GovRAMP

Version 1.0

Getting Started with GovRAMP: A Guide for Service Providers

October 2026

A practical guide to navigating GovRAMP membership, verification pathways, and continuous monitoring.



How to Use this Guide

This guide is designed to serve two purposes. Read straight through, it provides an end-to-end orientation to the GovRAMP journey—from joining as a member to maintaining a verified status. Read by section, each major part functions as a self-contained learning module that aligns directly with a companion course in GovRAMP Academy, our learning management system (LMS).

The Guide at a Glance

1. **Why Membership Matters** — Understand what GovRAMP membership unlocks and why it is the foundation for everything that follows.
2. **Choosing a Membership Tier** — Compare membership tiers and determine which option best fits your organization's stage, needs, and budget.
3. **The Six On-Ramps Explained** — Get an at-a-glance overview of each verification path, what it requires, and what it delivers.
4. **On-Ramp Deep Dives (Course Modules)** — Explore each On-Ramp in depth, including how to prepare, what to expect at each step, and what to do after earning your status.
5. **Picking the Right On-Ramp** — Use a self-selection framework to identify the right path, with guidance on how data classification and contract requirements influence the decision.
6. **Working With the PMO** — Learn who the PMO is, what they do at each stage of the process, and how to build a productive working relationship.
7. **Continuous Monitoring** — Understand the ongoing requirements for maintaining a verified status and how to make continuous monitoring part of your routine.

How to Read the Deep-Dive Modules

Every On-Ramp deep dive in Section 4 follows the same three-part structure, giving learners a consistent framework for understanding each verification path:

- **How to Prepare —** What to have in place—including documentation, evidence, and key decisions—before you begin.
- **What the Process Involves —** A step-by-step overview of the journey, from membership through achieving verified status.
- **What to Do Once You're Verified —** How to maintain your status, remain listed, and build toward the next level of verification.

A Note on Sequence

The On-Ramps are **not a required progression**. There is no mandatory starting point—you can pursue the path that best aligns with your product, data, and current contract requirements. The deep dives are presented from least to most rigorous simply to make the information easier to navigate.

About GovRAMP

What GovRAMP Is

GovRAMP is a nonprofit, member-driven program that provides a standardized, NIST-aligned approach to verifying and continuously monitoring the cybersecurity posture of cloud service offerings used by federal, state, local, tribal, territorial, and education governments. Founded in 2020 as StateRAMP, the program rebranded as GovRAMP in 2025 to reflect its expanded scope across the full public sector landscape.

GovRAMP is built on three foundational principles:

- **Verify once, serve many.** Providers complete a standardized verification that can be leveraged by government buyers across jurisdictions—reducing assessment burden for providers while saving time and resources for SLED agencies.
- **Continuous, not point-in-time.** Verification does not end when a status is achieved. Ongoing monitoring requirements provide continued visibility into a provider's security posture and help ensure that risk remains actively managed.
- **Standardized assurance.** A consistent NIST 800-53 Rev. 5 framework is applied across providers and scaled to the impact level of the data and services being protected.

As a 501(c)(6) membership organization, GovRAMP serves as a bridge between public- and private-sector security, procurement, and continuous risk-management needs. Service providers must become members to participate in the program, creating greater transparency for public-sector organizations evaluating providers and their commitment to security and risk management.

At its core, the GovRAMP risk-management framework is based on **identifiable risk acceptance**: matching the level of security required for different types of public-sector data with the NIST controls needed to provide that level of protection. The On-Ramps described in this guide translate that framework into practical verification paths, creating accessible entry points for providers across different sizes, products, and levels of security maturity.



Contents

How to Use this Guide 02

About GovRAMP 03

1. Why Membership Matters 05

2. Choosing a Membership Tier 06

3. The Six On-Ramps Explained 09

4. On-Ramp Deep Dives 13

4.1 Single Security Snapshot 13

4.2 Progressing Security Snapshot Program 15

4.3 Core Status 17

4.4 Ready Status 19

4.5 Authorized Status 21

4.6 Fast Track for Federal Program 23

6. Picking the Right On-Ramp 25

7. Working with the PMO 29

8. Resources & Next Steps 33

Glossary of Key Terms 34

1. Why Membership Matters

Before a service provider's product can be reviewed by the PMO, listed on the Authorized Product List, or pursue a verified GovRAMP status, the organization must be an active GovRAMP member. Membership is more than a badge—it is the gateway to the program's verification pathways, resources, community, and opportunities to connect with public-sector buyers.

What Membership Unlocks

Membership opens the full ecosystem

GovRAMP membership provides access to the broader ecosystem of resources and opportunities designed to help providers navigate verification, strengthen their security posture, and engage with the public sector.

Eligibility to Pursue Status
Membership is required for a product to be assessed by the PMO and for an organization to pursue any verified GovRAMP status.

Community & Influence
Participate in committees and task forces that help shape technology priorities, evolving security standards, and framework harmonization. Members can also participate in the annual Cyber Summit, member meetings, and other GovRAMP events that bring together SLED and industry leaders.

Product List Visibility
Gain visibility with public-sector buyers through the Authorized Product List (APL) or Progressing Product List (PPL), where SLED organizations can identify and evaluate participating providers.

Learning Community
Access the GovRAMP Learning Community, with self-paced education covering GovRAMP fundamentals, becoming a strong government partner, sales enablement, and deeper technical training for security teams.

2. Choosing a Membership Tier

Every membership tier provides the core benefits needed to participate in GovRAMP. Higher tiers add opportunities for greater visibility, executive access, and event savings for organizations looking to deepen their engagement with the GovRAMP community.

Tier 1 — Basic
Start Smart. Build Credibility.

$2,500 / year

Ideal for organizations entering the government cloud market or beginning their GovRAMP journey.

✓ Eligibility to participate in the GovRAMP Security Program (APL/PPL listing as applicable)
✓ Eligibility for event sponsorships (non-speaking)
✓ Listing in the GovRAMP Member Directory
✓ Access to the secure Member Portal
✓ Attendance at quarterly member meetings
✓ Access to recordings for the Virtual Education Series on the LMS
✓ Eligibility for committee nomination
✓ Member pricing on eligible GovRAMP in-person events
✓ GovRAMP Basic Member Badge

Tier 2 — Prime
Accelerate Growth. Deepen Engagement.

$5,000 / year

Adds expanded engagement opportunities, leadership access, and event savings.

