COALFIRE RAMPCON

06.09 — 06.10.2025 • WASHINGTON D.C.

Unified but Evolving:
The Shifting Terrain of FedRAMP, GovRAMP, and DoD CC SRG

ERIC KRAFT | DIRECTOR – PUBLIC SECTOR ADVISORY/ COALFIRE

MAX POST | DIRECTOR – PUBLIC SECTOR ADVISORY/ COALFIRE

JUSTIN RICHARDSON | DIRECTOR – PUBLIC SECTOR ADVISORY/ COALFIRE

Introduction to FedRAMP



What is FedRAMP?

Founded in 2011, the Federal Risk and Authorization Management Program (FedRAMP®) provides a standardized approach to security authorizations for Cloud Service Offerings. FedRAMP was codified by the FY23 National Defense Authorization Act (NDAA) as the authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information.



Key Players:

- U.S. Federal Government Agencies (Customers)
- Cloud Service Providers (CSPs)
- Third Party Assessment Organizations (3PAOs)
- FedRAMP Program Management Office (PMO)
- FedRAMP Board* (GSA, DoD, DHS, VA, FDIC)



Timeline and Major Steps:

- 6-9 Months to FedRAMP ATO
- Partnership Establishment
- Full Security Assessment
- Authorization Process
- Continuous Monitoring

What is FedRAMP 20x?

FedRAMP 20x Overview

FedRAMP 20x is an initiative aimed at modernizing the FedRAMP authorization process to make cloud security assessments faster, simpler, and more automated. It introduces a cloud-native approach that shifts more responsibility to cloud service providers, reducing redundant steps and paperwork.

Motivated by:

- The need for modernization and streamlining
- Lengthy timelines
- The need for better collaboration between agencies and cloud service providers

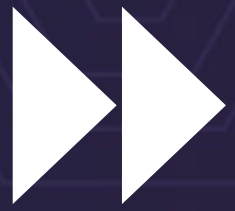
Goals of FedRAMP 20x:

- Automating security validation for over 80% of requirements, minimizing manual documentation
- Continuous monitoring with automated enforcement to prevent security lapses.
- Direct collaboration between cloud service providers and federal agencies.

Major Changes in FedRAMP 20x

Aspect	FedRAMP Rev. 5	FedRAMP 20x
Compliance Approach	Manual, document-heavy process	Automated compliance with machine-readable documentation (OSCAL)
Authorization Timeline	Lengthy, often months to a year	Streamlined, significantly reduced review timelines
Monitoring	Periodic security assessments	Real-time continuous monitoring
PMO Involvement	Extensive manual reviews	Reduced manual oversight, automated validations
Agency Engagement	Indirect, through FedRAMP PMO	Direct engagement between CSPs and federal agencies
Security Certifications	FedRAMP-specific controls	Allows leveraging existing certifications (ISO 27001, SOC 2, etc.)

Impact & Future Outlook



Expected Benefits

Accelerated Authorizations: The initiative has significantly increased the speed of approvals. Since the official announcement of FedRAMP 20x on March 24, there have been 29 new authorizations.
Reduced Bureaucracy: The Significant Change Notification Standard enables CSPs to make certain modifications without prior government approval, reducing delays.



Agency & Vendor Preparation

- **Ongoing Stakeholder Collaboration**: FedRAMP is actively engaging with DoD, DISA, CISA, VA, HHS, and OMB to align security standards with evolving federal needs.
- **Greater CSP Accessibility**: The program is lowering barriers for new CSPs, making FedRAMP authorization more attainable for a broader range of vendors.



Next Steps:

- **Phase One Pilot**: Uses Key Security Indicators instead of traditional baselines and is open to any CSP. Currently focused on FedRAMP Low authorizations, Phase Two will introduce FedRAMP Moderate authorizations.
- **Expanded Community Engagement**: Industry working groups, emerging tooling.

Introduction to GovRAMP



What is GovRAMP?

