GovRAMP

NASPO
National Association of
State Procurement Officials

Procurement Cloud Security Resource Tool

Guiding SLED Organizations in Procurement Best Practices for Cloud Service Providers

December 2025

A PROCUREMENT TOOLKIT CREATED BY THE NASPO/GOVRAMP PROCUREMENT TASK FORCE

Table of Contents

ABOUT GOVRAMP

Founded at the beginning of 2020, GovRAMP was born from the clear need for a standardized approach to the cybersecurity standards required from service providers offering solutions to state and local governments.

GovRAMP is a registered 501(c)(6) nonprofit membership organization comprised of service providers offering IaaS, PaaS, and/or SaaS solutions, third party assessment organizations, and government officials. Our members lead, manage, and work in various disciplines across the United States and are all committed to making the digital landscape a safer, more secure place.

Cloud Procurement Frequently Asked Questions

What is the cloud?

Cloud refers to cloud computing solution provided by a service provider that delivers on demand computing services over the internet. As defined by the National Institute of Standards and Technology (NIST):

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud computing solutions are separated by the services provided for the cloud service model, such as software, platform, or infrastructure. Before undertaking cloud procurements, organizations must understand the service model to be acquired and the business objectives or challenges to be solved. The organization and service provider's responsibilities and contract terms and conditions will vary based on the service model and objectives.

Analogy: Owning a Power Plant vs. Buying Electricity

Imagine your organization needs electricity. You have two options:

- Option 1: Build and maintain your own power plant. You buy the land, purchase equipment, hire engineers, and handle maintenance. It's expensive, time-consuming, and you pay for full capacity even if you don't use it all.
- Option 2: Buy electricity from the utility company. You pay only for what you use, scale up or down as needed,
- and the utility company handles all the infrastructure, maintenance, and upgrades.

Cloud Computing Works the Same Way

Instead of building and maintaining your own IT infrastructure (servers, storage, networking), you consume computing resources as a service from a cloud provider. This gives you:

- Cost Efficiency: Pay for what you use, not for idle capacity.
- Scalability: Instantly adjust resources to meet demand.
- Reliability: Providers handle maintenance, security, and compliance.
- Focus: Your team spends time on mission-critical work, not hardware upkeep.

Cloud computing is essentially utility-style IT—you consume computing power like electricity: on-demand, scalable, and managed by experts.

Why This Matters for Procurement

- Cloud is not just hosting; it's a service model with specific attributes.
- Contracts should reflect these characteristics to ensure scalability, security, and compliance.
- Understanding NIST's definition helps avoid misclassifying traditional IT services as "cloud."

What cloud services does procurement handle?

Procurement officials help organizations procure various cloud solutions, from web applications for email to platforms to develop and run custom-built software. Three common cloud services are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Software as a Service allows an organization to use a service provider's applications that run on a cloud infrastructure. Customers access the applications through web browsers or program interfaces. Platform as a Service allows an organization to run self-developed and acquired applications using programming languages and tools from a service provider. Infrastructure as a Service provides organizations with the capability to provision processing, storage, networks, and computing resources to control and run applications and systems. GovRAMP currently assesses SaaS, Paas, and IaaS products.

While the three services mentioned are common, various services are available in the cloud. These ever-evolving services put a finer point on the type of service provided. Still, each service typically fits within the three service models NIST defines. Procurement officials may see XaaS referenced, which refers to anything as a service; however, not all XaaS are cloud solutions. In addition, Cybersecurity as a Service (CSaaS) allows a third-party to monitor an organization's risk posture and provide expertise.

Considerations must also be made for professional services contracts where the service provider relies on cloud-based products to manage government data. For example, a health benefits provider may not own the cloud platform that stores your organization's employee information, but the platform they use should still comply with your organization's established security standards for cloud solutions. This ensures that sensitive data remains protected, regardless of whether the cloud product is directly procured or accessed through a third-party service.

Who are the key stakeholders in a cloud service procurement?

Security affects teams across an organization and with change management already being cumbersome, making decisions in a vacuum may complicate the procurement process. Here are some key stakeholders, their roles, and why their participation matters:

1. Information Security

- **Role:** Ensures the cloud solution meets organizational security requirements and complies with applicable regulatory standards.
- **Why Included:** They assess risks related to data confidentiality, integrity, and availability. Their input determines which security controls and assessment level (Low, Moderate, High) are necessary.

2. Procurement

- **Role:** Manages the acquisition process, contract terms, and vendor selection.
- **Why Included:** Procurement ensures that security requirements are embedded in the contract language and that vendors commit to compliance milestones. They also verify pricing and service-level agreements align with security obligations.

3. Risk Management

- **Role:** Evaluates organizational risk exposure and ensures alignment with enterprise risk appetite.
- **Why Included:** They help weigh the impact of using a cloud service without full authorization and guide decisions on interim solutions (e.g., Progressing Snapshot) versus waiting for full assessment.

4. General Counsel

- **Role:** Provides legal oversight on compliance, liability, and regulatory obligations.
- **Why Included:** Counsel ensures contracts include enforceable security clauses, breach notification requirements, and remedies for non-compliance. They also address data sovereignty and privacy laws and can provide valuable insight.