Includes all Basic benefits, plus:

✓ 10% discount on eligible GovRAMP in-person events
✓ GovRAMP Prime Member Badge
✓ Access to participation in the Biannual Virtual Education Series
✓ Eligibility to serve on one Task Force
✓ Attendance in the Provider Leadership Council (PLC)
✓ Quarterly office hours with GovRAMP Membership Staff (sales enablement)
✓ Eligibility for event speaking sponsorships
✓ Access to GovRAMP enablement information in the LMS

Tier 3 — Premier

Lead the Market. Amplify Your Influence.

$10,000 / year

Designed for established leaders seeking greater visibility, strategic access, and opportunities to shape the GovRAMP community.

Includes all Prime benefits, plus:

✓ One complimentary pass to GovRAMP in-person events, plus 20% off additional tickets
✓ GovRAMP Premier Member Badge
✓ Eligibility to serve on multiple Task Forces
✓ Participation in the Provider Leadership Council (PLC)
✓ Biannual 1:1 strategy call with GovRAMP executive staff
✓ Eligibility for a Member Spotlight across GovRAMP social media and web channels
✓ Invitations to exclusive government-industry roundtables
✓ Featured listing on the GovRAMP Partners Page
✓ Featured listing in the GovRAMP Community Directory

Tier 4 — Elite

Grow the Mission. Build the Ecosystem.

$25,000 / year

Designed for organizations seeking deeper strategic engagement, expanded leadership opportunities, and a more active role in advancing the GovRAMP ecosystem.

Includes all Premier benefits, plus:

✓ Two complimentary passes to GovRAMP in-person events, plus 25% off additional tickets
✓ First right of refusal for GovRAMP Task Forces
✓ Quarterly 1:1 strategy calls with GovRAMP executive staff
✓ First right of refusal for GovRAMP event sponsorship opportunities
✓ Annual virtual GovRAMP enablement session for your team
✓ Annual Member Spotlight across GovRAMP social media and web channels
✓ Customized co-branded marketing support
✓ Reserved seating at the GovRAMP Cyber Summit

Tier 5 — Champion
Stand Out. Drive Strategic Impact.

$50,000 / year

Reserved for organizations at the forefront of the cloud security and assurance landscape, with a demonstrated commitment to advancing the GovRAMP mission and shaping the broader ecosystem.

Includes all Elite benefits, plus:

✓ Four complimentary passes to GovRAMP in-person events, plus 30% off additional tickets
✓ GovRAMP Champion Member Badge
✓ Guest speaking opportunity in the Virtual Education Series
✓ One seat on the Provider Leadership Council (PLC) Board
✓ Monthly 1:1 strategy call with GovRAMP leadership
✓ Annual in-person GovRAMP enablement session for your team
✓ Biannual Member Spotlights across GovRAMP social media and web channels
✓ One fellowship sponsorship, with the ability to select one individual to serve as a mentor

Small Business Pricing Available

IIf your organization's annual revenue is less than $5 million, you may qualify for Small Business Membership Dues. Apply through the dedicated form.

Annual Revenue	Basic	Prime	Premier	Elite	Champion
< $1 Million	$1,000	$2,500	$5,000	$12,500	$25,000
$1 – 5 Million	$1,750	$3,500	$7,000	$17,500	$35,000

Renewal Note

All private-sector memberships renew annually on June 1, regardless of the original start date. 2026 Basic dues of $1,500 and Prime dues of $2,500 remain in effect through January 1, 2027.

3. The Six On-Ramps Explained

GovRAMP is not a single pass/fail assessment. It offers multiple pathways designed to meet providers where they are—from establishing an initial baseline to pursuing verified status. Each pathway serves a different purpose and can help providers build security maturity, demonstrate progress, or achieve a level of assurance that aligns with their product, data, and contractual requirements. While these pathways may appear linear, **they are not sequential**. There is no required starting point. The right path depends on factors such as the type and sensitivity of data your product handles, your existing security posture, and the requirements of your government contracts.

This section provides an at-a-glance overview of each pathway. Section 4 expands each On-Ramp into a practical, step-by-step guide.

Single Security Snapshot

Self-Assessment · Point-in-Time

40 NIST Controls

A one-time, PMO-validated assessment of your product's security posture against 40 foundational NIST 800-53 Rev. 5 controls. The Snapshot provides a security maturity score and gap analysis, helping you understand your current posture and identify what to address next. It goes beyond self-attestation while **not requiring a 3PAO assessment**.

VALIDATION	3PAO NEEDED?	OUTPUT
PMO Reviewed	No	Gap Analysis & Score

Best for: Providers looking for a focused, point-in-time assessment of their security posture before committing to an ongoing program or pursuing a higher level of verification.

Progressing Security Snapshot Program

Guided · Ongoing Improvement

40 High-Impact Controls

An ongoing program designed to help providers strengthen their security posture and demonstrate measurable progress toward GovRAMP verification. The program includes quarterly Snapshot assessments and monthly advisory calls with the PMO, providing structured guidance as providers identify and address security gaps.

Providers participating in the program may also receive public visibility through the Progressing Product List (PPL), subject to current listing requirements. Beginning January 1, 2026, products must demonstrate active improvement to remain eligible for PPL listing.

VALIDATION	3PAO NEEDED?	VISIBILITY
PMO Advisory	No	Progressing Product List

Best for: Providers seeking a structured, supported path to strengthen their security posture, demonstrate measurable progress to government buyers, and build toward a higher level of GovRAMP verification.

Core Status
PMO-validated baseline

60 NIST Controls

A verified status confirming implementation of 60 foundational NIST controls aligned to the Moderate Impact Level baseline. Core is assessed directly by the GovRAMP PMO and does not require a 3PAO assessment, providing a validated entry point for providers seeking to demonstrate foundational security maturity and prepare for higher levels of verification.

VALIDATION	3PAO NEEDED?	VISIBILITY
PMO Reviewed	No	Authorized Product List

Best for: Commercial products or SMB providers seeking faster, lower-cost market entry — and any provider whose product fits lower-impact use cases where full 3PAO investment isn't yet warranted.

Ready Status
3PAO-assessed readiness

80 NIST Controls

An independently assessed status demonstrating that a product meets GovRAMP's minimum mandatory requirements. Ready requires a third-party assessment of 80 NIST controls, documented through a Readiness Assessment Report (RAR) or Security Assessment Report (SAR), followed by PMO validation. It establishes independent assurance while preparing providers for Authorized or Provisional Verification.