StateRAMP (dba GovRAMP) is an effort to efficiently and effectively verify cybersecurity and third-party risk management for state and local governments. The goal is to create a framework that can be implemented by procurement for continuous cybersecurity improvements. GovRAMP is a 501c6 non-profit organization governed by a Board of Directors and committees.



Key Players:

- State, Local, and Educational entities (Customers)
- Service Providers (SPs)
- Third Party Assessment Organizations (3PAOs)
- GovRAMP Program Management Office (PMO)



Timeline and Major Steps:

- 6-9 Months to GovRAMP ATO
- Partnership Establishment
- Ready Security Assessment
- Full Security Assessment
- Authorization Process
- Continuous Monitoring

GovRAMP Rebranding

StateRAMP to GovRAMP Rebranding

StateRAMP’s rebranding represents the organization's continuous effort to integrate cybersecurity frameworks across various government levels, such as state, local, tribal, and educational institutions, while maintaining connections between the public and private sectors.

Why?

- Holistic approach to cybersecurity across multiple levels of government
- Inclusivity and unifying public sector cybersecurity
- Ability to serve the community industry that have diverse compliance goals and requirements

Impact?

- Legal name will remain as StateRAMP
- Phased transition to adopting the GovRAMP name and branding
- No effects to Service Providers and 3PAOs

Understanding Key GovRAMP Verified Status'

Status	Description
Core *(*new status)*	• Confirms implementation of 60 foundational NIST controls • Assessed by GovRAMP PMO and does not require a 3PAO assessment • Reduces the burden for providers where a full audit may not yet be practical • Based on the MITRE ATT&CK Framework and aligned with the Moderate Impact Level baseline • Requires quarterly continuous monitoring upon receiving status
Ready	• Attained by meeting the GovRAMP minimum mandatory requirements • Requires a 3PAO assessment of the GovRAMP minim mandatory requirements • Requires completion of at least 50% of required GovRAMP documentation • Requires continuous monitoring upon receiving status
Authorized	• Requires completion of all required GovRAMP documentation • Requires a 3PAO assessment • Requires completion of at least 50% of required GovRAMP documentation • Requires quarterly continuous monitoring upon receiving status

GovRAMP Holistic Public Sector Approach

Initiative	Objective and Impact
Framework Harmonization	• GovRAMP is aligning its controls and processes with other frameworks and compliance programs • Reduces compliance duplication, simplifies vendor onboarding, and promotes cross-jurisdictional trust
TX-RAMP Collaboration	• GovRAMP and TX-RAMP are working toward mutual recognition of security authorizations, enabling vendors to reuse assessments across programs • Accelerates time-to-market for cloud providers and reduces audit fatigue
Expanded Membership Model	• A new tiered membership structure was introduced in 2025, including annual renewal dates and differentiated pricing for providers and 3PAOs • Enhances sustainability of the program and provides clearer value tiers for participants.
Snapshot Program	• This tiered recognition system allows cloud products to be listed as 'Progressing' toward full authorization, offering visibility while they complete requirements. • Encourages transparency and incremental progress, helping vendors build trust with government buyers.
CJIS Overlay	• Set of controls tailored to help service providers conform with CJIS 5.9.5 requirements to meet the needs of criminal justice agencies • Enables law enforcement and justice agencies to adopt cloud solutions with confidence in compliance
FedRAMP 20x Influence	• The shift in FedRAMP's model which emphases automation, agency-led reviews, and faster onboarding has the potential to shape GovRAMP's approach to streamline its own processes • A working group has been established to monitor and identify potential opportunities for the growth of the GovRAMP program

Introduction to DoD CC SRG



What is the DoD CC SRG?

The Department of Defense (DoD) recognizes that cloud computing can augment & support critical national security missions that support the modern-day warfighter. Through the same concepts that spawned FedRAMP, the DoD Cloud Computing Security Requirements Guide (CC SRG) was created. CC SRG outlines a standardized security model that DoD mission owners/authorizing officials use, along with security controls and requirements necessary for cloud-based solutions.