5. Vendor Management

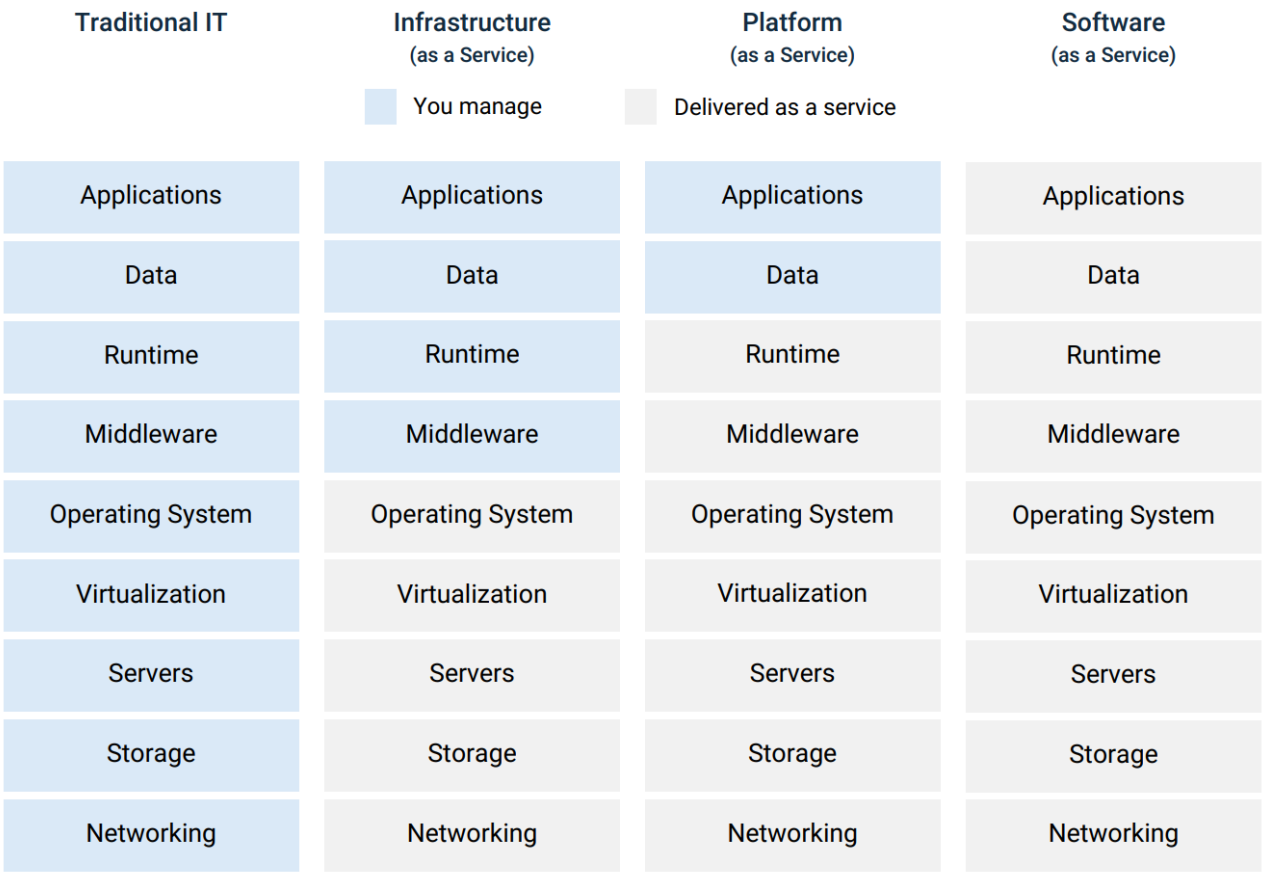
- **Role:** Oversees ongoing vendor performance and compliance throughout the contract lifecycle.
- **Why Included:** They monitor progress toward security milestones, manage reporting obligations, and ensure transparency from onboarding through continuous monitoring.

Does the type of cloud service shape a procurement?

Yes! Each cloud service model provides different services, which means organizations' and service providers' responsibilities will differ based on the service procured. The responsibility associated with each cloud service will require procurements of all types to be specific in the roles and responsibilities of each party. A question that often arises is, “If a SaaS solution/product is built on GovRAMP/FedRAMP Authorized infrastructure, then the SaaS solution doesn’t have to comply with GovRAMP because it’s infrastructure or platform is already in compliance, right?” No,

GovRAMP assessments apply to each service offering, not just the infrastructure it sits on. While a SaaS product may inherit certain security controls from its underlying platform, compliance does not end there!

Each GovRAMP security package includes a Control Responsibility Matrix (CRM), which requires the cloud provider to specify which controls are implemented directly, which are inherited from other layers of the cloud stack, and which are the responsibility of the customer, or a shared responsibility among these parties. Find the CRM here.



Guide to the Shared Responsibility Model

User's responsibility Service Provider's responsibility

	Saas Dropbox, Salesforce CRM, Zoom, Microsoft 365, Google Workspace	Paas Microsoft Azure App Service, AWS Elastic Beanstalk, Google Kubernetes Engine, Red Hat OpenShift	Iaas Microsoft Azure, Amazon Web Services (AWS), Google Compute Engine (GCE)
Applications	Service Provider	User	User
Middleware	Service Provider	User	User
Virtualization	Service Provider	Service Provider	User
Data	Service Provider	Service Provider	User
O/S	Service Provider	Service Provider	User
Networking	Service Provider	Service Provider	User
Runtime	Service Provider	Service Provider	User
Servers	Service Provider	Service Provider	Service Provider
Storage	Service Provider	Service Provider	Service Provider

By integrating GovRAMP in their organizations, states can utilize GovRAMP template language for solicitations and contracts. Organizations must ensure that their contract clauses address data security and privacy. The Center for Digital Government published the Best Practice Guide for Cloud and As-A-Service Procurements. The guide contains a clause comparison matrix that offers a glimpse into the difference the cloud solution makes in the wording used. Organizations that have yet to implement GovRAMP, FedRAMP, or a RAMP program can find value in the Best Practice Guide for Cloud and As-A-Service Procurement.

Who is responsible for identifying data types?

Understanding data types is primarily the responsibility of those who work with data, such as data owners, software developers, data analysts, and database administrators. These professionals need to know how data is stored, processed, and transferred. However, it is critical that procurement professionals involve these data owners early in the procurement process.

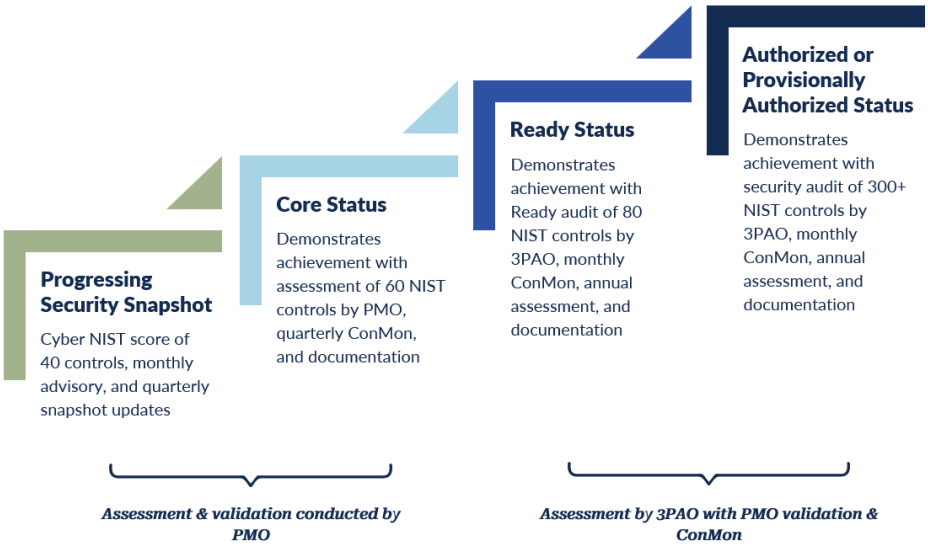
Data owners handle data classification in liaison with other data professionals such as data analysts and database administrators. These individuals are responsible for organizing data into easily understood and used categories. For example, they might classify data based on its sensitivity (e.g., public or confidential) or type, such as customer information or sales data, HIPPA, or Privacy Data (personally identifiable information, PII).
By doing this, data professionals help ensure that the data is appropriately managed, protected, and utilized. This classification helps organizations make better decisions, protect sensitive information, and comply with legal and regulatory requirements.