VALIDATION	3PAO NEEDED?	VISIBILITY
3PAO Assessment	Yes	Authorized Product List

Best for: Providers ready for independent third-party assessment who want to demonstrate that their product meets GovRAMP's minimum mandatory requirements and position themselves for broader government procurement opportunities.

Authorized Status
Full GovRAMP Authorization

300+ NIST Controls

Authorized Verification is GovRAMP's highest level of verification, confirming that a product meets the applicable GovRAMP requirements through a comprehensive third-party assessment, PMO validation, and government sponsorship or approval. The assessment covers 300+ NIST 800-53 Rev. 5 controls, depending on impact level, and includes ongoing continuous monitoring. A CJIS-Aligned Overlay is available for providers serving criminal justice use cases.

VALIDATION	3PAO NEEDED?	SPONSOR
3PAO (SAR) + PMO	Yes	Government Required

Best for: Providers serving moderate- and high-impact SLED workloads, regulated data, or contracts that require the highest level of GovRAMP verification.

Fast Track for Federal Programs
Reuse Existing Federal Work

FT Accelerated

An accelerated pathway for providers with existing federal security documentation. GovRAMP Fast Track allows providers to reuse materials such as a **Readiness Assessment Report (RAR), Security Assessment Report (SAR), and Continuous Monitoring (ConMon) documentation**. The PMO reviews existing materials for alignment with GovRAMP requirements, helping reduce duplicative assessment work, time, and cost. Fast Track also supports providers participating in evolving federal initiatives such as FedRAMP 20x.

VALIDATION	3PAO NEEDED?	ONBOARDING
Existing FedRAMP Work	Already Done	Within ~3 Months

Best for: Providers with existing federal security documentation who want to leverage their previous assessment work and streamline their path into the SLED market.

Program Insights

GovRAMP's 2025 Progress Report provides evidence of how participation in the Progressing Security Snapshot Program (PSSP), can support measurable improvements in security maturity. The analysis examined the impact of structured, ongoing assessments and advisory support on participating service providers' security programs.

The PSSP is designed around a simple principle: **security maturity improves through consistent assessment, feedback, and action**. Rather than treating compliance as a one-time exercise, the program gives service providers a recurring cadence for evaluating controls, identifying gaps, strengthening evidence, and improving their security practices over time.

The 2025 analysis draws on more than 28,600 control-level data points from 181 service providers across seven quarters of participation.

The findings demonstrate measurable progress:

- **Control performance improved by 40–60% within the first year** of PSSP participation, with the most significant gains occurring between the second and fourth quarters.
- **Service providers achieved a passing status on individual controls in an average of 2.2 quarters**, demonstrating that repeated assessment and feedback can help providers make steady progress.
- **Configuration management and identity assurance remain areas of challenge and opportunity**, highlighting where focused attention can contribute to broader security maturity.
- **Participation in the PSSP is associated with measurable improvement in security control performance over time**, reinforcing the value of structured, continuous security improvement.

The takeaway is straightforward: **when compliance is structured around continuous improvement, it can become a mechanism for strengthening security—not simply documenting it.**

Improving Accessibility

GovRAMP is also working to make independent third-party assessments more accessible through its 3PAO Discount Program. Launched in 2026, the voluntary program enables participating accredited 3PAOs to offer **assessment discounts of up to 30%** to service providers that have completed the PSSP or achieved Core Verification.

The program is designed to recognize early investment in security readiness and support more efficient, predictable assessment outcomes. GovRAMP reports that providers entering formal assessments after completing PSSP or Core often arrive with stronger documentation, more mature controls, and a clearer understanding of assessment expectations.

As of July 2026, 13 accredited 3PAOs participate in the Discount Program, giving service providers more options when selecting an assessment partner.

Together, the PSSP, Core Verification, and 3PAO Discount Program create a more accessible progression toward independent assessment—helping providers **prepare earlier, identify gaps sooner, and enter formal assessments with greater readiness.**

4. On-Ramp Deep Dives

Each On-Ramp below is a self-contained learning module. Every module follows the same three-part structure: **how to prepare, what the process involves, and what to do once you're verified**. The marker at the top of each module identifies the corresponding course in GovRAMP Academy.

GOVRAMP ACADEMY COURSE MODULE: Single Security Snapshot

4.1 Single Security Snapshot

The Single Security Snapshot is a 12-month, PMO-validated assessment of a product's security maturity against the top 40 NIST 800-53 Rev. 5 controls, with scoring informed by the MITRE ATT&CK framework. It provides a focused view of your current security posture, helping you identify strengths, gaps, and opportunities for improvement—without requiring a 3PAO assessment.

How to Prepare

A Snapshot is most valuable when you arrive prepared to demonstrate your current security posture with supporting evidence. Before your intake meeting:

- **Review the scoring criteria.** Review the GovRAMP Snapshot Criteria and Scoring Matrix to understand the controls evaluated, how scoring is weighted, and what evidence may support each criterion.
- **Gather supporting artifacts.** Be prepared to provide relevant evidence—such as policies, configuration screenshots, scan summaries, training records, and other documentation—for each criterion you believe your product meets.
- **Confirm your hosting environment.** Know whether your product is hosted in a GovRAMP- or FedRAMP-authorized infrastructure-as-a-service (IaaS) environment. Hosting environment can influence the Snapshot score because the PMO considers the level of visibility and security assurance available for the underlying infrastructure.
- **Inventory related security and compliance work.** Identify other security frameworks, assessments, penetration tests, or training programs your organization has completed. Relevant activities may contribute to your Snapshot score where they align with the applicable criteria.

How the Snapshot is Scored

The Snapshot produces a **security maturity score** based on a subset of NIST 800-53 Rev. 5 controls selected and weighted using the MITRE ATT&CK framework. The methodology is designed to emphasize controls and practices with the greatest potential impact on security defense.

- **Control implementation —** Whether applicable security controls and practices have been implemented and can be supported with evidence.
- **Security impact —** The relative importance of the control based on its contribution to reducing security risk.
- **Additional security practices —** Relevant environmental, technical, organizational, and compliance factors that provide additional insight into the product's security maturity.

For example, providers may receive additional scoring consideration for hosting in a GovRAMP Authorized IaaS environment because the PMO has greater visibility into the security posture of the underlying infrastructure. Additional points may also be available for recognized compliance frameworks, penetration testing, security training, and other qualifying practices.

What the Process Involves

The Snapshot follows a short, defined path and typically takes about three weeks from intake to results.