Key Players:

- U.S. DoD Mission Owners (Customers)
- Cloud Service Providers (CSPs)
- Third Party Assessment Organizations (3PAOs)
- Defense Information Systems Agency (DISA)
- Defense Security/Cybersecurity Authorization Working Group (DSAWG)



Timeline and Major Steps:

- 9+ Months to DoD PA
- DoD Partnership Establishment
- Full Security Assessment
- DSAWG review
- Cloud Connection Approval Process

DoD Impact Level Overview

Impact Level	Information Sensitivity	Security Controls (Minimum)	Additional Controls Based on Data	Separation	DoD Users Connect via	Location	Personnel Security Requirements
IL2	• Public • No PII/PHI • Non-Critical Mission Information	• FedRAMP Moderate	• N/A	• Virtual/Logical Public Community	• Internet	• US and outlying areas or DoD on-premises	• US Persons or Foreign Persons • Tier 1 BI
IL4	• CUI (includes PII/PHI) • Non-Critical Mission Info • Non-National Security Information	• FedRAMP Moderate	• Additional CNSSI 1253 Overlays (Table D1 CIA MMx)	• Virtual/Logical Limited Public Community • Strong logical separation, support for DoD “search and seizure”	• NIPRNet via BCAP	• US and outlying areas or DoD on-premises	• US Persons Only • Tier 2 BI
IL5	• Higher Sensitivity CUI (“Serious adverse affect”) standard • Non-National Security Information	• FedRAMP High	• Additional CNSSI 1253 Overlays (Table D1, CIA HHx))	• Virtual/Logical Federal Government Community • Must be physically separate from commercial environment	• NIPRNet via BCAP	• US and outlying areas or DoD on-premises	• US Persons Only • Tier 2 BI - non-sensitive moderate risk impact • Tier 4 BI - non-sensitive high risk OR access to customer data

DoD Impact Level Overview (cont.)

Impact Level	Information Sensitivity	Security Controls (Minimum)	Additional Controls Based on Data	Separation	DoD Users Connect via	Location	Personnel Security Requirements
IL5 NSS	• Unclassified National Security Information • National Security System (NSS)	• FedRAMP High	• Additional CNSSI 1253 Overlays (Table D1 + controls in CIA HHx)	• Virtual/Logical Government Community • Must be physically separate from commercial environment	• NIPRNet via BCAP	• US and outlying areas or DoD on-premises	• US Persons Only • Tier 2 BI - non-sensitive moderate risk impact • Tier 4 BI - non-sensitive high risk OR access to customer data
IL6	• Classified SECRET • National Security System (NSS)	• FedRAMP High	• Additional CNSSI 1253 Classified Overlays (Table D1 + CIA HHx)	• Virtual/Logical Federal Government Community • Must be physically separate from unclassified and commercial environments	• SIPRNet Direct	• US and outlying areas or DoD on-premises • Classified Facilities Only	• US Citizens Only • SECRET Clearance • Tier 5 BI

DoD CC SRG Authorization Process



Initial DCAS Intake

Authorizing a commercial cloud service offering begins by the Mission Owner initiating via the DoD Cloud Authorization Service (DCAS) web portal.

During the initial contact meeting, DISA will meet with the CSP and the DoD Sponsor to review the requirements for a DoD Provisional Authorization.

DISA staff will outline the authorization process and help the CSP, and the DoD sponsor determine the best path forward.



