GovRAMP

Framework Harmonization

Working Group

April 13, 2026

Agenda

GovRAMP Strategic Initiative: Framework & Regulatory Harmonization

- Program Updates
- GovRAMP Symposium on Regulatory Harmonization (March 9th in D.C.)
- CMMC Subgroup Takeaways (April 2nd)
- FedRAMP RFC Updates

Program Updates

Progressing Snapshot Study + 3PAO

GovRAMP Security Program

From On-RAMP progressing snapshot program to verified statuses

Snapshot

Cyber NIST Score of 40 Controls

Progressing Snapshot

Cyber NIST Score of 40 Controls + Monthly Advisory + Quarterly Snapshot Updates

Core Status

Demonstrates achievement with assessment of 60 NIST Controls by PMO, Quarterly ConMon + Documentation

Ready Status

Demonstrates achievement with Ready Audit of 80 NIST Controls by 3PAO, Monthly ConMon + Annual Audit + Documentation

Authorized or Provisionally Authorized Status

Demonstrates achievement with Security Audit of 300+ NIST Controls by 3PAO, Monthly ConMon + Annual Audit + Documentation

Assessment & Validation Conducted by PMO

Assessment by 3PAO, With PMO Validation & ConMon

2025 Progressing Security Snapshot

Compliance Done Right is Security in Motion

- 181 Cloud Service Providers
- 28,600 Data Points
- 7 Quarters of Measured Progress

The results are clear: structure, feedback, and repetition — the hallmarks of GovRAMP — are the drivers of measurable security progress.

Source: GovRAMP PSP Progress Report, December 2025

40 – 60%

Control performance improvement

Within the first year of participation

2.2 qtrs

Average time to pass a control

Fastest: IR-04 at 1.77 quarters

50%

Higher pass rates

For CSPs who stay engaged 4+ quarters

7.21%

Of total score: CM-06 alone

Requires 90 days of evidence to pass

3PAO Discount Program

Builds on GovRAMP's preparation and On-RAMP programs

GovRAMP Launches 3PAO Discount Program for Progressing Security Snapshot Graduates and Core-Verified Service Providers - GovRAMP

- Participating 3PAOs will offer assessment discounts of up to 30% for service providers that have participated in the GovRAMP Progressing Security Snapshot program or achieved GovRAMP Core verification. 3PAOs include:
  - A-LIGN
  - Prescient Security
  - Coalfire
  - Fortreum
  - RISCPoint

CMMC Alignment

Subgroup Takeaways

CMMC Alignment: Levels 1 & 2

Leverage GovRAMP to demonstrate compliance for Levels 1 & 2

- **CMMC Level 1 (**CMMC Assessment Guide Level 1)
  - **CMMC requires:**
    - Implementation of 15 basic safeguarding requirements from FAR 52.204-21 (protecting Federal Contract Information)
    - Annual self-assessment (no third-party assessment required)
    - All requirements must be fully implemented — POA&Ms are not permitted at Level 1
- **CMMC Level 2 – CUI (**CMMC Assessment Guide Level 2
  - **CMMC requires:**
    - Full compliance with NIST SP 800-171
    - CMMC Level 2 assessment (self-assessment or C3PAO depending on phase)
    - CSP must demonstrate **FedRAMP Moderate equivalency**

GovRAMP Aligns with "FR Moderate Equivalency"

- **GovRAMP Requirements for Authorization at Moderate Impact Level Align to FedRAMP Moderate Impact Level (Rev. 5)**
  - In February, the Standards & Technical Committee adopted federal overlay to GovRAMP Authorization (Low, Mod, High) that clearly demonstrate FedRAMP Rev. 5 requirements that are "overlay" to GovRAMP Rev. 5 requirements.
    - View GovRAMP Federal Overlay (Low_Moderate_High) v2.xlsx
    - **View Next slide for Moderate Impact Level Overlay**