1. **Become a GovRAMP Member:** All providers must be active members before a product can be validated, receive a status, or be listed.
2. **Submit a GovRAMP Service Request Form:** Submit the form to initiate your Snapshot and begin engagement with the PMO.
3. **Attend the Intake Meeting:** Before your one-hour intake, review the scoring criteria and prepare supporting artifacts.
4. **Receive Your Maturity Score (~3 weeks):** The PMO will provide a formal letter with your product's security maturity score. Scores are not publicly posted and may be shared at your discretion.
5. **Review the Gap Analysis:** Use the results to prioritize remediation and determine your next On-Ramp.

Once You're Verified

A Single Snapshot is **point-in-time** and does not require ongoing maintenance or public listing. The value comes from what you do next:

- **Choose your path.** Use your score and gap analysis to determine your next On-Ramp.
- **Consider going ongoing.** The Progressing Security Snapshot Program provides a structured, quarterly improvement cycle with PMO advisory support and PPL eligibility.
- **Share selectively.** You control who sees your score and may share it with prospective government buyers.

Single Security Snapshot Fee

Annual Revenue	Single Snapshot Fee paid to PMO
< $1 Million	$1,073
$1 – 5 Million	$1,610
> $5 Million	$2,683

4.2 Progressing Security Snapshot Program

The Progressing Security Snapshot Program (PSSP) builds on the initial Security Snapshot through quarterly assessments and monthly advisory support from the GovRAMP PMO. The structured cadence helps providers measure progress, address gaps, and strengthen their security posture over time while providing government buyers with an evolving view of security maturity.

Why it Works

The PSSP is designed around a simple principle: **security maturity improves through consistent assessment, feedback, and action**. GovRAMP's 2025 analysis examined more than **28,600 control-level data points from 181 service providers across seven quarters**. Participating providers improved control performance by **40–60% within their first year**, and individual controls reached a passing status in an average of **2.2 quarters**.

Configuration management and identity assurance remain areas where providers can face challenges, while also presenting opportunities for meaningful improvement.

How to Prepare

The program is built around measurable improvement, so preparation focuses on establishing a baseline and creating a sustainable process for ongoing progress:

- **Start with a Snapshot baseline.** Your initial Snapshot establishes the baseline from which your quarterly progress is measured.
- **Assign an internal owner.** Designate a product security lead to participate in monthly advisory calls and coordinate remediation activities.
- **Plan for quarterly evidence.** Establish a lightweight process for refreshing artifacts and documenting improvements each quarter.
- **Understand the improvement requirement.** Beginning January 1, 2026, products must have a score above zero to appear on the PPL and must demonstrate improvement with each quarterly Snapshot. Identical or declining scores may trigger the PMO's escalation process.

What the Process Involves

After enrollment and the initial Snapshot, the PSSP operates as a **structured, ongoing improvement cycle:**

1. **Become a GovRAMP Member:** Active membership is required before participating in the program.
2. **Submit a Service Request:** Submit the request, pay the applicable fee, and complete onboarding with the PMO.
3. **Complete Your Initial Snapshot:** Work with the PMO to establish your baseline score and identify priority areas for improvement.

4. **Participate in Monthly Advisory Calls:** Use your monthly advisory time to review progress, address questions, and identify opportunities to strengthen your security posture.
5. **Complete Quarterly Snapshots:** Provide updated evidence and demonstrate measurable progress against the applicable criteria.
6. **Maintain Progress Toward Verification:** Continue improving your security posture while working toward Core, Ready, Provisional, or Authorized Verification. The PSSP is designed as an on-ramp to verification, not a terminal status.

Once You're Participating

PSSP is designed as an ongoing improvement program rather than a finish line. To get the most value from participation:

- **Keep improving each quarter.** Demonstrating continued improvement helps maintain PPL eligibility and avoid escalation.
- **Use it to prepare for Core or Ready.** The advisory relationship and pre-assessment work can help you transition to Core, Ready, or Authorized with greater readiness.
- **Capture the TX-RAMP benefit.** PSSP participation can qualify you for TX-RAMP Provisional status without the standard 18-month expiration. Achieving Core, Ready, or Authorized can support TX-RAMP Level 2 requirements where applicable.
- **Explore the 3PAO discount.** Completing PSSP may qualify you for assessment discounts of up to 30% through the GovRAMP 3PAO Discount Program.

Annual Revenue	Monthly Progressing Fees paid to PMO
< $1 Million	$805
$1 – 5 Million	$1,073
> $5 Million	$1,717

4.3 Core Verification

Core is a PMO-validated verification confirming implementation of 60 prioritized NIST 800-53 Rev. 5 controls aligned with the Moderate Impact Level baseline. Assessed directly by the PMO, Core does not require a 3PAO assessment and includes quarterly continuous monitoring. It provides a validated security milestone and can serve as a foundation for pursuing Ready or Authorized Verification.

How to Prepare

Core is evidence-driven: the PMO reviews documentation and evidence demonstrating implementation of the 60 required controls. Build your evidence base before submitting.

- **Consider starting with the Progressing Snapshot.** Not required, but PSSP can help providers establish a baseline, identify gaps, and prepare for Core.
- **Complete the Moderate-baseline templates.** Prepare the System Security Plan (SSP), Incident Response Plan, Contingency Plan, Configuration Management Plan, and other required documentation listed in the Service Provider Package.
- **Collect evidence for all 60 controls.** Use the GovRAMP Core Control Evidence Package and Service Provider Package to organize your documentation and supporting artifacts.
- **Finalize policies and procedures.** Ensure required policies and procedures are documented, implemented, and supported by evidence.

What the Process Involves

Core is assessed directly by the PMO, so there is **no 3PAO assessment**. The evidence requirements, however, are substantive.

1. **Become a GovRAMP Member:** Active membership is required before participating in the program.
2. **Complete Documentation & Templates:** Finalize the required Moderate baseline documentation, including the SSP, Incident Response Plan, Contingency Plan, and supporting materials.
3. **Collect Evidence for All 60 Controls:** Organize evidence for each required control using the GovRAMP evidence collection resources.
4. **Submit for Core Review:** Submit your completed documentation and applicable PMO assessment fee for review. The PMO evaluates implementation against the 60 Core controls aligned to the Moderate Impact Level and MITRE ATT&CK framework.
5. **Achieve Core Verification & Begin Quarterly ConMon:** Once the PMO validates your submission, your product receives Core Verification and is listed on the Authorized Product List (APL). You then begin quarterly continuous monitoring to maintain your status.