Organizations can make more informed decisions that ensure their procurements align with organizational data strategies and mitigate potential data and privacy-related challenges by involving the data compliance officer to provide information on data requirements, quality standards, and potential data-related risks. The key objective is to have the appropriate business, security, and IT professionals involved at the conception phase of a potential procurement to identify the system, security, and data privacy requirements.

How does a vendor prove data security and privacy?

Vendors can provide assessments to organizations; however, the type of assessment matters and organizations must understand what they consider acceptable. One way organizations can increase their cybersecurity maturity is to implement a Risk and Authorization Management Program (RAMP). Depending on what type of program an organization establishes, it would detail what type of assessments they accept, such as FedRAMP, GovRAMP, a third-party attestation, or a self-assessment by the vendor. Each option has its pros and cons, but there are many benefits to contracting with vendors who hold a GovRAMP authorization or who are engaged in the GovRAMP security program. One benefit is that vendors must maintain and validate the security posture of their service offering(s) through quarterly scores or Continuous Monitoring and, where a verified status has been achieved, they must have an annual assessment completed by either the GovRAMP PMO or a third-party assessment organization to retain their verified status. The table below illustrates the GovRAMP Security Program steps.

GovRAMP Security Program Risk Acceptance Model



How do FedRAMP, GovRAMP, and RAMP differ?

FedRAMP (Federal Risk and Authorization Management Program) is a government-wide program that standardizes the security assessment, authorization, and continuous monitoring of cloud products and services. It provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by federal agencies.

GovRAMP (Government Risk and Authorization Management Program) is similar to FedRAMP but tailored explicitly for state, local, tribal, and territorial government agencies. GovRAMP provides a standardized approach to cloud security assessment and authorization for state and local governments, enabling them to adopt cloud technologies more efficiently and securely.

RAMP (Risk and Authorization Management Program) is a broader term encompassing FedRAMP, GovRAMP, and similar national, state, or local programs. RAMP programs aim to streamline and standardize the security assessment and authorization processes for cloud products and services across various government entities, ensuring consistency and adherence to security standards.

GovRAMP and FedRAMP

	GovRAMP	FedRAMP
Based on NIST 800-53 Rev. 5	✓	✓
Requires annual independent Third Party Assessment Organization (3PAO) assessment	✓	✓
Requires Monthly Continuous Monitoring	✓	✓
Impact Levels of Low, Moderate, and High	✓	✓
Verified statuses of Ready and Authorized	✓	✓
Available to any provider, regardless of federal contract status	✓	X
Documentation available to federal, state, local, public education institutions, and special districts	✓	X
Centralized PMO reviews all security packages to ensure consistent application of standards and verification	✓	X
Fast Track option for products with FedRAMP or GovRAMP	✓	X
Plans for mapping to other compliance frameworks: CJIS, MARSE, MMIS, IRS	✓	X
Nonprofit mission to improve cyber posture for state, local, public education institutions and special districts and providers who serve them	✓	X
Core Status and Progressing Snapshot	✓	X

How can procurement, data security, and privacy align?

Organizations can take the first step in aligning data security, privacy, and procurement by harmonizing procurement language and security policies, standards, and controls to eliminate conflicts and redundancies. In public procurements, general conditions, special conditions, requirements, and specifications are often layered into the solicitation package. When adopting new controls, reviewing other terms and conditions in the procurement is essential to avoid ambiguity and ensure the desired outcomes.

Adopting the most current version of NIST 800-53 as baseline controls for cloud services is another way organizations can align procurement, data security, and privacy. Avoiding customization, one-off controls, and incorporating a RAMP or

RAMP service in cloud procurements will provide more substantial, manageable security measures. Providing clear and specific controls a service provider must conform to during the contract enables all parties to ensure data security and risk management remain a priority throughout the contract's life.

By changing the procurement infrastructure and acquisition policies and processes with cloud service governance and risk authorization and management practices, organizations can position themselves to procure services that fall within their risk tolerance. Piloting and implementing continuous monitoring by qualified auditors for cloud service control compliance protects the public's interest and enables organizations to use as-a-service solutions more securely.

What to include in a procurement for a cloud service?

The following solicitation checklist is from the Center for Digital Government Best Practice Guide for Cloud and As-A-Service Procurements, which can help organizations when procuring cloud services through solicitations as well as other procurement methods.

Solicitation Checklist

- ☐ What is the cloud security, data and privacy standards, and controls that the service provider must meet?
- ☐ What level of RAMP authorization (impact levels) must the service provider meet?
- ☐ What status level must the service provider product meet (GovRAMP pending, authorized, etc.)?
- ☐ When must the service provider achieve this status level?
- ☐ What is mandatory for compliance and what is subject to negotiations?
- ☐ What is the basis upon which the jurisdiction will consider exceptions?
- ☐ Has the solicitation been reviewed for redundancy and conflicts in terms and conditions and any security controls and requirements?
- ☐ Will resellers be eligible for awards?
- ☐ If resellers are eligible for awards, are there flow down requirements that will place sufficient compliance and performance obligations on the ultimate service provider providing the resold product or service?
- ☐ If resellers are eligible for an award, are they required to resell FEDRAMP and/or GovRAMP authorized offerings and, if so, does the authorization apply specifically to the cloud service products involved in the solicitation?
- ☐ Is there a process to negotiate terms and conditions with the service provider providing the product sold by the reseller?

