FedRAMP

Federal Risk and Authorization Management Program

Brian Conrad, Acting Director

August 29, 2023

GSA

info@fedramp.gov

fedramp.gov

FedRAMP Mission and Vision

Mission

The Federal Risk and Authorization Management Program (FedRAMP) **promotes the adoption of secure cloud** services across the US Government by providing a **standardized approach to security and risk assessment**.

Vision

Accelerating the expansion of a marketplace of **secure cloud services** for the Federal Government

FedRAMP Yields Efficiencies For Agencies

Federal Security policy requires all systems to be authorized based on risk.

FedRAMP standardizes the process for cloud, providing:

DO ONCE, USE MANY TIMES

Doing security authorizations right the first time allows agencies to re-use work and eliminate duplicative efforts

TRANSPARENCY

Increased collaboration and creation of a community among the US Government and vendors that did not exist before, establishing the first government-wide FISMA program

VALIDATED WORK

FedRAMP validates security authorizations to ensure that there is uniformity among security packages

CENTRAL SHARING

Centralized repository where agencies can request access to security packages for expedient authorizations

Legal and Policy Framework

FISMA

Federal Information Security Modernization Act requires agencies to protect Federal Information. FISMA requires NIST to develop standards and guidelines

OMB A-130

OMB states that when agencies implement FISMA, they must use NIST standards and guidelines

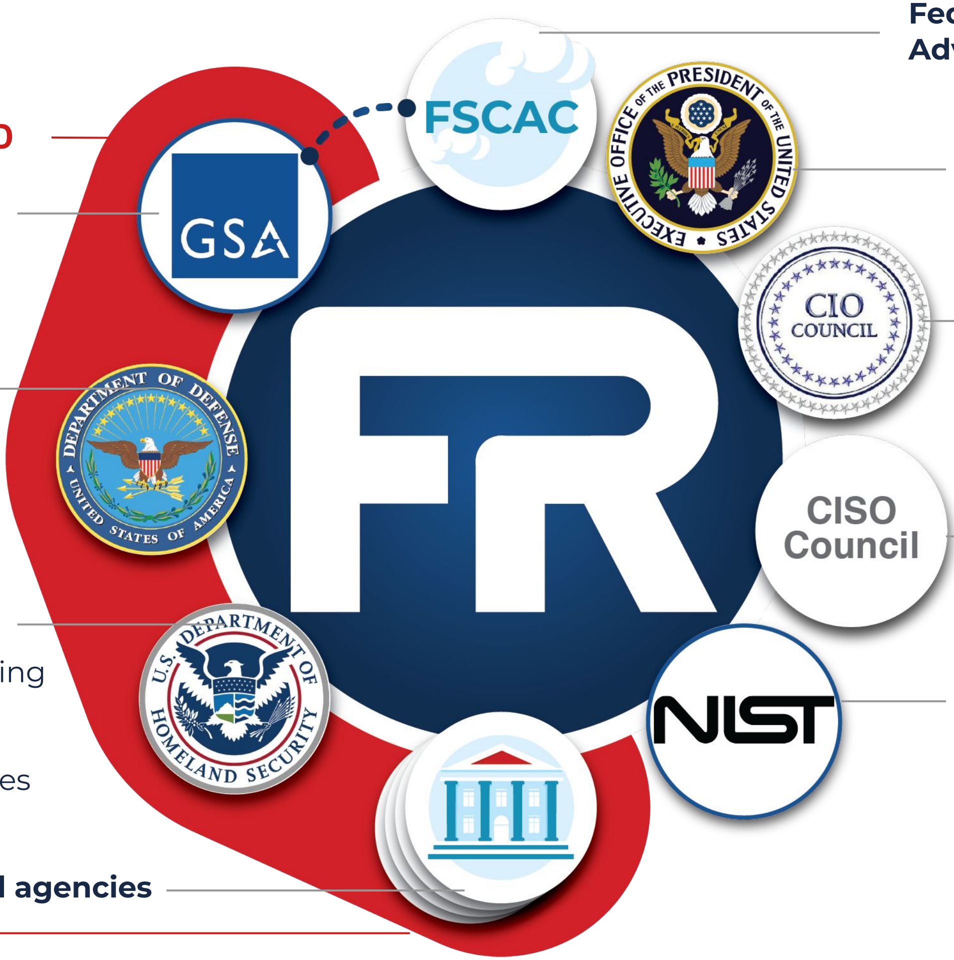
FedRAMP Policy

FedRAMP leverages NIST standards and guidelines to provide standardized security requirements for cloud services; a conformity assessment program; standardized authorization packages and contract language; a repository for authorization packages

FedRAMP Authorization Act

FedRAMP Authorization Act establishes a Government-wide program that provides a standardized, reusable approach to security assessment and authorization for cloud computing products and services that process unclassified information used by agencies.

