FedRAMP

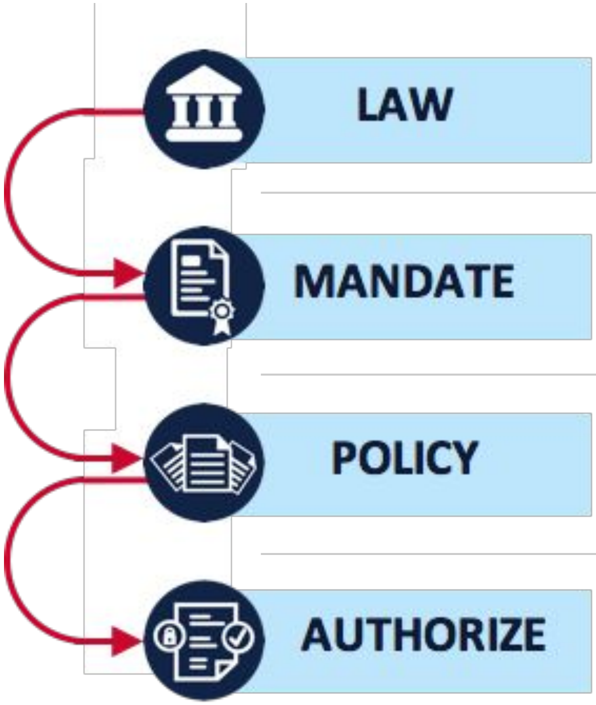
FedRAMP Overview

Brian Conrad, FedRAMP Program Manager for Cybersecurity
Military Librarians Training Workshop
December 10, 2019

FedRAMP 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.

Legal Policy and Framework for Securing Federal Information Systems



FISMA: Federal Information Security Management Act REQUIRES agencies to do cybersecurity

WHITE HOUSE: OMB states that when Agencies implement FISMA, they must use the NIST framework (Circular A-130)

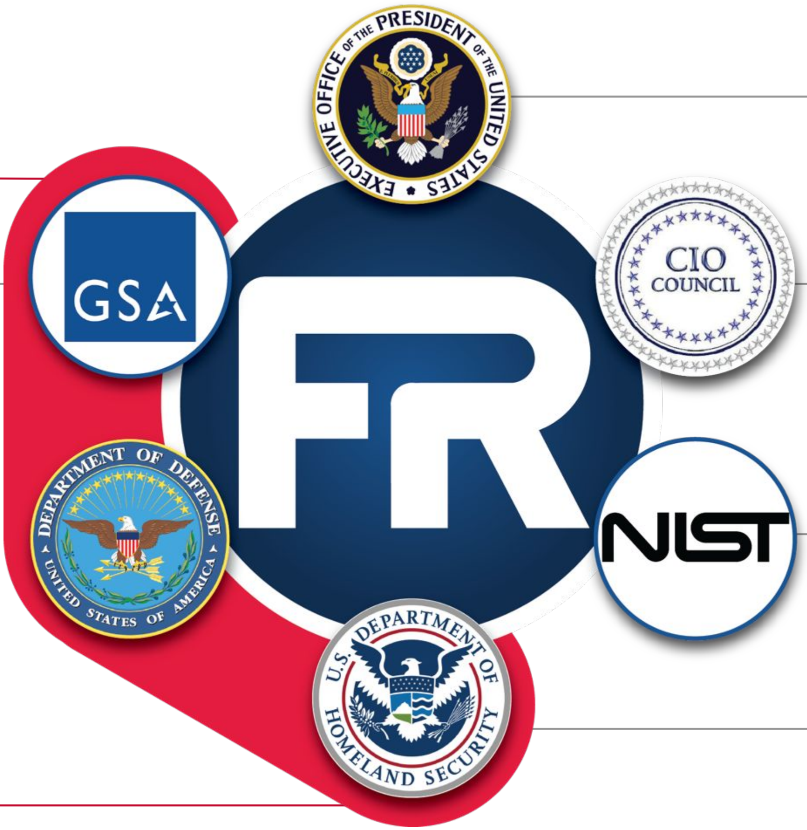
FEDRAMP: FedRAMP says when using cloud, agencies must implement NIST via FedRAMP requirements

AGENCY: Each Agency ultimate must individually authorize a system for use

Federal law requires that Agencies authorize their information systems.