Additional Resources

Center for Digital Government Best Practice Guide for Cloud and As-A-Service Procurements – Specifically, Appendix 7 Clause Comparison Matrix

NASPO

National Institute of Standards and Technology Glossary for IT definitions

GovRAMP

IRS 1075

Payment Card Industry Data Security Standard (PCI DSS)

Criminal Justice Information System (CJIS)

Health Insurance Portability and Accountability Act (HIPAA)

Family Educational Rights and Privacy Act (FERPA)

European Union General Data Protection Regulation (GDPR)

Gramm Leach Bliley Act (GLBA)

Controlled Unclassified Information (CUI)

Minimum Acceptable Risk Standards for Exchanges (MARS-E)

Better Data Security Though Classification: A Game Plan for Smart Cybersecurity Investments – NASCIO

NASCIO Resource Center

Buyer Be Aware – Integrating Cybersecurity into the Acquisition Process

Data Classification Tool

Introduction and Purpose

This document is intended to be used by state and local governments and procurement officials as a tool for determining the appropriate GovRAMP security requirements in procurements with the intent of procuring a service provider using or offering Infrastructure as a Service (IaaS), Software as a Service (SaaS), and/or Platform as a Service (PaaS) solutions that process, store, and/or transmit government data and any related information as defined by NIST 800-53, These include Personally Identifiable Information (PII), Personal Health Information (PHI), Payment Card Industry (PCI), and Criminal Justice Information (CJI). Identifying the data classification aids the Member Organization (Organization) in maintaining the security, confidentiality and integrity of their data in alliance with its governing body.

According to the Federal Information Security Management Act (FISMA) requirements, there are three distinct security objectives for information and information systems: confidentiality, integrity, and availability. These standards are used as the foundation to ensure vendors are providing solutions that meet the minimum security requirements to process, store, and transmit certain types of government data and any related information.

It is necessary for the Organization, as defined by the GovRAMP Bylaws, to accurately determine their required security baseline prior to publishing a procurement so that the Organization can select a vendor that meets the government's needs and provides the appropriate security controls to protect the government data. The determination to which procurements this process should apply should be based on the Organization's policies and/or standards. Procurement should partner with the information security team, Chief Information Officer, and Chief Information Security Officer and/or the Risk Management team to ensure the appropriate standards are included in the procurement.
This data classification self-assessment is based on the NIST 800-53 Revision 5 (or current) requirements and designed to help state and local governments easily identify the appropriate GovRAMP security category to include in a solicitation. Definitions of GovRAMP Core, GovRAMP Ready, GovRAMP Provisionally Authorized, and GovRAMP Authorized, as well as Low Impact, Moderate Impact, and High Impact, can be found in the GovRAMP Security Assessment Framework located here, with further information available on GovRAMP's Templates and Resources page. Additional guidance on mapping types of information to security categories can be found at SP 800-60 Vol. 1 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories | CSRC.

Instructions

Answer the questions in the survey section to determine what GovRAMP security category requirements you need to include in your solicitation to ensure your data is protected.

Survey Questions

1. Will the vendor process, transmit, and/or store non-sensitive State data, metadata, and/or data that may be released to the public that requires no additional levels of protection?
    a. If yes, GovRAMP Low is recommended.
2. Will the vendor process, transmit, and/or store personally identifiable information (PII) as defined by the U.S. Department of Labor (DOL)?
    a. If yes, GovRAMP Moderate is recommended.
3. Will the vendor process, transmit, and/or store protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA)?
    a. If yes, GovRAMP Moderate is recommended.
4. Will the vendor process, transmit, and/or store payment card industry (PCI) data as defined by the PCI Security Standards Council (PCI SSC)?
    a. If yes, GovRAMP Moderate is recommended.
5. Will the vendor process, transmit, and/or store criminal justice information (CJI) data as defined by FBI CJIS Division?
    a. If yes, GovRAMP Moderate is recommended.

    Note: States may add additional controls to GovRAMP Moderate to comply with the CJIS requirements.
6. Will the loss or unavailability of the data processed, transmitted, and/or stored by the service provider disrupt government operations?
    a. If yes, GovRAMP Moderate is recommended.
7. Will the loss or unavailability of the data that is processed, transmitted, and/or stored by the service provider result in a loss of confidence or trust in the government?
    a. If yes, GovRAMP Moderate is recommended.

Next Steps

Data processed, transmitted, and/or stored by the vendor includes information shared inside and outside of the provider's cloud service application. Similarly, if state or local laws have identified any other data type not included in the survey above as confidential, a GovRAMP Moderate is recommended. Once a procurement has been completed partner with the information security team, Chief Information Officer, Chief Information Security Officer, and/or Risk Management team to ensure the appropriate standards have been met.

NIST 800-53 and Cloud Procurement: Process Flows

Project Inception

- Business case starts with a project request identifying the business mission and goal the need fulfills including background, outcome, business, involved personnel and system requirements, data inventory, data classification and risks.
- This will include any known business standards and compatibility that the system must meet.
- This should include an outcome statement about what the agency needs to address their business challenge - not a prescriptive design.
    - Additionally, though this may not always be feasible, the team should consider the benefits of an initial "pilot" phase with a lower cost associated, enabling full award to be conditioned upon successful completion of that pilot phase.
- This work, managed under the business sponsor who initiates the project includes participation from the knowledgeable SMEs.
- Prepare to include, at a minimum, essential stakeholders early in the planning process:
    - Information Security
    - Procurement
    - General Counsel
    - Risk Management

    Vendor Management

Governance Review & Compliance

- Review and approval/disapproval of the cloud service provider (CSP) based project for compliance with enterprise architecture (EA) and security standards and policy.
- Documents completed in this step include approved project request with any additional requirements and a risk assessment with State RAMP Impact level and/or Security Snapshot.
- During pre-procurement risk assessment:
    - Verify or identify data classifications included in project.
    - Validate or determine appropriate GovRAMP Impact Level Classification (Low/Moderate/High) using GovRAMP Data Classification tool, and other specific requirements such as time deadlines for the work, Security Snapshot requirements, etc. based on data classification.
    - No projects can be procured without this review step to address compatibility, privacy standards, security standards, NIST 800-53 controls and other critical information essential to the procurement solicitation and successful contract execution.
- This can often be an iterative process between the governance review authority, requesting agency, Chief Information Security officer (CISO), Data Compliance Officer, appropriate SMEs and other identified stakeholders.

The next step is to identify the appropriate GovRAMP assessment level that must be achieved and sustained throughout the entire lifecycle of the resulting contract. This determination is not merely procedural. It is foundational to ensuring compliance and maintaining trust with government stakeholders.