New FedRAMP Governance Model



FedRAMP BOARD

FedRAMP PMO

Department of Defense

Department of Homeland Security
- US-CERT Incident Coordination
- Continuous Monitoring Data Analysis
- Issuance of Binding Operational Directives

Up to 4 additional agencies

Federal Secure Cloud Advisory Committee

Office of Management and Budget

CIO Council
- Cross Agency Coordination

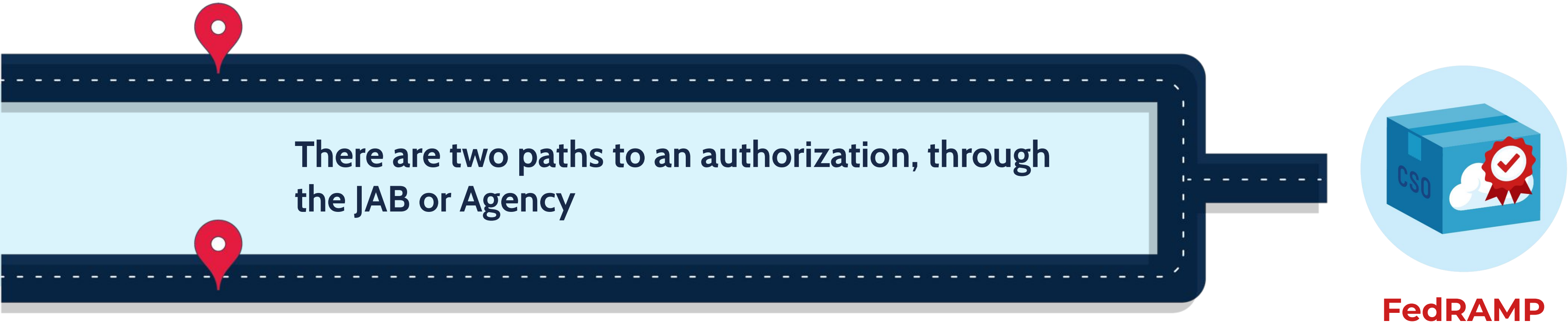
CISO Council

National Institute of Standards and Technology
- FISMA Standards
- Technical Advisors
- Technical Specifications

FedRAMP Paths to Authorization

Joint Authorization Board Provisional Authority to Operate (P-ATO)

- The primary governance and decision making body for the FedRAMP program
- CIOs of DoD, DHS, and GSA strictly review CSP packages for an acceptable risk posture using a standard baseline approach
- The JAB issues provisional authorizations (P-ATO); this is not a risk acceptance, but an assurance to Agencies that the risk posture of the system has been reviewed by DoD, DHS, and GSA, and approved. Each Agency must review and issue their own ATO that covers their Agency's use of the cloud service.



There are two paths to an authorization, through the JAB or Agency

FedRAMP Authorized

Agency Authority to Operate (ATO)

- *Agency Initial ATO:* Initial Agency reviews CSP FedRAMP security package; Agency/CSP submits the security package and Agency ATO to the FedRAMP PMO. FedRAMP confirms package meets FedRAMP requirements and makes security package available for Agencies to reuse.
- *Agency Leveraged ATO:* Agency reviews JAB or Initial Agency FedRAMP ATO security packages and issues Agency ATO. Agency sends a copy of ATO letter to FedRAMP PMO for record keeping.

FedRAMP Stakeholders

221
Federal Agencies

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

DEPARTMENT OF VETERANS AFFAIRS · UNITED STATES OF AMERICA

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

SMALL BUSINESS ADMINISTRATION 1953

DEPARTMENT OF COMMERCE · UNITED STATES OF AMERICA

DEPARTMENT OF TRANSPORTATION · UNITED STATES OF AMERICA

UNITED STATES DEPARTMENT OF AGRICULTURE

U.S.ARMY

300+
Cloud Service Providers (CSPs)

* Including 61 small businesses

Google

amazon

DocuSign®

ORACLE®

Adobe

IBM

salesforce

Microsoft

40
Third Party Assessment Organizations (3PAOs)

COALFIRE

SECURE IT

Booz | Allen | Hamilton
100 YEARS

schellman
formerly BrightLine

lunarline
Solutions Built on Security™

KRATOS
SECUREINFO®

FedRAMP PMO Worklanes

PMO Operations

- Develops customized baselines for Cloud Services
- Measures FedRAMP's performance through metrics collection/analysis
- Develops and enhances documentation and templates
- Executes the PMO's Incident Response Plan and ensures all incidents are resolved promptly
- Oversees and manages website

Agency Engagement

- Develops guidance for agency authorization process
- Reviews agency authorization packages and provides risk assessment
- Guides and supports agencies through the FedRAMP process including ongoing communication, Kick-off meetings, and agency/CSP partnership development

3PAO Performance

- Oversees 3PAO Program and vendors
- Develops 3PAO Requirements
- Partners with accrediting body

JAB Authorizations

- Facilitates JAB authorization of cloud service providers
- Sets guidance and procedures
- Manages repository and tracking of authorizations
- Manages governance process
- Ensures vendors holding JAB P-ATOs maintain their authorizations through Continuous Monitoring

Priority Projects

- * Threat-based authorizations
- * Digitizing FedRAMP security packages using Open Security Control Automation Language (OSCAL) to automate the authorization process
- Agency Liaison Program