Once You're Verified

Core is a 12-month verification maintained through quarterly continuous monitoring.

- **Submit quarterly ConMon.** Provide required vulnerability, POA&M, and asset inventory updates to maintain ongoing visibility.
- **Keep your APL listing current.** Continued compliance with monitoring requirements helps maintain your Core Verification and APL listing.
- **Build toward Ready or Authorized.** Core can serve as a foundation for future verification by helping you develop the documentation and evidence needed for a 3PAO assessment.
- **Explore the 3PAO discount.** Core-verified providers may qualify for assessment discounts of up to 30% through participating 3PAOs.

Annual Revenue	Annual Core Review Fee	Quarterly ConMon Fees
< $1 Million	$9,660	$268
$1 – 5 Million	$11,806	$537
> $5 Million	$18,246	$1,073

4.4 Ready Verification

Ready Verification is a **3PAO-assessed status** confirming that a product meets GovRAMP's minimum mandatory requirements. The assessment covers **80 NIST controls** and is documented through a Readiness Assessment Report (RAR) or Security Assessment Report (SAR), followed by PMO validation. Ready demonstrates independent assessment of a product's security readiness and can serve as either a final target or a foundation for pursuing Authorized Verification, depending on the product's maturity and impact level.

How to Prepare

Ready is the first verification stage that requires independent third-party assessment. Preparation centers on determining the appropriate impact level, completing required documentation, and selecting a qualified assessor.

- **Determine your Impact Level.** Identify whether your product falls within the Low, Moderate, or High impact level based on the data it processes and your government customers' requirements. Use the GovRAMP Data Classification Tool to support the determination.
- **Build your documentation.** Prepare the required policies, procedures, system documentation, and supporting evidence for your selected impact level. GovRAMP's Ready requirements include a minimum documentation threshold for the assessment.
- **Select an approved 3PAO.** Review GovRAMP participating 3PAOs and select an assessor that fits your product, scope, and timeline.
- **Budget for the Ready review.** Plan for the applicable PMO review fee, in addition to the separate cost of the 3PAO assessment.

Annual Revenue	Annual RAR Review Fee *(Paid to the PMO)*	Monthly ConMon Fees *(Paid to the PMO)*
< $1 Million	$537	$268
$1 – 5 Million	$2,683	$537
> $5 Million	$4,025	$1,073

What the Process Involves

Ready adds an independent 3PAO assessment to the membership, documentation, and PMO review process.

1. **Become a GovRAMP Member:** Active membership is required before participating in the program.
2. **Determine Your Impact Level:** Identify the appropriate impact level—Low, Moderate, or High—before completing your security package.
3. **Engage an Approved 3PAO:** Work with a GovRAMP participating 3PAO to conduct the independent assessment and prepare the applicable RAR or SAR.
4. **Complete Required Documentation & Submit for Review:** Complete the required documentation for your selected impact level and submit the Security Review Request and supporting materials to the PMO.
5. **Achieve Ready Verification:** Once the 3PAO assessment is complete and the PMO validates that the minimum mandatory requirements have been met, the product receives Ready Verification and is listed on the APL.
6. **Begin Continuous Monitoring:** Maintain Ready through ongoing monthly continuous monitoring and the required annual reassessment.

Once You're Verified

Ready is a 12-month status maintained through ongoing continuous monitoring.

- **Submit monthly and annual ConMon.** Maintain required monitoring activities, including vulnerability, POA&M, and other applicable security updates.
- **Plan your next step.** Ready can serve as a final target for some providers or as preparation for Authorized Verification. The documentation and assessment experience can provide a foundation for the next stage.
- **Share your verified status.** Ready products are listed on the APL, giving government buyers visibility into the product's independently assessed security readiness.

4. On-Ramp Deep Dives

LMS COURSE MODULE: Authorized Status

4.5 Authorized Status

Authorized is the highest level of GovRAMP verification: full NIST 800-53 Rev. 5 control implementation (300+ controls depending on impact level), a complete 3PAO Security Assessment Report (SAR), and — critically — government sponsorship. Both the PMO and a sponsoring government must agree the product meets all requirements. A CJIS-Aligned Overlay is available for criminal-justice data use cases.

How to Prepare

Authorized is the most rigorous path. Preparation is about full documentation, a complete assessment, and lining up a sponsor.

- **Determine your Impact Level.** Confirm Low, Low+, or Moderate using the Data Classification Tool and your government partners' requirements.
- **Plan for 100% documentation.** Unlike Ready's 50%, Authorized requires your full documentation set completed with your 3PAO.
- **Engage a 3PAO for a SAR.** Authorized requires a full Security Assessment Report, not just a readiness report.
- **Line up a government sponsor early.** Decide whether you'll secure your own sponsor (a CIO or designee from state, local, tribal, territorial, or public higher-education government) or leverage the five-member GovRAMP Approvals Committee.
- **Budget for the Authorized review fee.** See the fee table below.

Annual Revenue	Annual SAR Review Fee paid to the PMO	Monthly ConMon Fees paid to the PMO
< $1 Million	$1,610	$268
$1 – 5 Million	$5,367	$537
> $5 Million	$8,050	$1,073

A Note on Provisionally Authorized Status

A sponsoring government may assign a Provisionally Authorized status when a provider has submitted a package for Authorization consideration and meets most — but not all — requirements. This status may also be recommended if the product relies on interconnected technology(ies) that are not yet GovRAMP or FedRAMP authorized. Providers with Provisionally Authorized status comply with continuous monitoring, and an additional assessment may be required to reach full Authorization.

4. On-Ramp Deep Dives

4.5 Authorized Status

What the Process Involves
Authorized adds full assessment and government sponsorship to the Ready path.

1. **Become a GovRAMP Member**

   Active membership is required before validation, status, or APL listing.
2. **Optional: Submit a Service Request / Security Snapshot**

   A pre-Ready Snapshot provides a gap analysis against the Minimum Mandatory Requirements.
3. **Determine Your Security Category**

   Identify the required Impact Level before engaging a 3PAO or submitting documentation.
4. **Engage a Third-Party Assessment Organization**

   Engage a GovRAMP-approved 3PAO to complete your Security Assessment Report (SAR).
5. **Complete Documentation & Submit the Security Review Request**

   Complete 100% of your documentation, then submit the Security Review Request Form with completed documentation and the Authorized review fee. Your APL status updates to Pending.
6. **Obtain Government Sponsorship or Committee Approval**

   Secure a government sponsor directly, or leverage the GovRAMP Approvals Committee to serve as your appointed sponsor and confirm your package meets all requirements.
7. **Obtain GovRAMP Authorized Verified Status**

   Once the 3PAO attests, all critical controls and inquiries are resolved, and the PMO verifies you meet all mandatory requirements, your APL status updates to Authorized.
8. **Begin Continuous Monitoring**

   Start monthly and annual ConMon submissions per the GovRAMP Continuous Monitoring Guide (see Section 7).