To accomplish this, the organization's security policies and control framework must be fully aligned with the requirements outlined in the procurement package. Any misalignment can introduce compliance gaps, contractual risks, or delays in authorization. Therefore, close collaboration between the Information Security team and the procurement function is essential. This partnership ensures that security obligations are clearly understood, integrated into contractual terms, and supported by the necessary technical and operational measures from the outset. To streamline adoption, it is recommended that agencies have processes in place to determine who is responsible for ensuring providers meet timeline requirements. Conducting a post award-contract review with all stakeholders involved is ideal.

By embedding security considerations into procurement decisions early and maintaining continuous alignment, the organization can safeguard sensitive data, uphold regulatory commitments, and position itself for long-term success in delivering secure cloud services to government clients.

Assessment Determination

Upon completion of data classification, your organization also must consider any regulatory compliance associated with the data in addition to the impact on critical infrastructure should the confidentiality, integrity or availability of the data be compromised. Overlays may also be available for regulatory data (eg. CJIS Overlay).

Core is the floor! Many organizations use GovRAMP Core as the minimum assessment level to achieve in order to do business. GovRAMP Core was designed to offer an assessment that does not require a third-party assessing organization for products that may not handle sensitive data but still require security reviews. Although a product may process public data, the integrity of that data matters. A product may not process any data, but the availability of the product matters, ie. traffic control management software.

As the risks associated with the data and/or product increase, the level of assessment should also increase. GovRAMP Ready and GovRAMP Authorized are meant to address that increased risk. Provisionally Authorized is also available should a service offering meet the Authorization requirements but one of the following items are identified:

1. One of the product's interconnected technologies is not GovRAMP or FedRAMP Authorized; or
2. During the PMO review, it is identified that one or more deficiencies exist that the PMO and Sponsoring Body agree could reasonably be remediated through the issuance of a Plan of Action and Milestone entry and that these deficiencies do not materially affect the overall security posture of the product.

Overlays

In the context of a cloud product security assessment, a security overlay refers to an additional layer of security controls or requirements that are applied on top of a baseline security framework to address specific risks, compliance obligations, or organizational needs. With GovRAMP, the CJIS-Aligned Overlay is available to address additional compliance considerations aligned to the FBI's Criminal Justice Information Services (CJIS) Security Policy 5.9.5 requirements. This should be utilized when a service offering processes criminal justice information and tailored to help service providers achieve and 3PAOs validate conformance with CJIS Policy.

For more information on the overlay, visit Simplifying CJIS Conformance: Introducing the GovRAMP CJIS-Aligned Overlay - GovRAMP and GovRAMP CJIS-Aligned Overlay Control and Parameters.

Below is an example of a matrix used to evaluate what assessment level is necessary based on data type and impact on critical infrastructure. This is not the only methodology an organization may deploy to leverage GovRAMP in its organization. How you classify and evaluate data may vary based on your organization's already existing data policy and classification requirements.

Data Consideration			
Data Type	**Compliance/Regulatory Requirement**	**Data Sensitivity Classification**	**Minimum Assessment Required**
Data that is not required to be kept confidential by law, by contract, for business reasons, or for *any* other reason	None	Nonconfidential *Or* Confidential - Proprietary	GovRAMP Core
Data that includes PII, PHI, FTI, PCI Data, SSA Data, education records, unemployment records, any other information that is required to be kept confidential by law, by contract, for business reasons, or for *any* other reason	State/Local Code, IRS Pub 1075, HIPAA, PCI DSS, CMS, FISMA, 20 CFR 603, FERPA, others as applicable	Confidential – Sensitive *Or* Confidential - Proprietary	GovRAMP Authorized at the Moderate Impact level
CJIS Data	CJIS Security Policy	Confidential – Sensitive *Or* Confidential – Proprietary	GovRAMP Authorized + CJIS Overlay
Critical Infrastructure			
Will the compromise of confidentiality, integrity or availability of the product and/or data impact critical infrastructure?			
Yes		GovRAMP Authorized at the Moderate impact level	
No		GovRAMP Core	

What if a product does not have a GovRAMP assessment?

Organizations can leverage the Progressing Snapshot Program as an interim solution. This program enables a cloud service provider to demonstrate foundational product security assurance and transparency while working toward the full security assessment required for the contract. A Snapshot score of 100 alone is not sufficient. What matters is ongoing participation in the Progressing Snapshot process, which ensures that the product's score is actively improving and then maintained and monitored. This continuous engagement provides confidence that the provider is progressing toward compliance rather than remaining static.

Participating government agencies gain the ability to request access to progress reports throughout the lifecycle, starting from contract inception and up until the final assessment is completed and the product transitions to continuous

monitoring. The result? End-to-end transparency and accountability from day one of the contract through closeout, reducing risk and fostering trust in the provider's security posture

To learn more about each assessment and control requirements, please visit GovRAMP Templates and Resources.

Sourcing Planning & Strategy

- At this point the project package has been approved and is ready for formal procurement planning.
- The approved project package now includes appropriate requirements for Enterprise Architecture, Cybersecurity, Privacy, NIST Controls, GovRAMP Impact Level, and project timelines to allow a procurement team and appropriate SMEs to develop a procurement plan and sourcing strategy.
- Documents completed in this step include; project charter, refined and validated business needs, market analysis, sourcing strategy and sourcing plan designed to address client, governance and market constraints and conditions and result in the identified outcomes for the project.
- The plan will identify the sourcing method (RFP, competitive proof of concept, cooperative purchase, multiple awards, pre-qualification, limited competition, etc.).

Sourcing Execution

- Once the sourcing strategy and procurement plan are complete, reviewed and approved by the business owner, CISO and other key stakeholders, the source selection phase can begin.
- This phase creates the sourcing documents, selection process, evaluation process that align and harmonize with the procurement plan and when implemented help achieve the procurement strategy.
- In this phase the best qualified cloud service provider/s who meet the government's expectations for security, privacy and compliance with selected NIST 800-53 baseline controls are selected for contract award.
- For further reference see Solicitation Checklist for GovRAMP certification at the end of this document.

Contract Award Process

- This will vary depending on the sourcing method (RFP, cooperative contract, master agreement, etc.)
- Most contract steps will use standard clauses but aligned to the sourcing method and GovRAMP category impact level defined in the sourcing strategy.

