAMP is to provide a standardized, reusable approach to security assessment and authorization for cloud computing products and services that process unclassified information used by Federal agencies. The Office of Management and Budget (OMB) Memorandum M-24-15[1], issued in July 2024, modernizes FedRAMP through significant process updates to streamline Federal cloud service adoption and enhance security measures.

M-24-15 requires Federal agencies to issue an agency-wide policy to promote 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 (GSA) and the Cybersecurity & Infrastructure Security Agency (CISA).

The DOE Chief Information Security Officer (CISO) is issuing this Amplification Guidance in accordance with the Department of Energy (DOE) Order (O) 205.1D, *DOE Cybersecurity Program*[2], to provide additional guidance on implementation requirements found in M-24-15. This Amplification Guidance, in conjunction with DOE O 205.1D, serves as DOE's policy to meet the agency-wide policy requirement in M-24-15. The DOE CISO will work with Departmental Elements (DEs), program offices, sites, and national laboratories to refine this guidance to assist with DOE's implementation of M-24-15. DOE OCIO will incorporate updated FedRAMP policy standards into DOE O 205.1.

## Purpose

The purpose of this document is to provide DOE's community of designated Authorizing Officials (AO) with guidance to support the assessment and approval process for operating a cloud service offering (CSO), including cloud computing products or services.

FedRAMP provides a standardized process for assessing and authorizing cloud computing services used by Federal agencies. GSA's FedRAMP Program Management Office (PMO) supports enhanced security of Federal CSO procured and used by Federal agencies by conducting FedRAMP PMO certified authorizations. M-24-15 introduces changes to make the FedRAMP certification program more accessible, efficient, to enhance FedRAMP's

[1] Modernizing the Federal Risk and Authorization Management Program
[2] Department of Energy (DOE) Order (O) 205.1D, DOE Cybersecurity Program

services to align with current cybersecurity needs, reflecting the growing importance of cloud technologies in Federal operations.

**DOE O 205.1D Requirements and DOE FedRAMP Agency Authorization Process**

DOE 205.1D outlines the Department's established requirements for FedRAMP's role in the assessment and authorization process:

- DEs should abide by the FedRAMP Authorization Act per H.R. 7776, National Defense Authorization Act for Fiscal Year 2023, and subsequent OMB guidance applicable to the Act, and the DOE FedRAMP Agency Authorization Process.
- No procurement for cloud products/services shall be completed without having obtained a valid authorization to operate (ATO) / authorization to use (ATU) granted by an designated AO in accordance with review of the FedRAMP authorization.

As part of its implementation of DOE O 205.1, DOE established a FedRAMP Agency Authorization Program under the DOE OCIO in 2020. This DOE OCIO-led program is responsible for developing processes and practices to support the Department's compliance with the FedRAMP Authorization Act. This program has established the following standards for cloud services at DOE:

- All cloud services used by DOE organizations are required to have a FedRAMP ATO.
- Any use of non-FedRAMP products is a variance from Departmental policy and must have a documented justification and approval for use by the designated AO. At a minimum, non-compliant cloud products must demonstrate their compliance with one of the FedRAMP security baselines in accordance with the FedRAMP Authorization Act.
- If a DOE organization needs to use a cloud service that is not yet authorized, it may request DOE sponsorship through the OCIO Cybersecurity Compliance and Oversight Office (IM-32).

The *DOE FedRAMP Agency Authorization Process Guide*[3] (DOE FedRAMP Process Guide) outlines the steps and requirements of DOE's FedRAMP authorization practices.

The DOE OCIO is working on updates to the DOE FedRAMP Process Guide in response to M-24-15 requirements and revised GSA resource guidance. The updated DOE FedRAMP Process Guide will be available to DOE offices by October 1, 2025.