Once You're Verified
Authorized is a living status with the most comprehensive ongoing obligations:

- **Sustain full ConMon.** Monthly scans and POA&M updates, annual control reassessments, incident documentation, and significant change requests all apply (see Section 7).
- **MaintainPMO and sponsor alignment.** Keep the PMO and your sponsoring government (or the Approvals Committee) informed of material changes.
- **Capture reciprocity.** GovRAMP verified products flow to the TX-RAMP list via a weekly sync and are reusable across GovRAMP's participating governments.

4. On-Ramp Deep Dives

LMS COURSE MODULE: Fast Track for Federal Programs

4.6 Fast Track for Federal Programs

Fast Track lets providers reuse the security package and 3PAO audit they've already prepared for FedRAMP. The PMO maps your existing federal documentation — including the RAR or SAR and 90 days of continuous monitoring — to GovRAMP requirements, so you achieve a verified status without starting over. GovRAMP will be piloting 20X-to-GovRAMP pathways in 2026.

The PMO accepts documents in FedRAMP formatting, and most providers onboard within roughly three months. Fees match the standard process.

How to Prepare

Fast Track is about authentication and mapping rather than fresh assessment. Prepare by assembling your federal package.

- **Confirm eligibility.** You qualify if your offering has a federal authorization or is actively pursuing one (FedRAMP Rev. 5 work, or a completed FedRAMP RAR or SAR).
- **Assemble your federal security package.** Gather your federal package, 90 days of continuous monitoring (if applicable), and any required GovRAMP templates — FedRAMP formatting is accepted.
- **Coordinate with your 3PAO.** Your existing assessor can help compile and authenticate the documentation the PMO will review.
- **Plan sponsorship if pursuing Authorized.** Fast Track to Authorized still requires a government sponsor or the Approvals Committee; a federal agency cannot serve as the GovRAMP sponsor unless it is a participating government with GovRAMP.

What the Process Involves

Fast Track collapses the assessment work you've already done into a streamlined PMO review.

1. **Become a GovRAMP Member**

   Membership adds your organization and primary contact to the Member Directory and unlocks the members-only portal.

2. **Engage the GovRAMP PMO**

   Complete a Security Review Request Form to engage the PMO and share details about your company and product ahead of your intake call.

3. **Complete Required Documentation**

   Work with your 3PAO to submit your federal security package, 90 days of continuous monitoring (if applicable), and any necessary GovRAMP templates. FedRAMP formatting is accepted.

4. On-Ramp Deep Dives

4.6 Fast Track for Federal Programs

What the Process Involves (cont.)

4. **PMO Review**

   The PMO reviews your complete package and holds a call with you and your 3PAO to make any final adjustments.

5. **Begin Continuous Monitoring**

   Continuous monitoring maintains your status and APL listing. Providers with a federal authorization may submit their monthly reporting to the GovRAMP PMO unless otherwise specified, and may continue using FedRAMP templates for annual 3PAO packages.

Once You're Verified

Once mapped in, you carry the same ongoing obligations as the equivalent GovRAMP status:

- **Keep monthly reporting flowing.** Submit ConMon to the PMO; federal reporting can often be reused.
- **Mind data-sharing boundaries.** Where federally protected information limits what you can share, the PMO handles the situation case by case to balance federal and state needs.
- **Capture Texas reciprocity.** GovRAMP verified products sync weekly to the TX-RAMP list, satisfying the Texas requirement with minimal extra effort.

Texas Vendors

Texas law requires vendors using a cloud solution to serve the state to be TX-RAMP authorized. By administrative rule, TX-RAMP recognizes GovRAMP with automatic reciprocity, and GovRAMP runs a weekly sync so Authorized products appear on the TX-RAMP list with ease.

5. Picking the Right On-Ramp

There's no single right answer — but there are clearer-fit answers based on your stage, your data, and your contracts. This section walks through three lenses: a quick self-assessment selector, an introduction to data classification, and how data classification maps to GovRAMP impact levels and On-Ramps.

5.1 Start With the Quick Selector

Most providers can identify their most likely starting point with a quick self-assessment. The selector below isn't binding — it's a way to narrow down which On-Ramp deserves your first conversation with the PMO. Many providers mature to higher levels over time.

If you … are brand new to GovRAMP and want to understand your gaps before committing	**Single Security Snapshot**
If you … need to show momentum to government buyers while you mature	**Progressing Snapshot Program**
If you … are an SMB or new-to-government provider wanting credible market entry without 3PAO cost	**Core Status**
If you … are pursuing moderate-risk SLED contracts that expect independent assessment	**Ready Status**
If you … handle moderate/high-impact data, regulated data (CJIS, HIPAA, IRS, SSA), or contracts requiring full Authorization	**Authorized Status**
If you … already hold FedRAMP certification (or are well into the FedRAMP process)	**Fast Track for Federal**

A Reality Check

The Quick Selector reflects your starting preference — but public-sector buyers may have a stronger opinion. If a state, county, or school district has classified the data your product touches at a specific level, they often require a specific GovRAMP status. The next sections explain how that works.

5. Picking the Right On-Ramp

5.2 Why Data Classification Drives Your Decision

The Quick Selector helps you start the conversation. The data your product handles often makes the final decision — because most SLED governments tie cloud security requirements to data classification, not provider preference.

Before a SLED entity publishes a solicitation requiring "GovRAMP Authorized" or "GovRAMP Ready," they're typically making a judgment about the data the system will touch. Understanding how that judgment works — and where your product fits — is the difference between pursuing the right On-Ramp and over- or under-investing.

What data classification is.
Data classification is the process governments use to categorize information based on its sensitivity and the potential harm if it's exposed, altered, or lost. It's the foundation that informs almost every downstream security decision — including which cloud products are allowed to handle that data. Classification typically weighs three questions:

- **Who can lawfully see this data?** Public records vs. employee-only vs. need-to-know vs. legally restricted.
- **What's the regulatory framework?** HIPAA, FERPA, CJIS, IRS 1075, and state-specific privacy laws each carry their own requirements.
- **What's the harm potential?** Inconvenience, financial loss, public safety risk, or serious operational disruption?

