GovRAMP Overview

State of Nevada – Agency

October 2026

Why does GovRAMP Exist?

Standardizing Cybersecurity to Reduce Burden, Improve Risk Visibility, and Enable a "Verify Once, Serve Many" Model

As Cyber Threats Grow, How Do You Know…



If a cloud solution that is being used to deliver services that transmit, store, and/or process your data ***could impact security***?



If bidders meet minimum security standards ***before*** making an award for contract?



If a contracted product complies with your security standards ***throughout the duration of the contract***?

What is GovRAMP?

Creating a framework for continuous improvement in cybersecurity for state & local governments, providers, and the constituents they serve.

Government Risk Authorization Management Program

Who We Are

A 501(c)(6) nonprofit membership organization that supports state, local, federal, educational, tribal, and nonprofit organizations **in securely adopting cloud technologies**.

A Government Engagement Team (GET) and Program Management Office (PMO) working to **advance cybersecurity standards and procurement efficiency** for our participating organizations.

What We Do

Establish a **standardized, streamlined security verification process** for cloud service providers.

Maintain an Authorized Product List of cloud products that meet GovRAMP's security standards.

Serve as a no-cost, trusted partner for SLED agencies.

How We Do It

Leverage NIST 800-53 Rev. 5 framework to assess and verify security of cloud products.

Facilitate a **shared security assessment process** to reduce redundancy and increase procurement efficiency.

Provide transparency through continuous monitoring.

Support governments throughout every step of the GovRAMP adoption process.

GovRAMP's Security Framework

GovRAMP's baseline requirements are built on NIST 800-53 Rev. 5. that aligns with NIST Cyber Security Framework (CSF)

This streamlined, comprehensive authorization process:

- Reduces barriers to security for all sizes of service providers
- Minimizes the cost of security compliance for all service providers
- Provides governments a shared resource for procurement and continuous compliance & monitoring

Incorporating GovRAMP's assessment options of Progressing Snapshot, Core, Ready, Provisionally Authorized, or Authorized at the appropriate Impact Level can help you build out your RAMP program.

Find policies, templates, and resources online at: GovRAMP.org/document-library



GovRAMP Impact Levels

- Not every contract requires GovRAMP authorization status. The key to determining security requirements is assessing the type of data a vendor processes, transmits, or stores.
- The **Cloud Procurement Resource Tool** and **Data Classification Tool** help identify the necessary GovRAMP security requirements for cloud service providers that handle government data.
- GovRAMP has defined the following Impact Level Categories that align to NIST 800-53:

Low

GovRAMP Low Control Baselines

Moderate

GovRAMP Moderate Control Baselines

High

GovRAMP/FedRAMP High Control Baselines

GovRAMP Security Program Risk Acceptance Model

KEY

NIST* – National Institute of Standards and Technology
PMO* – Program Management Office (RAMPQuest)
ConMon* – Continuous Monitoring
3PAO* – Third Party Assessment Organization

Moderate Impact

Security Snapshot

Cyber NIST score of 40 controls

Moderate Impact

Progressing Security Snapshot

Cyber NIST score of 40 controls, monthly advisory, and quarterly snapshot updates

Moderate Impact

Core Status

Demonstrates achievement with assessment of 60 NIST controls by PMO, quarterly ConMon, and documentation

Low, Moderate, and High Impact

Ready Status

Demonstrates achievement with Ready audit of 80 NIST controls by 3PAO, monthly ConMon, annual assessment, and documentation

Low, Moderate, and High Impact

Authorized or Provisionally Authorized Status

Demonstrates achievement with security audit of 319 (mod) NIST controls by 3PAO, monthly ConMon, annual assessment, and documentation

Assessment & validation conducted by PMO

Assessment by 3PAO with PMO validation & ConMon

GovRAMP Program Offerings

Single Snapshot

Achievable in 3-6 Weeks

The evidence-based GovRAMP Security Snapshot helps service providers start their cybersecurity journey, while offering governments a first look at cloud products' risk maturity. It validates the product's maturity by examining the top 40 most impactful controls determined by MITRE's ATT&CK® Framework as the basis. The Security Snapshot is valid for a period of 12 months from the date of issuance and may be leveraged by multiple organizations during that time period.

