



Federal Risk and Authorization Management Program (FedRAMP)

Overview

Background on FedRAMP

Guiding Frameworks

National Institute of Standards and Technology (NIST) has developed key frameworks for comprehensive guidelines for cybersecurity:

- NIST 800-171 Non-Federal Networks
- NIST 800-53 Federal Organization

FedRAMP Authorization Act

Signed as part of the FY23 National Defense Authorization Act (NDAA)

- The Act codifies the FedRAMP program as the authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information

Key Take Aways from Act

- Federal agencies are **required by law** to protect federal data stored in the cloud.
- Federal agencies do this by authorizing cloud services that demonstrate compliance with one of the FedRAMP security baselines (Low, Med, High)

FedRAMP Policy Memo

- States that “each Executive department or agency shall use FedRAMP when conducting risk assessments, security authorizations, and granting ATOs [Authority to Operate] for all federal executive department or agency use of cloud services.”

Cloud Authorization Process

- **Two approaches**

- A provisional authorization (PA) through the Joint Authorization Board (JAB)
- Authorization through an agency (e.g. HPCMP)

How to get to a PA?

There are multiple paths to a DoD Provisional Authorization (DoD). A DoD component can sponsor a Cloud Service Provider (CSP) for a DoD Provisional Authorization

Who can help navigate?

Cloud Assessment Division, as the DoD Cloud Authorization Services (DCAS) team

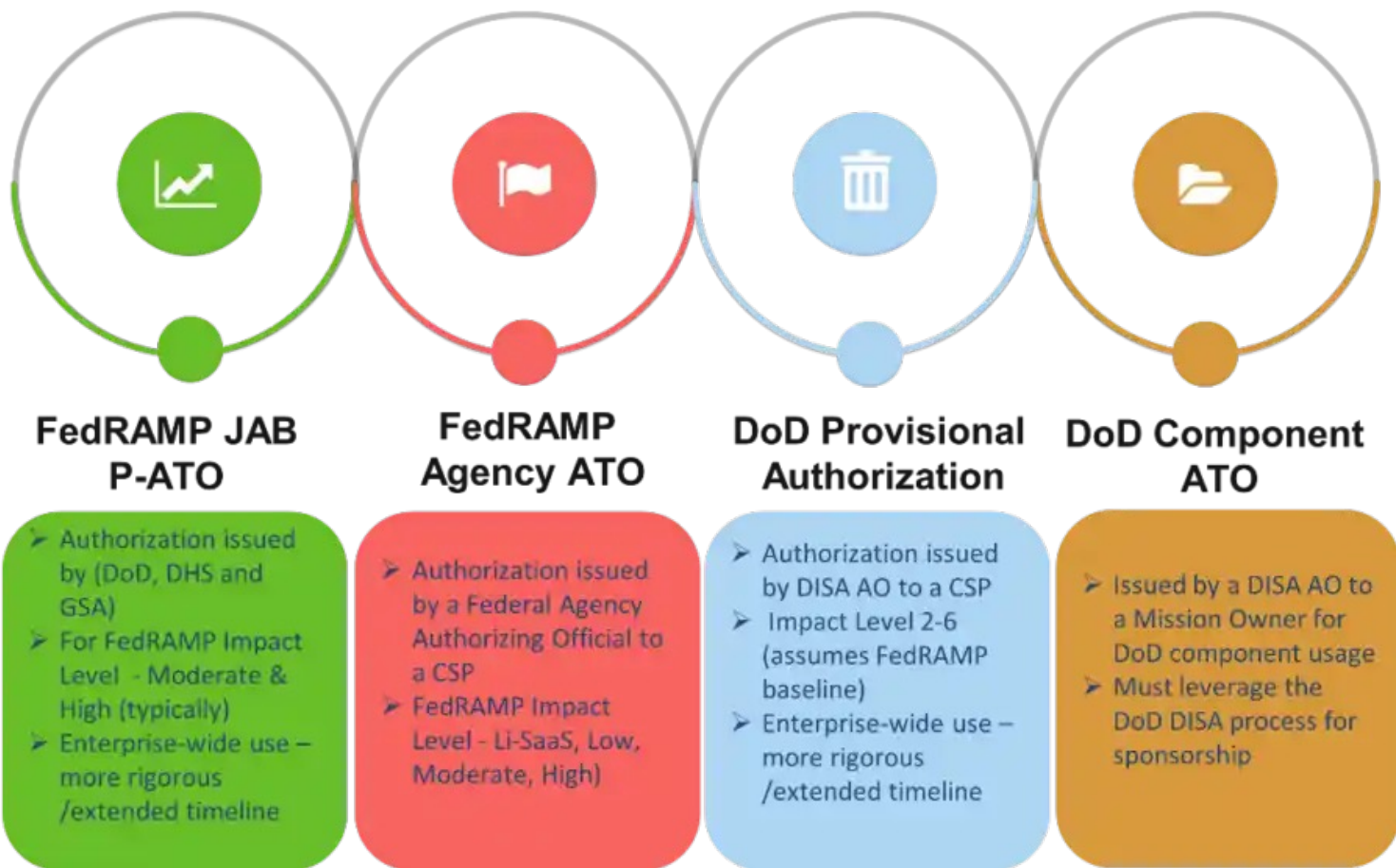
What does the DCAS team do?