[3] DOE-FedRAMP-Agency-Authorization-Process-Guide_v1.2_Signed

**New FedRAMP Requirements from M-24-15:**

M-24-15 introduced new requirements for agency use of FedRAMP products and services, including:

- Ensure authorization artifacts meet FedRAMP requirements and are of sufficient quality for reuse by other Federal agencies;
- Ensure authorization materials are provided to the FedRAMP PMO using machine-readable and interoperable formats
- Ensure that agency governance, risk, and compliance (GRC) tools and system inventory tools can produce, transmit, and ingest machine readable authorization artifacts using the Open Security Controls Assessment Language (OSCAL) or any succeeding formats as identified by FedRAMP;
- Ensure that relevant contracts include language incorporating the FedRAMP security authorization requirements established by GSA; and
- Regularly review continuous monitoring materials provided by cloud service providers (CSPs) and provide timely and actionable feedback as necessary to manage risk to the Government.

M-24-15 also requires agencies to report on relevant FedRAMP security metrics and on costs related to the issuance of FedRAMP authorizations. DOE OCIO will use the existing OCIO data call process to collect information from DEs in response to OMB reporting requests.

**Leveraging FedRAMP Authorizations for Reuse**

The FedRAMP Authorization Act requires agencies to leverage other agency security authorization materials within the FedRAMP repository to the greatest extent possible. The GSA FedRAMP PMO has developed the *FedRAMP Reusing Authorizations for Cloud Products Quick Guide*[4] to provide guidance to agencies in preparing materials for reuse by other agencies.

DOE OCIO and DEs are expected to leverage FedRAMP PMO-certified authorizations by:

- Confirming the existence of a FedRAMP authorization in the secure repository maintained and provided by the FedRAMP PMO.
- Access existing FedRAMP authorization materials through the submission of a FedRAMP package access request form to view the PMO's secure repository. ATO letters, annual assessment results, system change information, inventories, and

[4] FedRAMP Reusing Authorizations for Cloud Products Quick Guide

any relevant supplementary cloud system information are examples of documentation materials found in the secure FedRAMP repository which can be used to support locally-used ATOs to DE use approved FedRAMP systems.

- The DOE OCIO FedRAMP liaison approves and submits FedRAMP package access request forms for individuals based on roles and need to know. See the DOE FedRAMP Process Guide for detailed steps for requesting access to FedRAMP packages through the OMB Connect.gov platform.
- CSPs must ensure that their system security information and system authorization materials meet interoperability formats in accordance with applicable DOE guidance and guidelines.

**Presumption of Adequacy**

The FedRAMP Authorization Act states that the assessment of security controls and materials within the authorization package for a FedRAMP authorization shall be presumed adequate for use in an agency ATO for cloud computing products and services. M-24-15 directs agencies to presume that if a given cloud product or service has a FedRAMP authorization at a given Federal Information Processing Standard (FIPS) 199 impact level, agencies can presume the security assessment documented in the authorization package is adequate for their use in issuing an ATO at or below the FIPS 199 impact level

DOE OCIO established the following policy regarding security controls and materials for a FedRAMP approved CSO on DOE IT networks:

- For any CSO, including cloud computing products or services, that the DOE seeks to authorize that has received a FedRAMP authorization at a given FIPS 199 impact level, DOE will match the existing assessed of security controls and materials within the FedRAMP package for that CSO. DEs are encouraged to evaluate the need for additional security and privacy controls appropriate to the planned use of the CSO for DOE business.

**Developing Machine-Readable FedRAMP Documentation**

The Foundations of Evidence Based Policy Act of 2018 and other recent data-management legislation require Federal agencies to produce documentation in machine-readable and interoperable formats, in accordance with any applicable guidance from OMB. M-24-15 requires ATO documentation packages to be developed in machine-readable format to support reuse of ATO package materials by other Federal agencies. M-24-15 denotes OSCAL as OMB's preferred formatting standard for ATO documentation.

- The DOE Chief Data Officer, located in the DOE OCIO, is assessing available formatting standards for Departmental data products. Once these formatting standards are defined, DOE OCIO will direct CSPs to use these standards for submitted documentation.

**Maintaining an Inventory of Machine-Readable Documentation**

DOE O 205.1D requires DEs to maintain inventories of systems, including documentation of systems with approved ATO packages. In implementing the requirements of M-24-15, DEs must:

- Ensure that governance, risk, and compliance (GRC) tools and system inventory tools used to develop, share, and maintain ATO package documentation can produce, transmit, and ingest machine-readable authorization artifacts.