Process:

1. Membership
2. Complete initial GovRAMP Security Snapshot

Progressing Snapshot

First Snapshot Achievable in 3-6 Weeks

A major goal of the GovRAMP Progressing Security Snapshot Program is enhancing cyber maturity among providers and fostering information sharing that facilitates effective government risk management by integrating the principles of "trust but verify" and a consultative approach.

The program includes quarterly assessments (Snapshots) and monthly consultative calls with the GovRAMP PMO Advisory team. Service providers gain insight into their products' gaps in achieving NIST-based security controls and guidance on how to best address those gaps, with a focus on what matters most for improved security outcomes.

Process:

1. Membership
2. Complete initial GovRAMP Security Snapshot
3. Complete monthly consultative calls with GovRAMP PMO Advisory team

GovRAMP Program Offerings

GovRAMP Core

Achievable in 12 Months

The GovRAMP Core security status provides an early step in verified GovRAMP statuses to demonstrate the maturity of a cloud product's security program. This early step demonstrates achievement of baseline NIST 800-53 Rev. 5 controls and documentation requirements as assessed and validated by the GovRAMP PMO. The provider may optionally submit a Pen Test. Like other GovRAMP verified statuses, the Core Status is valid for 12 months and may be extended for an additional 12 months by undergoing an annual assessment prior to the status expiration. There is no limit to the number of extensions a product may obtain.

To maintain a GovRAMP Core security status, the provider must comply with quarterly continuous monitoring requirements that include submission of evidence of Core requirement compliance as requested by the GovRAMP PMO, in addition to Web App Scans, Vulnerability Scans, Policy Compliance Scans and a POA&M spreadsheet.

GovRAMP Ready

Achievable in 12-18 Months

A Ready status indicates that the product meets GovRAMP's Minimum Mandatory Requirements and most critical controls. The Ready requirements are published here and vary by Impact Level for Low, Moderate, or High. The security package for Ready includes a Readiness Assessment Report (RAR) submitted by a GovRAMP 3PAO, attesting to the minimum mandates. The required Ready documentation, including boundary diagram, inventory worksheet, roles, and permissions matrix, must be included in the security package provided to our Security Team through the GovRAMP Program Management Office (PMO). The GovRAMP PMO provides independent validation and verification that the security package and RAR comply with the standards established by the GovRAMP governing board and committees.

GovRAMP Program Offerings

GovRAMP Provisionally Authorized

Achievable in 18-24 Months

A Provisionally Authorized status may be assigned by a sponsoring government or Approvals Committee to a package submitted for Authorized Status, if the product meets the Authorization requirements, but one of the product's interconnected technologies is not GovRAMP or FedRAMP Authorized. To achieve Provisionally Authorized, the interconnected technology must leverage a current GovRAMP Security Snapshot.

GovRAMP Authorized

Achievable in 18-24 Months

An Authorized Status indicates the product or offering meets all the required NIST controls by impact level and the provider has completed the necessary documentation, including a 3PAO Security Assessment Report. To obtain Authorized status, a security package needs approval from the Approvals Committee or a Government Sponsorship. They will serve as authorization officials and confirm the package meets GovRAMP requirements.