5.3 How SLED Governments Typically Classify Data

Most SLED governments use some variation of a four-tier classification scheme. The exact labels differ by jurisdiction, but the underlying logic is consistent.

Tier	What it is	Common Examples
Public	Information explicitly intended for public release — open data, published budgets, meeting agendas, press releases.	Open data, public records, press releases
Internal	For government employee or contractor use; not classified or regulated. Disclosure would be inconvenient but not harmful.	Internal memos, draft policies, routine HR comms
Confidential	Sensitive information whose disclosure could cause real harm. Often subject to state privacy laws or regulatory frameworks.	PII, financial records, student records (FERPA), health data (HIPAA)
Restricted	Highly sensitive information where unauthorized access could cause serious harm. Often legally restricted.	Criminal-justice data (CJIS), tax data (IRS 1075), active investigations, critical infrastructure

5. Picking the Right On-Ramp

5.4 The Technical Anchor: FIPS 199 Impact Levels

Under the hood, GovRAMP measures impact using the federal standard for security categorization, FIPS 199. It evaluates the potential consequences of a breach across three properties: **confidentiality** (disclosure), **integrity** (modification or destruction), and **availability** (loss of access). Each is rated Low, Moderate, or High, and the system's overall level is the highest of the three. That overall rating drives which NIST 800-53 baseline applies — and which On-Ramp realistically fits.

Impact Level	Definition	What it Means	Typical Examples
Low	Limited adverse effect	Minor harm — inconvenience, manageable financial loss, or limited operational impact.	Public-facing services, non-sensitive admin tools
Moderate	Serious adverse effect	Significant operational, financial, or reputational harm. Most SLED workloads handling PII, student, or health data land here.	PII systems, HR platforms, citizen portals, most SaaS handling regulated data
High	Severe or catastrophic effect	Major harm to operations, finances, or individuals — potentially including loss of life or critical-infrastructure disruption.	Public safety, criminal justice (CJIS), emergency response, critical infrastructure

5.5 Mapping Data Classification to On-Ramps

Bringing it together: the table below shows how generic SLED data classifications typically map to FIPS 199 impact levels, and which GovRAMP On-Ramps governments most commonly require or accept for each.

SLED Tier	FIPS 199	On-Ramps That Typically Fit	Notes
Public	Low	Snapshot · Progressing · Core	Reusable validation is usually enough. Full Authorized is rarely required.
Internal	Low–Moderate	Core · Ready	Core often sufficient. Larger or risk-averse buyers may require Ready.
Confidential	Moderate	Ready · Authorized	Where most SLED authorization requirements concentrate. 3PAO assessment expected.
Restricted	Moderate–High	Authorized (often with overlay)	Full Authorization typically required. CJIS data needs the CJIS-Aligned Overlay.

GovRAMP recently developed the following Data Classification Tool and associated worksheet to also assist in creating a better breakdown of data types and associated risk.

5. Picking the Right On-Ramp

Important

These mappings are typical, not universal. Always confirm the specific requirement language in the solicitation or contract — some jurisdictions are stricter than the baseline, some have overlays (like CJIS) that override the general mapping, and some publish their own classification schemes that map differently.

5.6 When the Contract Tells You What to Pursue

Increasingly, SLED solicitations are explicit about which GovRAMP status is required for which data types. If you're responding to a solicitation, the answer to "which On-Ramp?" often isn't yours to choose. Watch for language like:

"Cloud service offerings must hold a current GovRAMP Authorized status…"

What it means: Full Authorized status is required. Core or Ready won't qualify. Plan for 3PAO assessment.

"…or be actively progressing toward authorization with a verified status of Core or higher within 12 months."

What it means: On-Ramp model in play. Core may be enough to bid, but you'll be expected to advance. Common in transitional adoption.

"CJIS-Aligned Overlay required for systems handling criminal justice information."

What it means: Authorized status plus the CJIS overlay — a higher bar than baseline Authorized. Plan accordingly.

"FedRAMP Moderate (or equivalent GovRAMP Authorized) accepted."

What it means: Fast Track is your friend. Existing FedRAMP work can be mapped into GovRAMP without starting over.

When in doubt: ask the procurement contact directly. **"What data classification level will this system touch, and what GovRAMP status is required at that level?"** is a fair, professional question that often saves weeks of misaligned effort.

6. Working With the PMO

Every On-Ramp runs through the same partner: the GovRAMP Program Management Office. Now that you've seen the paths, this section explains who the PMO is, what they do at each stage, and how to get the most from the relationship. Treating the PMO as a strategic partner — not just a gatekeeper — is one of the highest-leverage moves a provider can make.

How Providers Work with GovRAMP

Most providers can identify their most likely starting point with a quick self-assessment. The selector below isn't binding — it's a way to narrow down which On-Ramp deserves your first conversation with the PMO. Many providers mature to higher levels over time.

Membership Team

GovRAMP's Membership Team helps providers identify the best membership tier (see Section 2) as they begin their journey to a verified status and ensures access to the benefits in each tier — helping providers leverage the opportunities and access that membership delivers.

PMO

GovRAMP contracts with RAMPQuest to serve as the GovRAMP Program Management Office (PMO) — the team providers work with on their verified-status efforts. The PMO is your point of contact at every stage:

- **Before assessment:** orientation, On-Ramp guidance, and access to NIST-aligned templates and reference documentation.
- **During the Progressing Snapshot Program:** monthly advisory sessions, quarterly snapshot reviews, and gap-prioritization support.
- **During the Core assessment:** the PMO assesses the product security package directly, with no 3PAO required.
- **During formal assessment:** liaison with your 3PAO, review of your assessment package, and coordination with government sponsors when needed.
- **At verified status:** validation that your product meets the standard for your chosen status, and listing on the APL or PPL.
- **After verification:** ongoing review of continuous monitoring artifacts, significant change requests, and annual control reassessments.

Monthly Office Hours

The PMO also has monthly office hours scheduled the first Wednesday of every month at 2pm ET. Link to access the meeting is available on the GovRAMP Events page.