**FedRAMP Contract Language**

M-24-15 requires Federal agencies to ensure that relevant contracts include language incorporating the FedRAMP security authorization requirements.

- DOE OCIO is working with the Office of Management's Procurement Office to develop language for contracts. Additional information will be provided via appropriate channels once FedRAMP contract language has been approved for incorporation into DOE contracts.

**Continuous Monitoring**

The FedRAMP Authorization Act requires Federal agencies to continuously diagnose and mitigate against cyber threats and vulnerabilities associated with usage of CSOs. Additionally, agencies are required to regularly review continuous monitoring materials provided by CSPs.

**DOE's Continuous Monitoring (ConMon) Process**

The final phase of the DOE FedRAMP ATO process is Continuous Monitoring (ConMon). ConMon is an ongoing process enabling DOE designated AOs to ensure that the security posture of the CSO is maintained throughout the system's lifecycle.

DOE OCIO provides detailed guidance on the steps and activities of the DOE ConMon process in the DOE FedRAMP Guide. DOE O 205.1D and other DOE CISO guidance requires system authorization information and system monitoring information to be updated monthly to remain current with the latest system authorization information.

An important aspect of the DOE ConMon process is monitoring and oversight of authorized systems for identified non-compliant issues. The DOE FedRAMP Process Guide includes escalation steps for remediation of non-compliant systems, including:

- Identification: The DOE ConMon team identifies non-compliance and documents it.
- Notification: The DOE ConMon team promptly notifies the CSP of the identified non-compliance issue.
- CSP Response: CSP investigates and responds with proposed remediation actions.
- DOE Review: The DOE ConMon team analyzes the CSP's response.
- Escalation: The DOE ConMon team will escalate the issue with the CSP to the designated DOE authorizing official (AO).
- Significant Change Request (SCR), Deviation Request (DR), or Mitigation Plan: The DOE ConMon team will evaluate these options if non-compliance persists or is unable to be resolved due to justifiable reasons.
- Reporting and Escalation to FedRAMP PMO: If the CSP fails to provide a plan acceptable to the DOE ConMon team or fails to meet the dates identified in the plan, the DOE ConMon team will escalate the issue to the FedRAMP PMO for further action. Failure to resolve non-compliance issues may result in the FedRAMP PMO re-assessing the FedRAMP authorization of the cloud product.
- Remediation: DOE monitors the CSP's remediation progress and rescinds the FedRAMP ATO if necessary.

**Outreach and Information Sharing in DOE's ConMon Process**

The DOE OCIO ConMon team holds regular ConMon meetings with CSPs, Third Party Assessment Organizations (3PAOs), DE system owners, and DE Information System Security Officers (ISSOs) to oversee security control assessments, advise and respond to questions, identify cyber threats and risks, and to provide status updates SCRs and DRs submitted to the FedRAMP PMO.

In addition, DOE utilizes the USDA Connect dashboard to evaluate and share CSP vulnerabilities as part of the ConMon process.

**Questions**

The DOE OCIO FedRAMP Agency Authorization program and ConMon team can be reached by emailing doefedramp@hq.doe.gov.

## Additional Resources

**GSA FedRAMP PMO Resources:**

- FedRAMP Agency Authorization Playbook: FedRAMP Agency Authorization Playbook
- CSP Authorization Playbook: CSP Authorization Playbook
- FedRAMP laws, regulations, standards, and guidance reference guide: FedRAMP-Laws-Regulations-Standards-and-Guidance-Reference.xlsx
- Reusing Authorizations for Cloud Products Quick Guide: Reusing_Authorizations_for_Cloud_Products_Quick_Guide.pdf
- FedRAMP Continuous Monitoring Performance Management Guide: FedRAMP Continuous Monitoring Performance Management Guide

**DOE FedRAMP Guidance:**

- DOE O 205.1D, DOE Cybersecurity Program: Department of Energy Cybersecurity Program
- DOE FedRAMP Agency Authorization Process Guide: DOE-FedRAMP-Agency-Authorization-Process-Guide_v1.2_Signed