DISA & CSP Authorization Planning

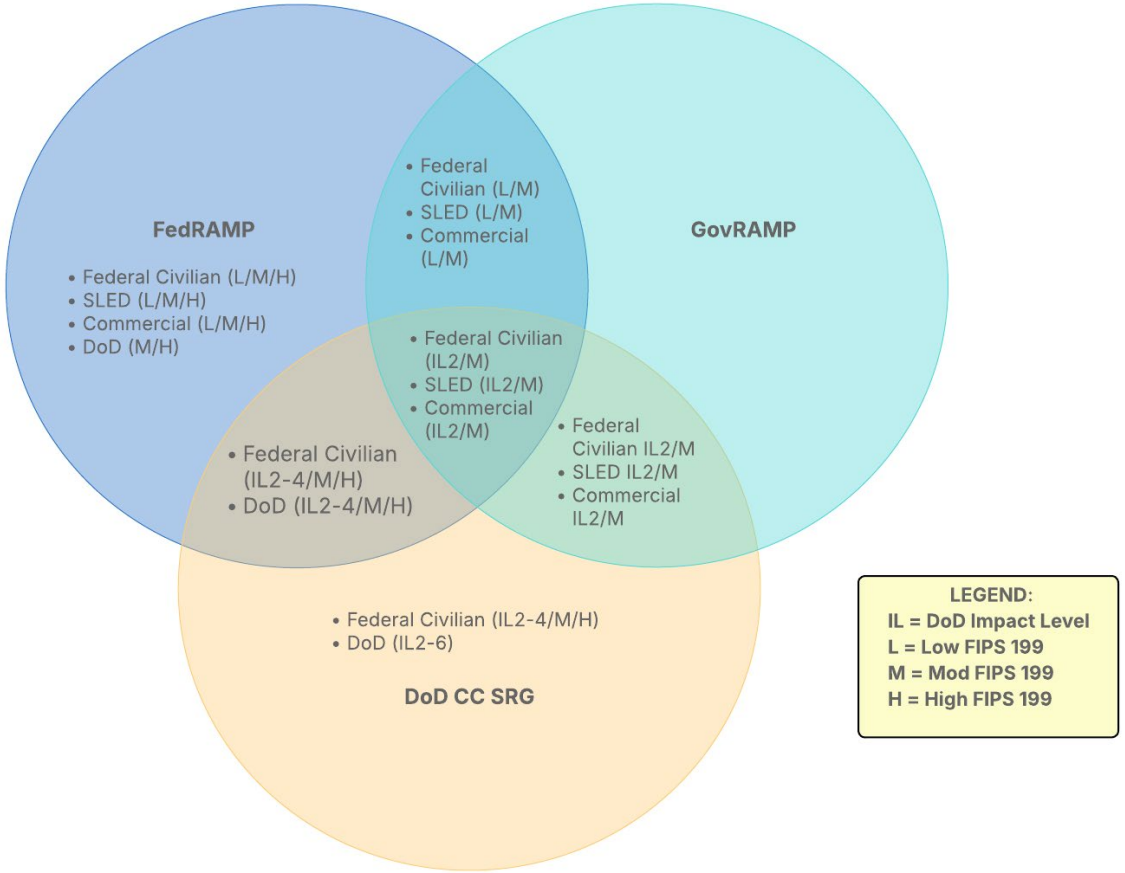
- The DoD CC SRG authorization process extends upon processes established by FedRAMP.
- A CSP will undergo initial and annual assessments in coordination with a 3PAO and will separately be assessed by DISA's Cloud Assessment team.
- Once assessed by DISA, an Authorizing Official (AO) grants a DoD Provisional Authorization.



DoD Mission Owner Onboarding

- A provisional authorization is DISA's "stamp of approval" that you meet the core security requirements for connection to the DISN
- DoD Mission Owners maintain operational control of their networks and must still grant you an ATO for the CSP's CSO
- DISA Cloud Connection Process Guide (CCPG) follows for onboarding to DoD Boundary Cloud Access Point (BCAP)

Customer Reciprocity Across Programs



Q&A

Agenda Topic title:

SPEAKER NAME | JOB TITLE (COMPANY)

COALFIRE RAMPCON
06.09 — 06.10.2025 • WASHINGTON D.C.

COALFIRE RAMPCON
06.09 — 06.10.2025 • WASHINGTON D.C.