Provides support to DoD components through the pre-screening, assessment, validation, and management of the initial authorization process for Cloud Service Offerings (CSO)

Where to find the information?

Sponsors and CSPs should also be familiar with the cloud authorization process; a summary presentation is available for download from the document library (cyber.mil)

DoD Cloud Authorization Terminology



Roadmap to DoD PA

Impact Level	Non-DOD FedRAMP Agency ATO (FedRAMP Moderate/High)	DoD Component Assessed PA
IL 2	<p>DoD does not require any additional assessment review.</p> <ul style="list-style-type: none"> A FedRAMP reciprocity memo has been issued by the DOD for FedRAMP Moderate and High Impact baselines) 	<p>Without a FedRAMP JAB P-ATO or FedRAMP Agency ATO, DoD Component assessment may only be performed under two circumstances:</p> <ol style="list-style-type: none"> If the DoD organization has a validated mission requirement that only specific CSP's cloud offering can fulfill the DoD charter, or If the DOD organization is acting as a CSP develops and offers the cloud service offering. <p>The CSP's CSO is fully assessed by a FedRAMP-approved 3PAO and the DISA Cloud SCA.</p> <ul style="list-style-type: none"> The CSP's CSO must be assessed and validated against both the FedRAMP Moderate/High Baseline and DoD's FedRAMP+ requirements. The DoD organization with a need for that CSP's CSO to be authorized will be required to support resourcing for the full assessment, in coordination with the DISA cloud security assessment team.
IL 4/5	<p>DoD leverages the FedRAMP JAB /Agency ATO package and adds additional DoD specific controls not addressed by FedRAMP.</p> <ul style="list-style-type: none"> The acceptable minimum baseline is FedRAMP Moderate. FedRAMP High baseline systems will be accepted as the basis of an IL4 PA without an additional assessment of additional FedRAMP+ controls and control enhancements (C/CE); however, assessment of non C/CE based requirements in the SRG is needed. 	
	<p>Audit must be performed by a FedRAMP 3PAO</p> <ul style="list-style-type: none"> The CSP/3PAO submit documentation (SSP/SAP/SAR/POAM, etc.) to the DISA SCA-R for review and validation by the Joint Validation Team (JVT) toward awarding a DoD PA. 	

*DISA Authorizing Official (AO) is the AO for all DoD PA's

Terms

● FedRAMP Marketplace

- A searchable, sortable database of cloud service offerings (CSOs) that have achieved a FedRAMP designation. Marketplace as a resource to:
 - Research CSOs that are FedRAMP Authorized, FedRAMP Ready, or FedRAMP In Process
 - Research federal agencies that use FedRAMP Authorized CSOs
 - Research FedRAMP recognized 3PAOs

● FedRAMP Designations

- FedRAMP Ready: A designation provided to CSOs which indicates that a 3PAO attests to a CSO's security capabilities, and that a FedRAMP Readiness Assessment Report (RAR) has been reviewed and deemed acceptable by the FedRAMP PMO. FedRAMP Ready indicates a CSO has a high likelihood of successfully completing an initial FedRAMP authorization with the Joint Authorization Board (JAB) or a federal agency. FedRAMP
- In Process: A designation provided to CSOs that are actively working toward a FedRAMP authorization with either the JAB or a federal agency. For updates, agencies can either contact the cloud provider via the email address provided on the CSO's FedRAMP Marketplace page, or reach out directly to the FedRAMP PMO via intake@fedramp.gov.
- FedRAMP Authorized: A designation provided to CSOs that have successfully completed the FedRAMP authorization process with the JAB or a federal agency. FedRAMP Authorized CSOs are available for government-wide reuse.

Overall Authorization Process with Agency

The Authorization Process

01 Preparation

Readiness Assessment

(Optional, but highly recommended)

- RAR Development
- FedRAMP PMO Review of RAR
- Remediation (if needed)
- ✓ FedRAMP Marketplace Designation – Ready



Pre-Authorization

- Partnership Establishment
- Authorization Planning
- Kickoff Meeting
- ✓ FedRAMP Marketplace Designation – In Process

02 Authorization

Full Security Assessment

- Security Authorization Package (SSP, SAP, SAR, POA&M)*



Agency Authorization Process

- Agency Review of Security Authorization Package
- SAR Debrief
- Remediation
- Agency Final Review
- Agency Issues ATO
- FedRAMP PMO Review
- Remediation (if needed)
- ✓ FedRAMP Marketplace Designation - Authorized

03 Continuous Monitoring

Post Authorization

- Ongoing Continuous Monitoring Deliverables
- Annual Assessment


* The full security assessment may be prepared in advance of the authorization phase, or completed during the authorization phase. This is dependent on the agency's review approach.