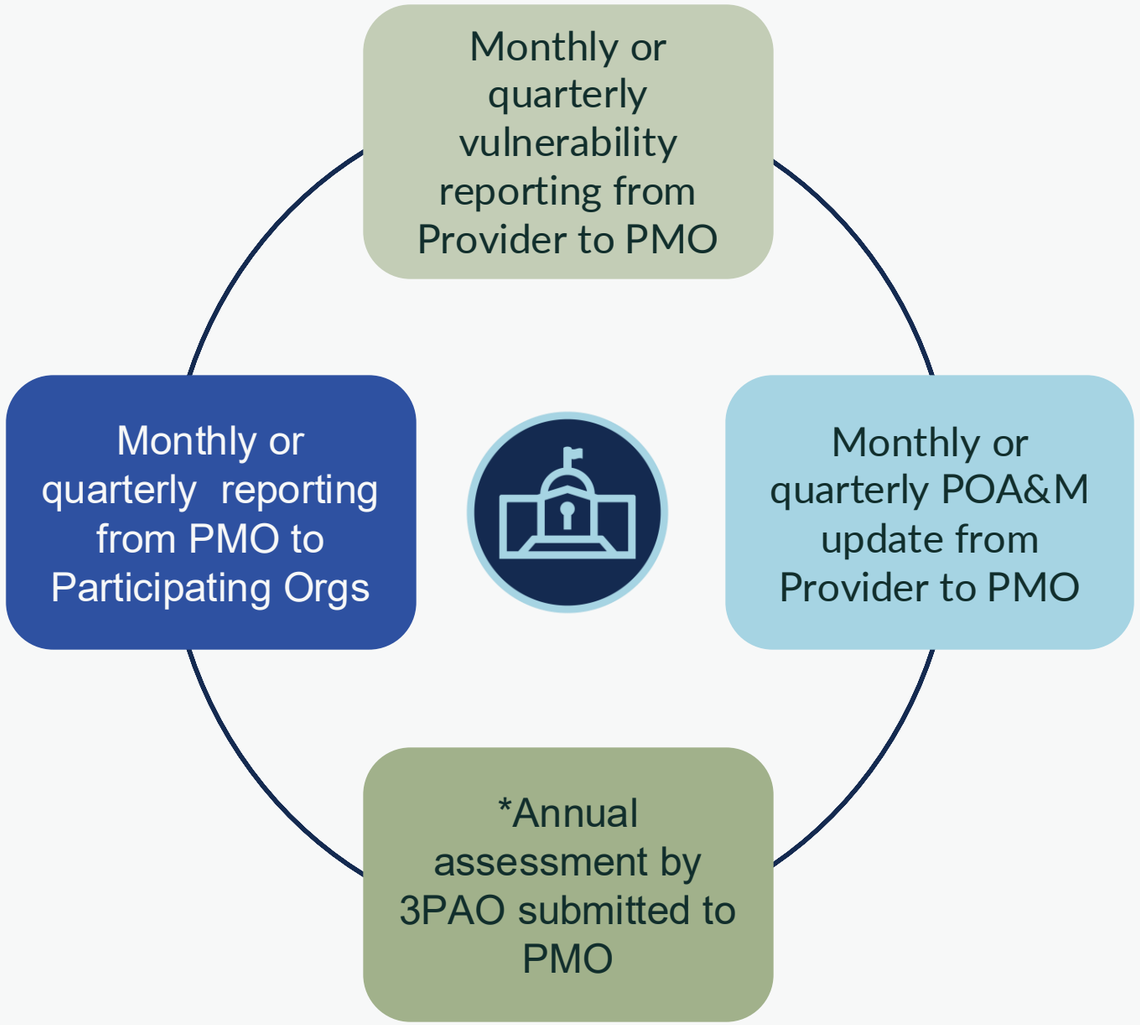
CJIS Overlay

GovRAMP CJIS-Aligned Overlay Control and Parameters - GovRAMP

For criminal justice agencies ensuring that cloud-based solutions meet CJIS standards is critical to protecting sensitive data. The CJIS-Aligned Overlay streamlines the path to conformance, enabling service providers to deliver secure, compliant solutions while reducing the burden on government decision-makers.

The overlay provides essential guidance for service providers by:

- **Streamlining the Assessment Process**: The overlay consolidates CJIS requirements with GovRAMP's existing framework, reducing redundancy and confusion.
- **Providing Clear Direction**: Each control is mapped to CJIS Policy 6.0, offering straightforward guidance on how to implement and assess compliance.
- **Facilitating Informed Decision-Making**: By clarifying a product's CJIS conformance, the overlay empowers agencies to evaluate cloud solutions confidently.



Continuous Monitoring

Providers must comply with Continuous Monitoring (ConMon) requirements to maintain the status of Core, Ready, Authorized, or Provisionally Authorized.

Providers may grant viewing access to Participating Governments at the Standard Access level or the Elevated Access level.