Training & Outreach

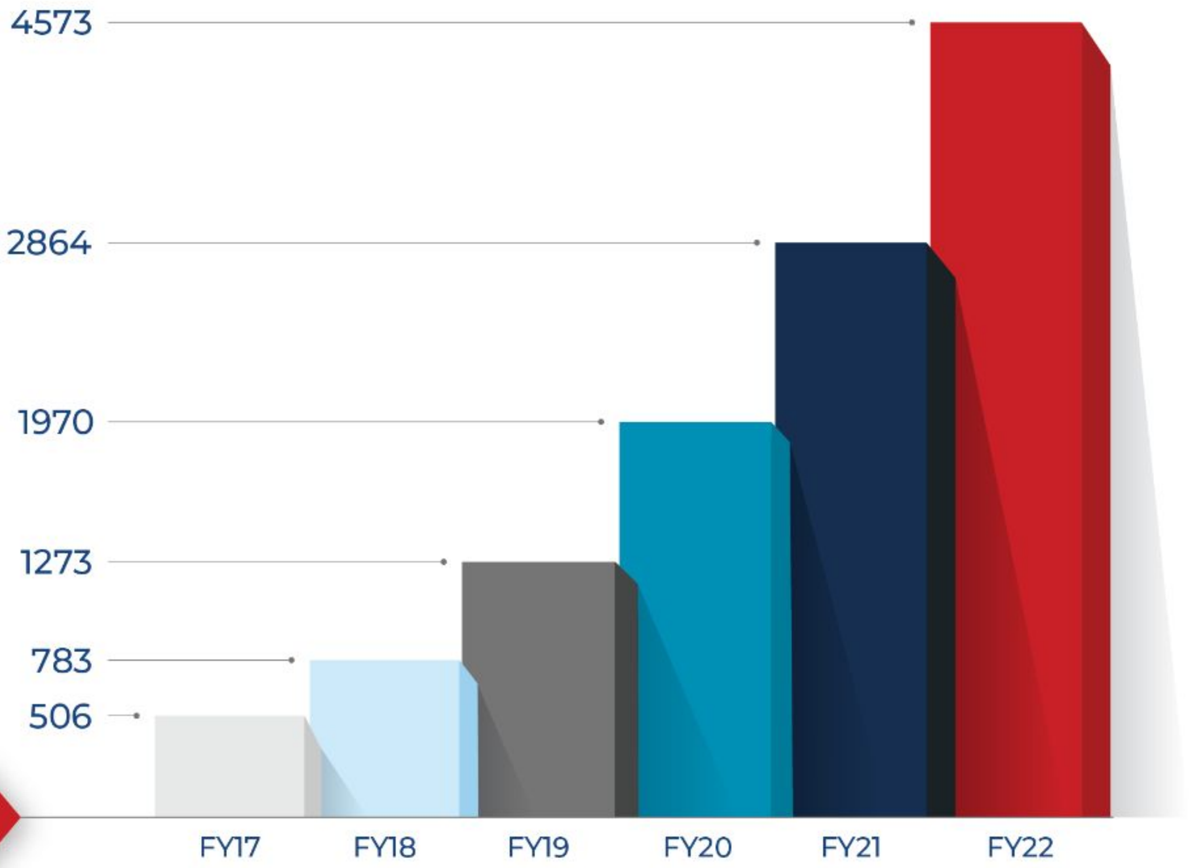
- Oversees all FedRAMP training, including required 3PAO training, ISSO trainings, and other training offered by the PMO
- Develops and implements a training strategy to establish a cohesive training approach
- Creates and delivers customized agency training
- Creates and reviews blogs and monthly Newsletters
- Manages stakeholder feedback through Annual Survey

***Threat-based authorization approach and future OSCAL phases are/will primarily funded through external funding sources.**

Program Growth

Marketplace Growth over the Years:

From FY20 to FY22, FedRAMP has seen an **increase in reuse of 132%** as demand rises.



Reuse

Q&A

Major FY23 Changes

Operationalizing Legislation

- Facilitate the ease of reuse and increase volume of ATOs
- Establish FACA Advisory Board
- Plan for changes to the Joint Authorization Board
- Work with OMB to update FedRAMP memo

Increase in Funding

- Allow PMO to grow to address increased demand and modernization efforts

Rev 5 Transition

- Modernize baselines

Modernize baselines External/ 3rd Party Services

(Authorization Boundary Guidance)

- Enable a risk management approach for protecting federal data

FedRAMP Long Term Goals

GOALS

1

Grow the FedRAMP Marketplace:

Continue to partner with government and industry to promote the adoption of secure cloud services across the federal government

2

Transform Processes:

Incorporate automation and process improvements to improve the efficiency and stakeholder experience of the end-to-end FedRAMP process with the ability to accommodate future growth

3

Promote Knowledge Sharing:

Provide more opportunities for dialogue and feedback by hosting additional events for collaboration, feedback, training and exchange of ideas and practices

Thank You

Learn more at **fedramp.gov**

🐦 **@FEDRAMP**