FedRAMP is FISMA for cloud services and is required for all Executive Agencies.

FedRAMP Governance



Office of Management and Budget

FedRAMP PMO

- ISIMC Guidance
- Cross Agency Coordination

JOINT AUTHORIZATION BOARD

- FISMA Standards
- Technical Advisors
- Technical Specifications

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

FedRAMP Landscape

FedRAMP Authorized CSPs cover more than

5 MILLION assets available for Federal use

&

1/3 of the world's internet traffic

4 security baselines to match government use to risk

HIGH *(421 controls)*	LOW *(125 controls)*
MODERATE *(325 controls)*	TAILORED *(36 controls*)*

165 Authorized Cloud Services

1300+ Agency Reuses of Authorized Services

159 Participating Government Organizations

220+ Participating Industry Partners

POINTS OF CONNECTION

750+ Annual meetings with agencies and vendors

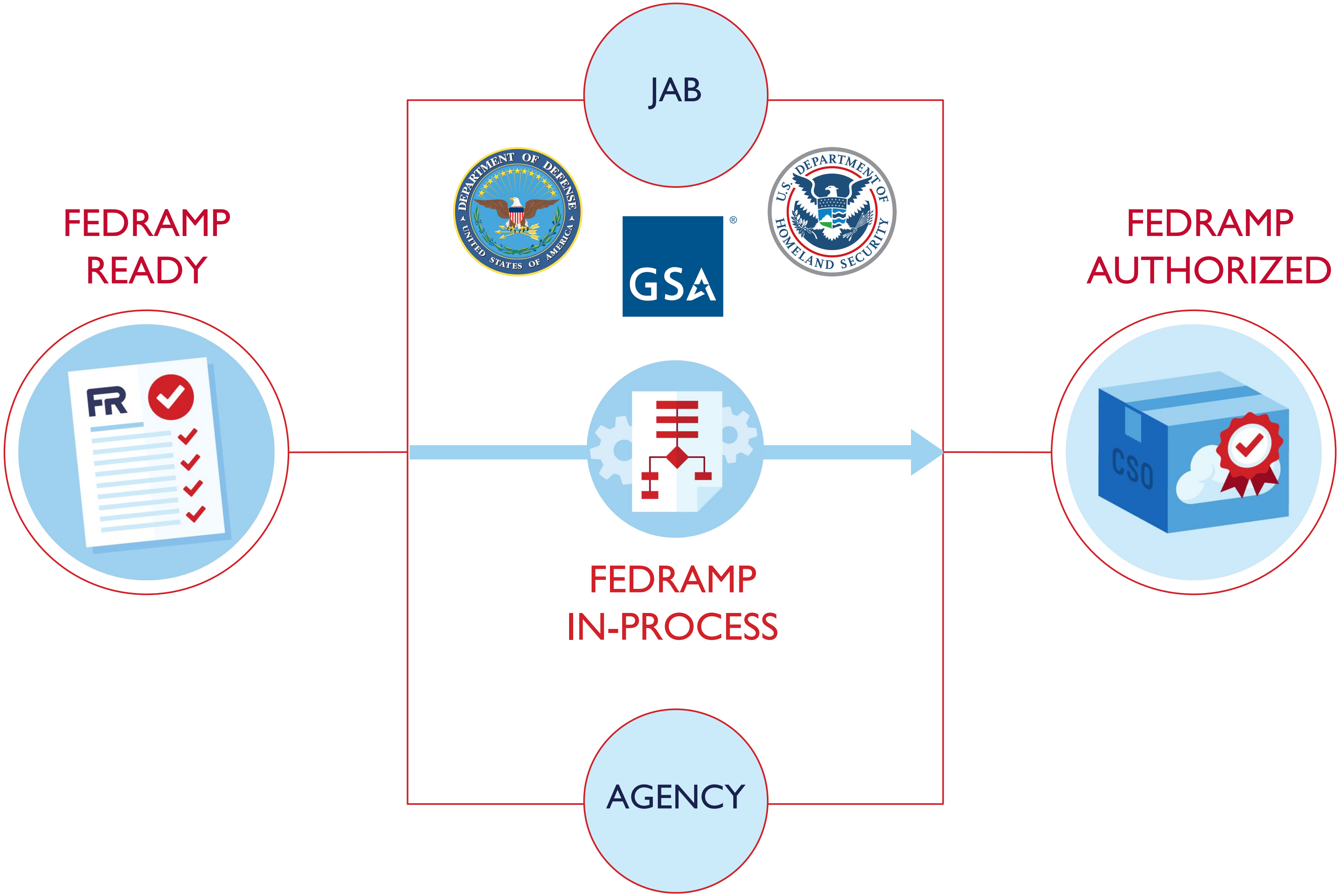
4,200+ Followers on Twitter

11,000+ Stakeholders on listserv

20,000+ Questions answered through info@fedramp.gov

**testable*

FedRAMP Designations



FEDRAMP READY

JAB

FEDRAMP IN-PROCESS

AGENCY

FEDRAMP AUTHORIZED

FedRAMP Baselines

FedRAMP provides 4 baselines for authorizing cloud services according to the security impact for the use of the service at Agencies

Tailored for LI-SaaS

- Specific to SaaS with low-risk use cases architected on FedRAMP-authorized infrastructure clouds
- Consolidated security documentation
- Enables agencies to *tailor* Low baseline to core, critical controls, commensurate with risk

Low

- 125 controls
- Limited adverse effect on Agency operations in the event of system breach
- Services do not store PII beyond that required for user login capability

Moderate

- 325 Controls