		GovRAMP Parameters	
ID	**Control Name**	**GovRAMP-Defined Assignment / Selection Parameters (Numbering matches SSP) [Dec 2023]**	**FedRAMP Moderate Parameter**
AU-11	Audit Record Retention	AU-11 [a time period in compliance with government requirements]	AU-11 [a time period in compliance with M-21-31]
CA-6	Authorization	CA-6 (e) [when a significant change occurs]	CA-6 (e) [in accordance with OMB A-130 requirements or when a significant change occurs]
CA-8 (2)	Penetration Testing | Red Team Exercises	**Control Not Selected by GovRAMP**	
CP-9 (8)	System Backup | Cryptographic Protection	CP-9 (08) [all backup files]	CP-9 (08) [all backup files]
IA-2 (6)	Identification and Authentication (organizational Users) | Access to Accounts —separate Device	IA-2 (6)-1 [local, network and remote] IA-2 (6)-2 [privileged accounts; non-privileged accounts]	IA-2 (6)-1 [local, network and remote] IA-2 (6)-2 [privileged accounts; non-privileged accounts] IA-2 (6) (b) [FIPS-validated or NSA-approved cryptography]
IA-2 (12)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS	**Control Not Selected by GovRAMP**	
IA-8 (1)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES	**Control Not Selected by GovRAMP**	
MP-5	Media Transport	MP-5 (a) [all media with sensitive information] [prior to leaving secure/controlled environment: for digital media, encryption in compliance with government requirements.	MP-5 (a) [all media with sensitive information] [prior to leaving secure/controlled environment: for digital media, encryption in compliance with Federal requirements and utilizes FIPS validated or NSA approved cryptography (see SC-13.); for non-digital media, secured in locked container]
SA-4 (10)	Acquisition Process | Use of Approved PIV Products	**Control Not Selected by GovRAMP**	
SC-8 (1)	Transmission Confidentiality and Integrity | Cryptographic Protection	SC-8 (1) [prevent unauthorized disclosure of information AND detect changes to information]	SC-8 (1) [prevent unauthorized disclosure of information AND detect changes to information]
SC-13	Cryptographic Protection	SC-13 (b) [FIPS-compliant or modern cryptography, see FIPS 140-2 Annex A]	SC-13 (b) [FIPS-validated or NSA-approved cryptography]

GovRAMP's On-RAMP

Leverage GovRAMP's On-RAMP Programs to help Prepare for CMMC

- **Start with GovRAMP Progressing Snapshot Program & Core to Prepare for CMMC**
  - **Achieve BOTH GovRAMP Authorization and FedRAMP Equivalency for CMMC**
    - Progressing Snapshot Program has demonstrated effectiveness in preparing providers for GovRAMP verified statuses.
      - View Report: GovRAMP Progress Report 2025 Shows Cloud Providers Improve Security Controls by 40–60% in First Year - GovRAMP
    - Core Status demonstrates achievement of foundational NIST 800-53 controls that are building blocks to GovRAMP Authorized and CMMC Levels 1 & 2.

Strengths

- Strong FedRAMP Equivalency Alignment
- On-RAMP Programs Enable Faster Market Entry
- Proven Precedent Using FedRAMP Rev. 5 for GR
- Verified Authorization Tracking (APL)
- Supervised Continuous Monitoring (ConMon)
- Continuous Monitoring Exceeds CMMC Requirements
- No Federal Sponsor or Contract Required

Opportunities

- Leverage Existing FedRAMP Rev. 5 Equivalency Work
- CMMC Level 1 (Self-Attestation) Alignment
- CMMC Addendum / Overlay for GovRAMP Authorizations
- Documentation, Guidance, and Webinars on Alignment
- Templates and Tools for Evidence Mapping
- Evidence Ingestion and Automation
- Expansion Beyond CSPs
- Alignment with Federal CUI Guidance (GSA)

Weaknesses

- Limited DoD / DoW Awareness of GovRAMP
- Practical Challenges with No Control-Deficiency POA&M Expectation
- Assessment Body Misalignment (3PAO vs. C3PAO)
- CMMC Rigidity Limits Change Flexibility
- Boundary Differences Between GovRAMP and CMMC
- Limited Approved Precedent Under Strict POA&M Interpretation
- Strict DoD Incident Response Timeline Requirements
- Contract-Specific Requirement Variability for CSPs

Threats

- Open POA&Ms Not Accepted Under CMMC Rule
- FedRAMP 20x Uncertainty for DoD / DoW
- CMMC Phase 2 Timeline Pressure (Fall 2026)
- Future Transition From NIST 800-171 to Rev. 3
- ITAR and Data Sovereignty Uncertainty for CUI

Next Steps

Subgroup Takeaways

- Demonstrate GovRAMP Satisfaction of FedRAMP Equivalency for CMMC
- Build a Clear Business Case Addressing CMMC Demand and Speed-to-Market Constraints
- Quantify CMMC Compliance Through GovRAMP and SSP Reuse
- Engage CyberAB Through Targeted Briefings and Subgroup Presentations

FedRAMP RFCs

Updates

Closed FedRAMP Request for Comments (RFC)

(HTTPS://WWW.FEDRAMP.GOV/RFCS/)