Continuous Monitoring

- This flow initiates continuous monitoring for the appropriate NIST 800-53 controls throughout the contract's life.
- Confirm monitoring and reporting requirements with provider including:
    - Confirm roles and responsibilities for reporting and monitoring,
    - Identify contacts
    - Identify timelines and key dates
- Other information is required by the contract.
    - Adopt Monitoring and Reporting procedures to clarify and document the responsibilities of the party.
- Begin monitoring and reporting.
    - GovRAMP's role in Continuous Monitoring
        - Provides centralized oversight and review of vendor continuous monitoring after authorization.
        - Reduces the need for procurement to collect assess security artifacts directly.
        - Shares monitoring results with GovRAMP participating governments to support decisions around product usage and risk.
        - Maintains an up to date authorized vendor Authorized Product List (APL), as well as a Progressing Product List (PPL), that procurement and IT teams can reference during contract oversight.

Solicitation Checklist for GovRAMP Requirements

- Solicitation documents and/or selection documents clearly set out:
    - GovRAMP Impact Level product certification (Core, Ready, Authorized, Provisionally Authorized), including NIST control baseline (Low, , Moderate, or High) as appropriate for the provider service/s sought.
    - The time when the appropriate Impact Level must be achieved (fixed date, or amount of time). When appropriate, GovRAMP Progressing Security requirement (reports, timelines).
    - Identify proof required to validate certifications for Impact Levels and Snapshot requirements.
    - Include requirements for continuous monitoring and reporting to the contracting officer or representative that include:
        - access to GovRAMP 3PAO reports,
        - required notice to the contracting officer for any change in Impact Level Status,
        - receipt of reports, non-disclosure requirements,
        - provider's cooperation in developing a monitoring and reporting procedure,
        - and other items to create a workable and accountable process for timely reporting of provider's change in compliance with selected NIST 800-53 baseline controls.
    - Remedies to address noncompliance with required baseline controls and loss of Impact Level status.

- Form a sourcing team and evaluation committee with representatives of the client agency, CISO, CIO and other key government stakeholders.
- Identify mandatory GovRAMP, security and privacy requirements that are not subject to mandatory requirements in the RFP.
- Require mandatory submission of GovRAMP Impact Level certification, and/or official GovRAMP 3PAO, or
- Security Snapshot report (if required) with the proposal. This third-party report will be by the Contracting Officer to validate the products are compliant with NIST 800-53 baseline controls and responsive to the RFP.
- Minimize overlap and default to standard NIST 800-53 baseline controls by reviewing security, privacy and GovRAMP language in solicitation documents.

GovRAMP Standard Draft Policy Language

State/Entity _____ Draft Policy Language

1. Purpose

a. This policy is intended to address risk and protect privacy in State/ Entity _____ government information systems through a standardized and reusable approach based on controls derived from NIST 800-53, Rev 5, or most current controls to acquire commercially offered cloud products and services such as Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service that host information systems or applications operated by an agency or on behalf of an agency by a contractor or other organization.

b. The policy is further intended to promote standardization in procurement, contract management, compliance monitoring and foster contract competition among cloud-based service offerors progressing toward obtaining validated NIST 800-53 Rev 5 controls.

c. The goal of this policy is to eventually contract with providers whose cloud-based products and services offering have achieved a GovRAMP security status at the appropriate baseline control level determined by the State/Entity _____.

2. Policy

RISK MANAGEMENT ASSESSMENT AND PROCUREMENT

a. The State/Entity _____ requires an independent 3rd party attestation of the presences of NIST 800-53 Rev 5, or most current version, specifically through GovRAMP, for cloud-based information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information containing confidential or proprietary data (as defined in Section XXX) through a contract with an agency of State/Entity _____.

b. At a minimum, a current GovRAMP Security Snapshot must be provided prior to contract award and GovRAMP Core status must be achieved and documented within 12 months of the contract award. Should it be deemed necessary by State/Entity, GovRAMP Ready status must be achieved and documented within 12 months of the contract award. GovRAMP Authorization status shall be achieved and documented within 18 months of the award. A GovRAMP Security Snapshot must be maintained, to include monthly progress reporting until GovRAMP Ready Status is achieved. GovRAMP Security Snapshot monthly progress reporting should indicate progression toward GovRAMP Ready status.

c. Should the jurisdiction choose to accept a GovRAMP Provisionally Authorized status in lieu of Authorized status, service providers must provide proof of its Provisionally Authorized status to the jurisdiction at the time that the contract is awarded.
d. Nothing in this policy prevents State/Entity _____ from contracting for cloud-based product offering and service that are certified as GovRAMP Authorized when circumstances warrant and at least three (3) qualified providers meet the requirements.

3. Exceptions

Exceptions may be made on a case-by-case basis by the CISO in accordance with the State/Entity _____ Exceptions policy.

GovRAMP Procurement Solicitation Best Practices

Purpose

This language should be used in procurements where the organization's third-party risk management policy is applicable. The guidance and proposed clauses below should be implemented and conform to the requirements as set forth in the organization's policy. The proper clauses as required by the needs of this solicitation should be selected and added to provide guidance to the bidders/respondents as to the expectations they need to meet both during the solicitation process and following award and contract execution.

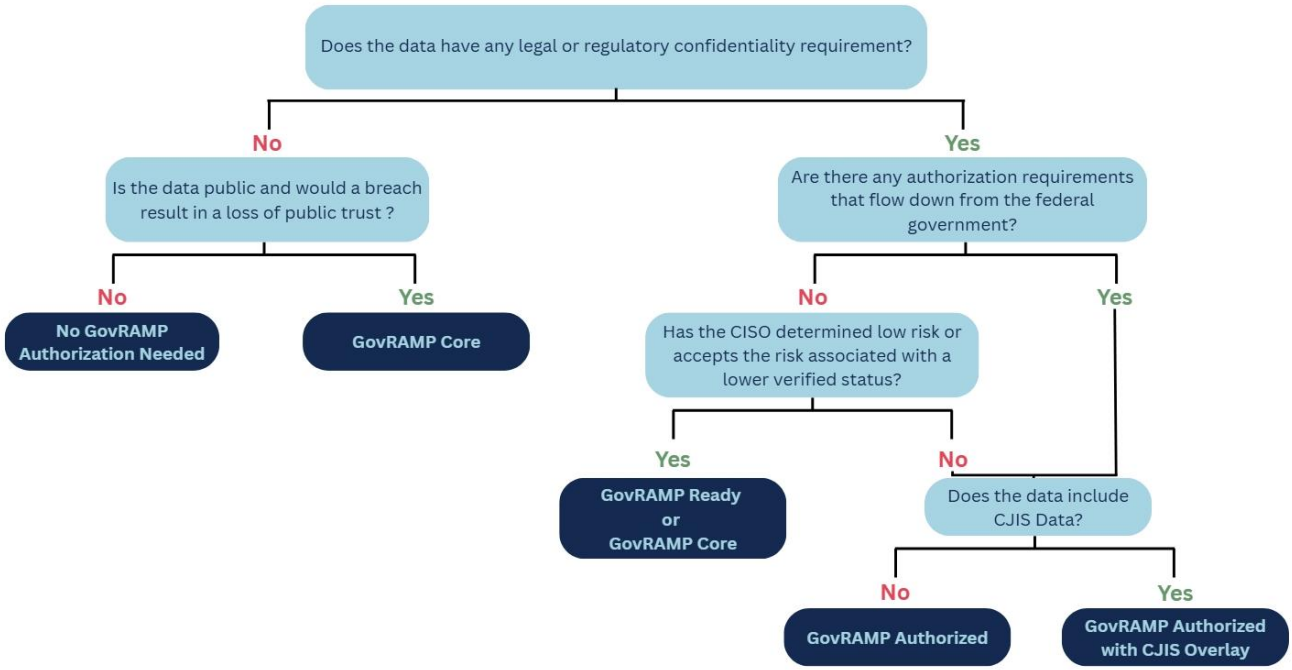
Please note, these are model clauses. The exact language that your organization chooses to implement will be dependent on your policies and the needs of your organization. Language will vary based on the type of procurement, as well as the selection process utilized in that procurement, the cloud product, risk, and/or other factors determined by your organization.