View GovRAMP policies that establish our security standards & requirements here: **govRAMP.org/document-library**

GovRAMP Fast Track Program

To expedite the process of achieving a verified GovRAMP status for FedRAMP Rev. 5 products, organizations can enroll in the GovRAMP Fast Track Program.

Benefits:

- No need to re-engage a 3PAO, you may submit the same FedRAMP security package for review even if the FedRAMP review process has not been completed.
- Only required to cover the cost of membership, the GovRAMP PMO technical review and continuous monitoring fees.
- Allows participating organizations to meet continuous monitoring requirements where FedRAMP does not provide continuous monitoring visibility to non-federal agencies.
- GovRAMP does not require a government sponsor or contract in order to receive a verified status.
- Turnaround time is 6-8 weeks from date product entered the GovRAMP PMO queue but may be longer based on the quality of the package submission and/or the number of products in queue ahead of you (including those waiting for approvals committee review).

Benefits of GovRAMP Adoption

One standard. One framework. One secure repository. One continuous monitoring process.

Benefits for Government

- Reduced procurement timelines
- Consistent, reuseable risk decision
- Standardized security expectations
- Continuous monitoring across contract lifecycle

Benefits for Providers

- Verify once, serve many customers
- Lower compliance and audit costs
- Clear, predictable security requirements
- Expanded access to government markets

GovRAMP & Nevada

Overview of Nevada's GovRAMP Adoption and state-specific resources

Nevada's Adoption

Key Transition Milestones:

July 1, 2026 – Requirements Take Effective

- New cloud contracts must align with GovRAMP requirements.
- Vendors must achieve at least GovRAMP Core status, with an on-ramp period available to reach the required level.

July 1, 2028 – Transition Period Ends

- New cloud contracts must continue to meet GovRAMP requirements.
- The on-ramp period ends; vendors must meet the required GovRAMP status at contract award as specified in the solicitation or contract.