6. Working With the PMO

What the PMO Does for Providers

- **Reviews and validates assessment packages** across all status levels — including SSPs, RARs, and SARs.
- **Hosts monthly advisory sessions** for Progressing Snapshot participants to work through gaps and prioritize improvements.
- **Provides templates and reference documentation** aligned to NIST 800-53 Rev. 5, MITRE ATT&CK, and the GovRAMP framework.
- **Issues and maintains your verified status** on the APL or PPL, including significant-change reviews.
- **Acts as a liaison** between providers, 3PAOs, and the Approvals Committee (or government sponsor) during authorization.
- **Provides ongoing maturity guidance** after verification, helping you sustain compliance through continuous monitoring.

How to Get the Most Out of the PMO

1. **Engage early.** Talk to the PMO before you choose an On-Ramp — not after you've invested in the wrong one.
2. **Bring questions to advisory sessions.** If you're in the Progressing Snapshot Program, those monthly slots are the highest-value time you have. Come with specific blockers.
3. **Use the templates as-is when you can.** The PMO's reference documents are battle-tested. Custom formats slow review.
4. **Be transparent about gaps.** Hidden gaps surface in 3PAO assessments anyway. The PMO can help you plan around known weaknesses.
5. **Communicate significant changes.** Architecture, ownership, or scope changes need a formal Significant Change Request — surprises after the fact erode trust.
6. **Stay engaged after verification.** ConMon isn't a checkbox. PMO guidance helps you keep pace as NIST evolves.

7. Continuous Monitoring

A point-in-time verification tells governments your security posture was strong on a specific date. Continuous Monitoring (ConMon) tells them it's still strong today. ConMon is a fundamental GovRAMP differentiator — and once you achieve a verified status, it becomes the bulk of your ongoing GovRAMP work.

Monthly

Vulnerability Scan Results
Authenticated scans of operating systems, web applications, and databases — submitted with remediation tracking for any findings.

POA&M Updates
Plan of Action & Milestones updates tracking every open weakness, planned remediation, and status change since the last report.

Annual

Control Assessments
A defined subset of controls is reassessed each year on a rolling basis, ensuring full coverage over the assessment cycle.

As Needed

Incident Documentation
Security incidents are documented and reported per GovRAMP requirements, including impact, response, and lessons learned.

Significant Change Requests & Notifications
Significant Change Requests - Architecture, scope, ownership, or major control changes require formal review before they take effect in the authorized boundary.
Significant Change Notifications – notification of a significant change post-implementation.

Ongoing

Vulnerability Deviation Requests
Formal requests for any deviation from standard scanning requirements — with justification and compensating controls.

Note

Core status uses a lighter quarterly ConMon cadence (vulnerability scans, POA&M updates, and asset inventories), while Ready, Provisionally Authorized and Authorized follow the monthly and annual cycle above.

7. Continuous Monitoring

Building a Sustainable ConMon Practice

The providers who handle ConMon well treat it as a routine engineering function, not a quarterly fire drill. A few principles that consistently pay off:

- **Automate evidence collection.** Scan exports, ticket data, and configuration baselines should flow into your ConMon submissions automatically wherever possible.
- **Own POA&Ms in real time.** Don't let weaknesses age. Every open POA&M with a stale date erodes confidence with the PMO and sponsoring agencies.
- **Plan annual assessments early.** Know which controls are coming up for reassessment 90 days in advance, not 30.
- **Build incident reporting into your IR runbook.** Make GovRAMP notifications part of standard incident response, not a separate workflow.
- **Treat significant changes as a planning input.** Loop in the PMO during architecture reviews — not after the change is deployed.

8. Resources & Next Steps

Direct links to the official GovRAMP resources referenced throughout this guide.

- Membership Pricing
- Service Providers
- Small Business Resources
- Approved 3PAOS
- Single Security Snapshot
- Progressing Security Snapshot Program
- Core Status
- Ready Status
- Authorized Status
- Fast Track Program
- Program Participants (APL & PPL)
- Templates & Resources
- Data Classification Tool
- Continuous Monitoring Guide

Start Where you Are

You don't have to start at Authorized. You don't even have to know which On-Ramp is right yet. **The single most important step is becoming a member — that's what unlocks the PMO conversation, the templates, the snapshot tools, and the visibility that makes everything else possible.** From there, GovRAMP is designed to grow with you. Wherever you are in your security journey, there's a path forward that fits.

Glossary of Key Terms

3PAO *Third-Party Assessment Organization*	An accredited independent assessor that conducts GovRAMP assessments and produces the RARs and SARs used to validate Ready and Authorized statuses.
APL *Authorized Product List*	GovRAMP's daily-updated public list of products with a verified Core, Ready, Provisionally Authorized, or Authorized status.
ATO *Authorization to Operate*	A formal, risk-based government approval allowing a system to operate within a specific environment.
ConMon *Continuous Monitoring*	Ongoing security activities required to maintain a verified status, including scans, POA&M updates, reassessments, and change notifications.
GET *Government Engagement Team*	The GovRAMP team that supports government organizations with policy adoption, procurement alignment, and change management.
NIST SP 800-53 Rev. 5 *NIST Special Publication 800-53, Revision 5*	NIST's catalog of security and privacy controls. GovRAMP uses selected controls to establish Low, Moderate, and High baselines.
PMO *Program Management Office*	The RAMPQuest-operated team that guides providers through GovRAMP's Security Program, reviews submissions, and supports ongoing monitoring.
POA&M *Plan of Action & Milestones*	A document tracking security weaknesses, planned remediation steps, and target completion dates.
PPL *Progressing Product List*	GovRAMP's public list of products participating in the Progressing Security Snapshot Program and working toward a verified status.
PSS / PSSP *Progressing Security Snapshot / Program*	A structured program providing PMO guidance to help providers improve their security maturity. Participating products appear on the PPL.
RAR *Readiness Assessment Report*	A 3PAO report assessing whether a product meets the requirements for Ready status.
SAR *Security Assessment Report*	A 3PAO report documenting a full security assessment and supporting authorization decisions.
SLED *State, Local, Tribal, Territorial & Education*	The public-sector market served by GovRAMP, distinct from the federal sector.
Sponsor	A government official or the GovRAMP Approvals Committee that reviews a product's security package and PMO recommendation to confirm authorization requirements have been met.
SSP *System Security Plan*	The primary document explaining how a provider implements required NIST controls within its system.



GOVRAMP.ORG | INFO@GOVRAMP.ORG | LINKEDIN.COM/COMPANY/GOVRAMP

© 2026 GovRAMP
All content, concepts, and designs contained within this document are the intellectual property of GovRAMP and its creative collaborators. Reproduction, distribution, or adaptation without express written permission is strictly prohibited.