Instructions on Use

To deploy GovRAMP within an organization's procurement and contracting process, follow these steps:

1. Determine the appropriate level of cybersecurity maturity and compliance required for your solicitation by evaluating the scope of relevant data and nature of the cloud service product. (See Procurement Cloud Security Resource Tool Flow Chart below for an example of how you can right size your risk approach.)
2. Select the corresponding guidance and clauses from the 'Accept,' 'Prefer,' or 'Require' sections, as well as the Additional Continuous Monitoring and Pre-Contract Requirements sections below to include in your solicitation documents. For ease of use, all clauses will be in traditional typeface, while guidance will be bolded in italics.
3. Ensure continuous monitoring clauses are incorporated into your contracts to maintain security compliance throughout the contract duration.
4. Communicate clearly with potential vendors about the expectations and requirements for GovRAMP compliance.

Right Sizing Risk Assessments



Guidance and Clauses

REQUIRE

Requiring GovRAMP ensures a unified, secure, and efficient approach to managing third-party cloud services within your organization. It provides a standardized framework for assessment and monitoring, reduces duplication of effort, and sets clear expectations for vendors, ultimately strengthening overall information security governance.

Requiring GovRAMP is best practice as it offers the most benefit with the least drawbacks:

- ✓ Streamlined, standardized assessment for all third-party cloud products handling organizational data.
- ✓ Centralized continuous monitoring and artifact repository for improved oversight and transparency.
- ✓ Supports transition to an oversight model, reducing operational burden on agency security teams.
- ✓ Clear signal to vendors about security requirements before contracting, minimizing compliance gaps.
- × Initial change management lift is challenging, but long-term benefits outweigh short-term effort.

Option 1: Require with Transition Period

Use these clauses where your organization requires GovRAMP compliance to meet your RAMP Policy and allows a transition period.

Solicitation Clause

Use this clause when the market is in transition, and immediate NIST control compliance is not required.

Cloud service products subject to RAMP authorization – The successful proposer's cloud service product offering(s) that collect, process, store, maintain, transmit, dispose, and/or could impact government data must demonstrate compliance with National Institute of Standards and Technology (NIST) Special Publication 800-53 (revision 5 or latest version) at the Impact Level specified below or be enrolled in the GovRAMP Progressing Snapshot Program having received at least one non-zero score until the product achieves GovRAMP (Core/Ready/Provisionally Authorized/Authorized) at a Public Control Baseline of (Low, Moderate, or High).

Continuous Monitoring & Progress Reporting

Use this clause to ensure that progress reporting and continuous monitoring are maintained for the duration of the contract. This clause is also used to ensure that progress reporting and continuous monitoring access is provided to the organization for the duration of the contract.

Continuous Monitoring – The successful proposer must agree to provide continuous monitoring access through GovRAMP as requested. Access Products without a GovRAMP status of Ready, Authorized, or Provisionally Authorized must enroll in the GovRAMP Progressing Security Snapshot Program, complete quarterly Snapshots, and provide monthly progress reporting to GovRAMP until GovRAMP Core, Ready, GovRAMP Authorized, or GovRAMP Provisionally Authorized status is obtained. The requirements for this contract are outlined below.

On-RAMP Option:

Use this clause to set deadlines for achieving GovRAMP Core/Ready/Authorized/Provisionally Authorized status.

If the provider does not already have a GovRAMP status of Core, Ready, Authorized, or Provisionally Authorized, the appropriate status must be achieved in the following timeframes: (1) GovRAMP Core or Ready status at a Public Control Baseline of (Low, Moderate, or High) must be obtained not later than 12 months after execution of this contract; (2) GovRAMP Authorized or Provisionally Authorized status at a Public Control Baseline of (Low, Moderate, or High) must be obtained not later than 18 months after execution of this contract. Subsequent Security Snapshots should reflect progress toward increased security controls and GovRAMP status. [Organization Name] must be granted visibility and access through GovRAMP for progress reviews as requested.

Option 2: Require without Transition Period

Use these clauses where your organization requires GovRAMP compliance to meet your RAMP Policy and does not allow a transition period.

Solicitation Clause

Use this clause for markets where competition exists between cloud service providers who have achieved GovRAMP Core, Ready or Provisionally Authorized Status. You should select the Public Control Baseline (Low, Moderate, or High) necessary for your specific procurement/contract.

Cloud service products subject to RAMP authorization – The successful proposer's cloud service product offering(s) that collect, process, store, maintain, transmit, dispose, and/or could impact government data must demonstrate compliance with National Institute of Standards and Technology (NIST) Special Publication 800-53 (revision 5 or latest version), and must possess GovRAMP Core, Ready, Provisionally Authorized or Authorized status at the Public Control Baseline of (Low, Moderate, or High) at the time of award.

Continuous Monitoring: GovRAMP Core to Provisionally Authorized or Authorized

Use this clause to ensure that continuous monitoring is maintained and access is provided to the organization for the duration of the contract.