RFC	Request for Comment On	Description	Closed
0019	Reporting Assessment Costs	Outlines a new cost reporting requirement for FedRAMP recognized independent assessors (aka Third-Party Assessment Organizations/3PAOs) and cloud service providers, how this data will be managed, and related corrective actions for those who fail to supply it as required.	2-12
0020	FedRAMP Authorization Designations	Proposes changes to directly tackle the confusion between “FedRAMP authorization” and an agency “authorization to operate” to align with terminology and usage in statute, OMB policy, and NIST materials.	2-19
0021	Expanding the FedRAMP Marketplace	Proposes expanding the FedRAMP Marketplace to better serve the entire FedRAMP community.	2-19
0022	Leveraging External Frameworks	Proposes a temporary high speed path to FedRAMP authorization for cloud services with existing security assessments from external security frameworks so that federal agencies and providers can test and pilot these services prior to investing in a full FedRAMP authorization path.	2-26
0023	Rev5 Program Certifications (No Sponsor Required)	Proposes a time-limited opportunity for cloud service providers who have already completed significant progress towards a FedRAMP Rev5 Certification but are struggling to find an agency sponsor due to budgetary constraints with agency information security programs.	2-26
0024	FedRAMP Rev5 Machine-Readable Packages	Proposes modifications to the FedRAMP Rev5 process for current and future Rev5-based assessments and authorizations to ensure that cloud service providers produce machine-readable authorization data that can be ingested by agency tools.	3-11

RFC 22 and RFC 23

- FedRAMP RFC 22 Initial Comment:
  - *"This initial outcome also explains that external frameworks will be adopted incrementally over time, depending on demand, throughput, and relevance. The most frequently leveraged external framework by agencies today for pilot authorizations is SOC 2 Type II and that is where FedRAMP will start for 20x Class A FedRAMP Certifications. FedRAMP is aware of the limitations of this external security framework and will establish some initial guardrails, but Class A FedRAMP Certifications are intended to be transitory…" (Excerpt)*
  - Disappointed to see GovRAMP not included as an external framework to be leveraged.

- FedRAMP RFC 23 Initial Comment:
  - *"In Stage 3, tentatively, FedRAMP hopes to open Rev5 Class A Certifications to any cloud service provider using an external security framework that is 80%+ compatible with FedRAMP Rev5 requirements. Then to open Rev5 Class B and C Certifications to specific types of GRC automation tools and services with proven agency demand." (Excerpt)*
  - GovRAMP Authorizations would meet this requirement, and we are optimistic to see it include Rev 5 Class B and C Certifications (align with Low and Moderate Impact Levels). We will continue to stay engaged, supporting this path for authorization for all CSPs. FedRAMP has said they will publish more detail in June 2026.

Open FedRAMP Request for Comments (RFC)

(https://www.fedramp.gov/rfcs/)

RFC	Request for Comment On	Description	Closing
0025	Retrospective on the Public Comment Process	This RFC proposes to improve the public comment process by inviting FedRAMP stakeholders to share their insights and recommendations from their experiences with the process during the past year.	4/21
0026	Clarifying CA-7 Continuous Monitoring Expectations for Rev5 Providers	Clarifies and proposes to update the FedRAMP CA-7 Continuous Monitoring control for Rev5 providers to ensure they share sufficient ongoing authorization data with all agency customers. The RFC also proposes to remove outdated references to the JAB, establish new requirements for vulnerability and collaborative monitoring, and a structured timeline with corrective actions for non-compliance starting in 2027.	4/22
0027	FedRAMP Rev5 Security Controls Baseline Update for AC, AT, AU, CA, and CM Control Families	Proposes updates to the Additional FedRAMP Security Technical Controls Requirements and Guidance for FedRAMP Rev5 baselines in the Access Control (AC), Awareness and Training (AT), Audit and Accountability (AU), Assessment, Authorization and Monitoring (CA), and Configuration Management (CM) control families. The proposed updates aim to align requirements with FedRAMP's current rules and approach to lower the burden for cloud service providers.	4/22
0028	FedRAMP Rev5 Security Controls Baseline Update for CP, IA, IR, MA, and MP Control Families	Proposes updates to the Additional FedRAMP Security Technical Controls Requirements and Guidance for FedRAMP Rev5 baselines in the Contingency Planning (CP), Identification and Authentication (IA), Incident Response (IR), Maintenance (MA), and Media Protection (MP) control families. These changes aim to refresh outdated requirements, align with current FedRAMP rules, and lower the compliance burden for cloud service providers.	4/22
0029	FedRAMP Rev5 Security Controls Baseline Update for PE, PL, PM, PS, and PT Control Families	Proposes updates to the Additional FedRAMP Security Technical Controls Requirements and Guidance for FedRAMP Rev5 baselines across five control families- Physical and Environmental Protection (PE), Planning (PL), Program Management (PM), Personnel Security (PS), and PII Processing and Technology (PT). The updates are designed to refresh outdated statements, align with current rules, incorporate changes based on NIST 800-53 Rev 5.2.0., and to lower the burden for cloud service providers by eliminating previous pain points.	4/22
0030	FedRAMP Rev5 Security Controls Baseline Update for RA, SA, SC, SI, and SR Control Families	Proposes updates to the Additional FedRAMP Security Technical Controls Requirements and Guidance for FedRAMP Rev5 baselines in the Risk Assessment (RA), System and Service Acquisition (SA), System and Communications Protection (SC), System and Information Integrity (SI), and Supply Chain Risk Management (SR) control families. The updates are intended to refresh outdated guidance to match current FedRAMP rules and lower the compliance burden for cloud service providers.	4/22
0031	Updated Incident Communications Procedures	Proposes updates to FedRAMP's mandatory Incident Communications Procedures for all cloud service providers.	5/12