- 80% of federal use cases for cloud services
- Breach would result in serious adverse effects on Agency operations

High

- 421 controls
- Severe or catastrophic adverse effects on Agency operations in the event of system breach
- Common use cases include financial systems, health systems, and law enforcement or emergency services systems

Breaking Down the Baseline: What Does this Mean?

FedRAMP baselines are organized according to **17 control families defined by NIST**

NIST Control Families

- AC - Access Control
- AU - Audit & Accountability
- AT - Awareness & Training
- CM - Configuration Management
- CP - Contingency Planning
- IA - Identification & Authentication
- IR - Incident Response
- MA - Maintenance
- MP - Media Protection
- PS - Personnel Security
- PE - Physical & Environment Protection
- PL - Planning
- RA - Risk Assessment
- CA - Security Assessment & Authorization
- SC - System & Communications Protection
- SI - System & Information Integrity
- SA - System & Services Acquisition

EXAMPLE CONTROL AREAS

Encryption

SC-13 SC-8 SC-28

Helps ensure that only authorized parties can understand/decode the information.

Identification & Authentication

IA-2

Reduces the likelihood of account compromise and helps ensure that only the people who should have access to information do.

Vulnerability Scanning & Malicious Code

RA-5 SI-2

Helps ensure vendors have what they need in place to continually respond to evolving threats.

Boundary Protection & System Interconnections

CA-3 SC-7 AC-4

Ensures federal data is protected from end to end and maintains a secure perimeter.

Configuration Management

CM-6 SI-2

Provides visibility into what is changing and the impact of those changes.