01. July 1, 2026

02. July 1, 2028

Requirements Effective

Applies to new cloud contracts

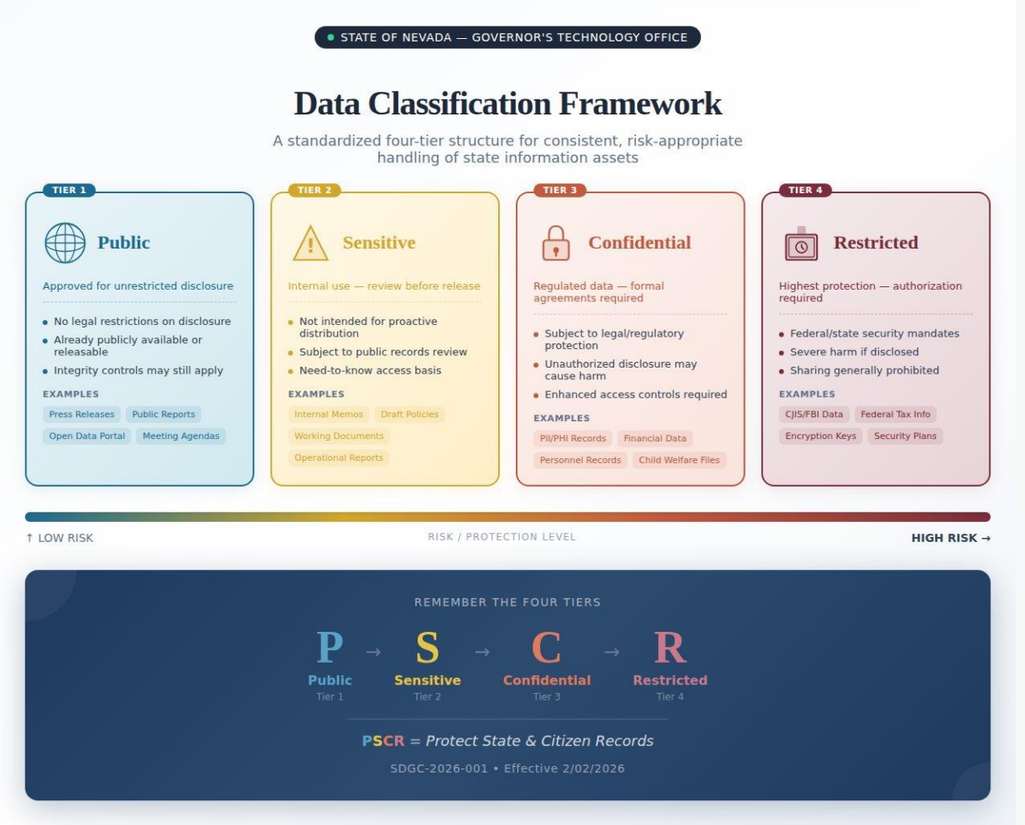
Transition Period Ends

The on-ramp period ends; vendors must meet the required GovRAMP status at contract award as specified in the solicitation or contract.

Data Classification

For additional information, please review:

[State of Nevada’s Statewide Policy for Data Classification (SDGC-2026-001)]



Onboarding Providers

How vendors get started with GovRAMP

Getting Started with GovRAMP

Membership & Security Program: Key steps for cloud service providers pursuing a GovRAMP authorization.

Email info@govramp.org

Join today at Private Sector Membership | GovRAMP

Step 1: Join	Join GovRAMP and establish your organization within the program. Join GovRAMP and establish your organization within the program.
Step 2: Identify	Work with the GovRAMP PMO (RAMPQuest) to determine the most appropriate authorization path for your cloud offering.
Step 3: Prepare	Receive guidance, resources, and support from the GovRAMP PMO to help you navigate the authorization process.
Step 4: Assess	Document and assess security controls to demonstrate alignment with GovRAMP requirements
Step 5: Advance	Advance through your selected authorization path with ongoing support and engagement from the GovRAMP PMO.



State of Nevada & GovRAMP

Why GovRAMP?

Protecting Nevada's most sensitive and critical information is crucial to operational resiliency. While cybersecurity teams work non-stop to protect and defend networks and systems from bad actors, threats are always changing. Firms must be proactive by strengthening those networks and systems. One way to accomplish this is by ensuring providers and products with any critical data are meeting minimum cybersecurity standards. This is where GovRAMP comes in.

The State of Nevada is working towards a standardized approach to the security assessment of cloud computing services. GovRAMP has partnered with the State of Nevada to assist providers with ensuring that their products are meeting those minimum-security controls as indicated by GovRAMP in accordance with the NIST 800-53 security controls, while also affording them the benefit of transferable credentials through standardized cybersecurity verification. GovRAMP allows providers to **verify once to serve many** while also simplifying the procurement process and expediting the time to contract. Product cybersecurity validation can be used with any of our participating government members.

New Cloud Product Requirements

The State of Nevada's Government Technology Office (GTO) ensures that all executive branch offices utilizing cloud services meet strict security standards. In an effort to create a standardized process and provide resources to its agencies, the GTO has leveraged the GovRAMP framework for authorization and continuous monitoring to protect the confidentiality, integrity and availability of state information.

As of July 1, 2026, all new contracts containing a cloud component will include risk assessment requirements that align with the GovRAMP program which is based on National Institute of Technology and Standards (NIST) 800-53 (Rev 5). At minimum, products must achieve a GovRAMP Core status. In some cases, based on data type, a GovRAMP Authorized/Provisionally Authorized status may be required. Nevada will provide an "on ramp" that allows vendors time to achieve the required status under the contract. Exact details on the requirements for each contract will be outlined in the purchasing mechanism or associated contract.

Please note as of **July 1, 2028**, contracts will contain the requirements outlined above without an "on ramp."

Additional details on Nevada's information security policies will be available soon.

Nevada's Program Page

A centralized resource for state-specific GovRAMP Requirements, guidance, and implementation support.

The Program Page provides access to:

- Announcements
- Document Library
- Training Library
- Points of Contact
- GovRAMP Requirements
- Resource Links

Visit the GovRAMP Nevada Program Page

Questions?

Email our team at get@govramp.org.
Thank you!