RFC 25

Retrospective on the Public Comment Process:

https://github.com/FedRAMP/community/discussions/128

- *Most of the commentary has been positive, as has been GovRAMP's experience*

- *Additional comments include*
  - *Too many RFCs*
  - *Discourse also happening on LinkedIn & Working Group Chats*
  - *30 days is insufficient*
  - *Needs to have an anonymous option*
  - *Discoverability / Notifications*

RFC 26

Clarifying CA-7 Continuous Monitoring Expectations for Rev5 Providers

https://github.com/FedRAMP/community/discussions/130

- Allows Service Providers to either:
  - Use FedRAMP's new Vulnerability Detection and Response Balance Improvement Release for Rev5 or
  - Submit monthly monthly POA&Ms and scan results (traditional path)
- Providers MUST provide recurring monitoring information (including meetings) to all agency customers and FedRAMP using one of the following two collaborative continuous monitoring processes:
  - Collaborative Continuous Monitoring Balance Improvement Release for Rev5
  - FedRAMP Rev5 Continuous Monitoring Playbook or successor materials
- Introduces Corrective Action Plan (CAP) triggers for failure to comply, including delisting
  - Applies only to SPs using the FedRAMP Rev5 Continuous Monitoring Playbook
  - Collaborative Continuous Monitoring Balance Improvement Release for Rev5 already has sanctions

RFCs 27 through 30

FedRAMP Rev5 Security Controls Baseline Update

- Multiple Control families grouped into each RFC
  - RFC 27 = AC, AT, AU, CA, & CM *https://github.com/FedRAMP/community/discussions/131*
  - RFC 28 = CP, IA, IR, MA, & MP *https://github.com/FedRAMP/community/discussions/132*
  - RFC 29 = PE, PL, PM, PS, & PT *https://github.com/FedRAMP/community/discussions/133*
  - RFC 30 = RA, SA, SC, SI, & SR *https://github.com/FedRAMP/community/discussions/134*

- Incorporates updates from NIST SP800-53 rev 5.2 and the Balance Improvement Release (BIR)

- Many comments asking for clarification on document references, and new 20x acronyms

RFC 31

Updated Incident Communications Procedures

https://github.com/FedRAMP/community/discussions/138

This RFC proposes updates to the Incident Communications Procedures as follows:

- Move reporting on incidents causing an impact to availability into public status pages or other notification mechanisms without requiring federal-specific reporting.
- Focus incident reporting on likely or confirmed incidents that threaten confidentiality or integrity of federal customer data.
- Clearly define the expected incident reporting data for federal reportable incidents.
- Modify the expected timeframes for federal reportable incidents to factor for the potential adverse impact to the government and the level of commitment from the cloud service provider for managing agency risk, including much stricter requirements for cloud services that commit to Class D (High) certifications to align with the potential impact of an incident to such systems used by agencies.

Note: No comments in GitHub as of 4/10/2026

GovRAMP CYBER SUMMIT

PRESENTING SPONSOR carahsoft.

SAN ANTONIO

NOV 15-18, 2026

Registration Now Open

More Security. Less Burden.
Advancing secure, efficient cloud adoption across government through shared assurance, collaboration, and practical implementation

govramp.org/2026-cyber-summit/

Membership Reminder

Renewal Deadline: June 1, 2026

Renew your GovRAMP membership to maintain access to program resources, engagement opportunities, and recognition.

Log in to your Member Portal (members.govramp.org/portal/) to renew or contact the GovRAMP team (info@govramp.org) to discuss membership renewal.

Q2 GovRAMP Member Meeting

Thursday, June 11 | 2 – 3 PM ET

A quarterly gathering of GovRAMP members across the public and private sector to connect, share updates, and align on program priorities.

If you are interested in attending, please email info@govramp.org for registration details.