FedRAMP Yields Efficiencies

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

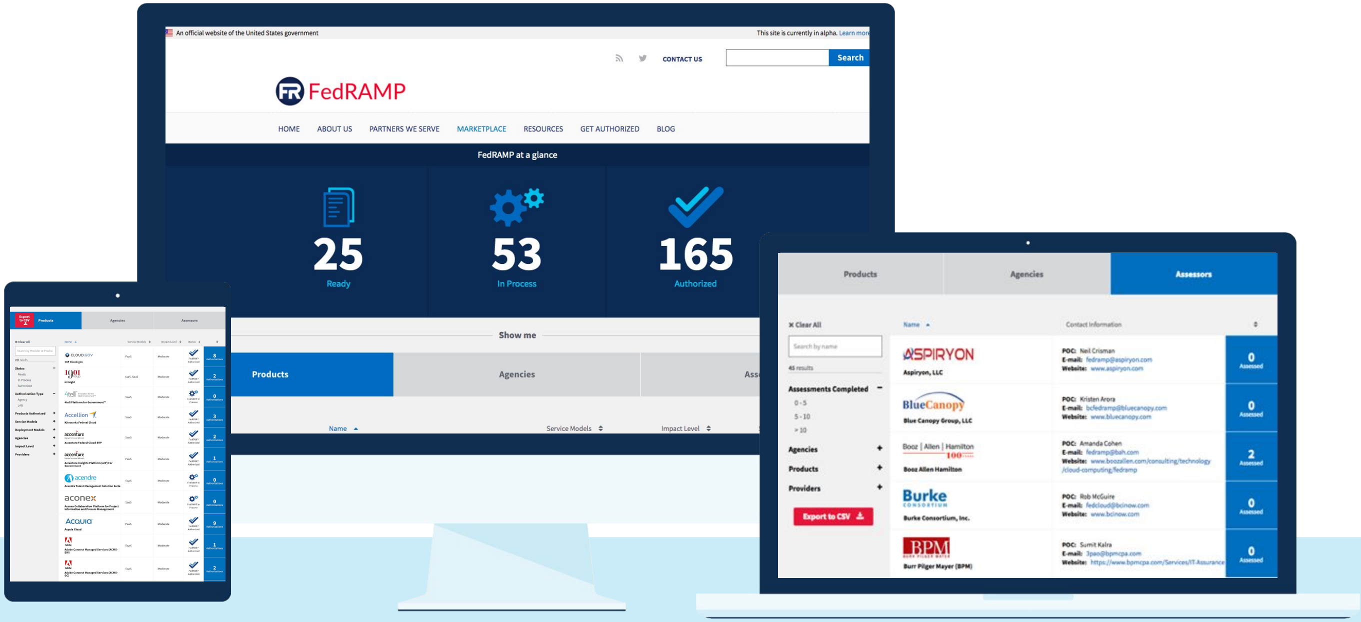
VALIDATED WORK

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

FedRAMP Marketplace



An official website of the United States government

This site is currently in alpha. Learn more

CONTACT US

Search

FedRAMP

HOME ABOUT US PARTNERS WE SERVE MARKETPLACE RESOURCES GET AUTHORIZED BLOG

FedRAMP at a glance

25 Ready

53 In Process

165 Authorized

Show me

Products | Agencies | Ass

Name ▲ | Service Models ⇕ | Impact Level ⇕

Products | Agencies | Assessors

✕ Clear All

Search by name

45 results

Assessments Completed −

0 - 5

5 - 10

> 10

Agencies +

Products +

Providers +

Export to CSV

Name ▲	Contact Information	⇕
ASPIRYON Aspiryon, LLC	POC: Neil Crisman E-mail: fedramp@aspiryon.com Website: www.aspiryon.com	0 Assessed
BlueCanopy Blue Canopy Group, LLC	POC: Kristen Arora E-mail: bcfedramp@bluecanopy.com Website: www.bluecanopy.com	0 Assessed
Booz | Allen | Hamilton 100 Booz Allen Hamilton	POC: Amanda Cohen E-mail: fedramp@bah.com Website: www.boozallen.com/consulting/technology/cloud-computing/fedramp	2 Assessed
Burke CONSORTIUM Burke Consortium, Inc.	POC: Rob McGuire E-mail: fedcloud@bcinow.com Website: www.bcinow.com	0 Assessed
BPM Burr Pilger Mayer (BPM)	POC: Sumit Kalra E-mail: 3pao@bpmcpa.com Website: https://www.bpmcpa.com/Services/IT-Assurance	0 Assessed

- Provides a searchable database of all cloud services with a FedRAMP designation
- Enables researching of Authorized services and Third Party Assessment Organizations (3PAOs)
- Provides contact information and service descriptions for all cloud services

Questions?

Learn more at www.Fedramp.gov

Contact us at info@fedramp.gov

@FEDRAMP