Provisional Authorization (PA) JAB Process

JAB Authorization Process



01 Preparation

FedRAMP Connect

-  FedRAMP Connect Business Case
- Prioritized to work with JAB




Readiness Assessment *(required)*

-  RAR Development
- FedRAMP PMO Review of RAR
- Remediation (if needed)
-  FedRAMP Marketplace Designation - Ready



Full Security Assessment

-  Security Authorization Package (SSP, SAP, SAR, POA&M)

02 Authorization

JAB Authorization Process

- Kickoff (~1 week)
-  FedRAMP Marketplace Designation - In Process
- Review (~3-4 weeks)
- Remediation (~3 weeks)
- Final Review (~4 weeks)
- JAB P-ATO Issued
-  FedRAMP Marketplace Designation - Authorized

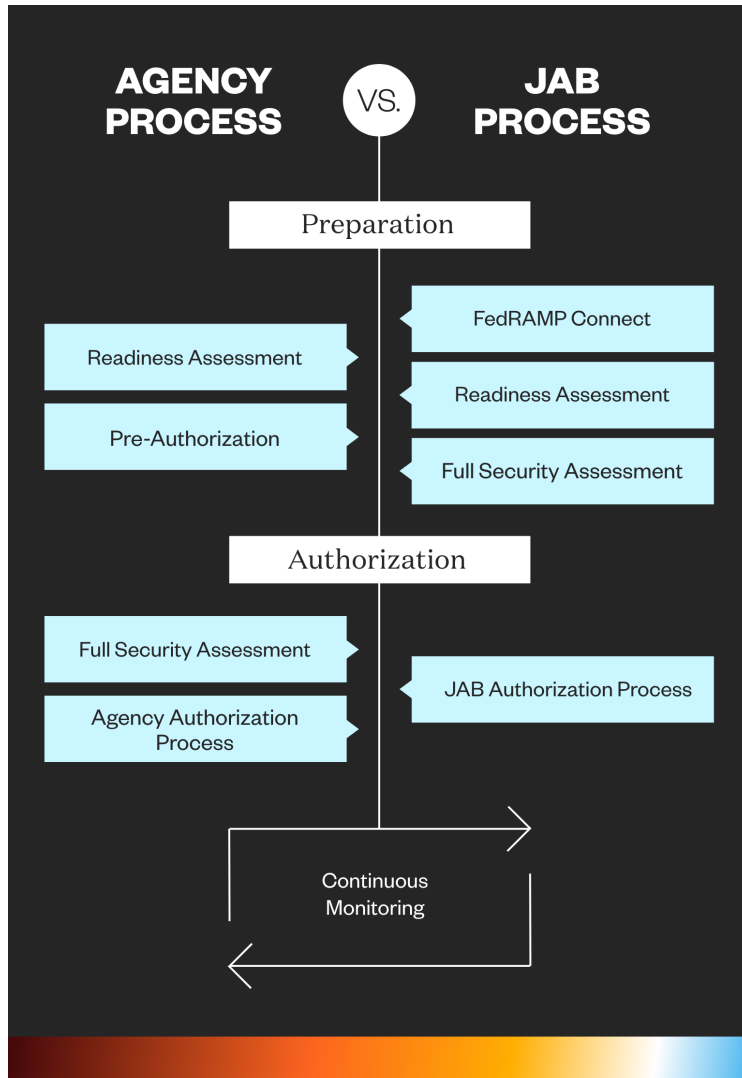
03 Continuous Monitoring

Post Authorization

-  Ongoing Continuous Monitoring Deliverables
-  Annual Assessment

Note: During the authorization process a CSP must be prioritized by the JAB before entering the JAB P-ATO process. The CSP can obtain FedRAMP Ready status either before or after the JAB's prioritization.

Process Difference



FedRAMP Connect

Process by which Cloud Service Providers (CSPs) are evaluated based on the JAB Prioritization Criteria and prioritized to work with the JAB.

- Currently 12 CSO's per year
- Prioritization criteria consist of **three categories**: Demand, FedRAMP Ready, and Preferred Characteristics

Readiness Assessment (FedRAMP Ready):

- A 3PAO attests to the readiness of a CSP's cloud offering
- FedRAMP PMO then reviews and approves based on RAR

Full Security Assessment:

- SSP, SAP, SAR, POA&M, and one month of continuous monitoring deliverables must be completed using FedRAMP-provided templates and should be submitted together

Authorization:

- JAB P-ATO signifies that all three JAB Agencies reviewed the security package and deemed it acceptable for the federal community.

ConMon:

- While each agency's Authorizing Official (AO) maintains the final approval authority for the use of a system by that agency, the **JAB acts as a focal point** for continuous monitoring activities of systems with a P-ATO.