Continuous Monitoring - Products with GovRAMP status must grant visibility and access through GovRAMP for continuous monitoring as requested. Once a product transitions from Ready to Provisionally Authorized or Authorized status, it must maintain its Provisionally Authorized or Authorized status for the duration of the contract. Government must be granted visibility and access through GovRAMP for continuous monitoring as requested.

HYBRID

Adopting a hybrid model for GovRAMP—where organizations can accept, prefer, or require compliance when necessary—offers both benefits and challenges:

- ✓ Leverages GovRAMP Continuous Monitoring - provides ongoing security oversight for participating cloud products, improving risk management.
- ✓ Encourages Provider Community Alignment with NIST 800-53 - promotes adoption of standardized security controls, strengthening overall security posture.
- × Lacks Consistent Apples-to-Apples Comparisons - Variability in provider implementations makes it difficult to uniformly compare security levels across vendors.

Solicitation Clause

Use these clauses when your organization intends to gain the flexibility to tailor solutions on a contract-by-contract basis while still leveraging some of the benefits of the GovRAMP program. Select the appropriate clause based on that particular solicitation/contract.

Accept: The successful proposer's cloud service product offering(s) that collect, process, maintain, use, share, disseminate, or dispose of information containing or impacting confidential or proprietary government data must demonstrate compliance with either GovRAMP or FedRAMP at a Public Control Baseline of (Low, Moderate, or High), or HITRUST at a Level (X).

Prefer: Cloud service products subject to RAMP authorization - The successful proposer's cloud service product offering(s) that collect, process, store, maintain, transmit, dispose, and/or could impact government data must demonstrate compliance with one of the standards accepted in accordance with the [Name of the Organization's Policy] policy. However, those proposers who hold a verified GovRAMP status of Core, Ready, Provisionally Authorized, or Authorized at a Public Control Baseline of (Low, Moderate, or High) shall be awarded preference over other standards in accordance with the points matrix outlined below.

Require: For contracts involving high risk data - The successful proposer's cloud service product offering(s) that collect, process, store, maintain, transmit, dispose, and/or could impact government data must demonstrate compliance with one of the standards accepted in accordance with the [Name of the Organization's Policy] policy. However, those proposers who hold a verified GovRAMP status of Core, Ready, Provisionally Authorized, or Authorized at a Public Control Baseline of (Low, Moderate, or High) shall be awarded preference over other standards in accordance with the points matrix outlined below.

Continuous Monitoring: GovRAMP

Use this clause when the cloud service provider is relying on GovRAMP, including monthly continuous monitoring, to satisfy your organization's cybersecurity standard.

Continuous Monitoring - Products utilizing a GovRAMP security status to satisfy this cybersecurity standard, must maintain its status for the duration of the contract and must grant visibility and access through GovRAMP for continuous monitoring as requested.

PREFER

Preferring GovRAMP when necessary, offers notable advantages but also introduces challenges. This approach helps promote security standardization and simplifies assessments for compliant products, yet it can create inconsistencies and operational complexity.

Preferring GovRAMP statuses:

- ✓ Encourages provider community alignment with NIST 800-53 standards.
- ✓ Makes it easier for governments to assess cyber maturity for GovRAMP products.
- × No guarantee that proposed products meet specific security needs.
- × No apples-to-apples comparison of products' cybersecurity posture.
- × Continuous monitoring oversight may be ad hoc or decentralized.

Use these clauses where your organization prefers GovRAMP compliance over other standards. You can choose to implement an evaluation point preference when utilizing proposal-based solicitations, or a simple preference in those cases where you are selecting products from a master contract.

Solicitation Clause

Use this clause where your organization prefers GovRAMP compliance in proposal-based solicitations.

Cloud service products subject to RAMP authorization - The successful proposer's cloud service product offering(s) that collect, process, store, maintain, transmit, dispose, and/or could impact government data must demonstrate compliance with one of the standards accepted in accordance with the [Name of the Organization's Policy] policy. However, those proposers who hold a verified GovRAMP status of Core, Ready, Provisionally Authorized, or Authorized at a Public Control Baseline of (Low, Moderate, or High) shall be awarded preference over other standards in accordance with the points matrix outlined below.

Continuous Monitoring: GovRAMP

Use this clause when the cloud service provider is relying on GovRAMP to satisfy your cybersecurity standard.

Continuous Monitoring - Products utilizing a GovRAMP security status to satisfy this cybersecurity standard must maintain its status for the duration of the contract and must grant visibility and access through GovRAMP for continuous monitoring as requested.

ACCEPT

Adopting a model that simply accepts GovRAMP along with other frameworks provides flexibility but introduces complexity. While it leverages existing security programs and promotes standards, it can create inconsistencies and additional burdens for internal teams.

Accepting GovRAMP statuses in addition to other frameworks:

- ✓ Leverages GovRAMP continuous monitoring for participating cloud products.
- ✓ Encourages provider community to move toward NIST 800-53 standards.
- × No apples-to-apples comparison of products' cybersecurity posture.
- × Continuous monitoring oversight may be ad hoc or decentralized.
- × Burden remains on internal information security teams to complete risk assessments.
- × Creates a less streamlined security process for the vendor community.

Solicitation Clause

Use this clause when your organization accepts GovRAMP alongside other cybersecurity standards.

Cloud service products subject to RAMP authorization - The successful proposer's cloud service product offering(s) that collect, process, maintain, use, share, disseminate, or dispose of information containing or impacting confidential or proprietary government data must demonstrate compliance with either GovRAMP or FedRAMP at a Public Control Baseline of (Low, Moderate, or High), or HITRUST at a Level (X).

Continuous Monitoring: GovRAMP

Use this clause when the cloud service provider is relying on GovRAMP, including monthly continuous monitoring, to satisfy your organization's cybersecurity standard.

Continuous Monitoring - Products utilizing a GovRAMP security status to satisfy this cybersecurity standard, must maintain its status for the duration of the contract and must grant visibility and access through GovRAMP for continuous monitoring as requested.

Additional Continuous Monitoring Language

Specify continuous monitoring requirements for the duration of the contract.

Continuous Monitoring – For any resulting award(s) and subsequent contract(s), the awarded contractor(s) will:

1. Grant access to continuous monitoring and reporting upon receiving award for GovRAMP Security Snapshot, GovRAMP Progressing Snapshot, Core, Ready, Provisionally Authorized, or Authorized status throughout the life of the contract.
2. Comply with (insert jurisdiction) requests to review all Third-Party Assessment Organization (3PAO) audits, risk assessments, vulnerability assessments, and penetration tests of the contractor's environment.
3. Respond to all vulnerabilities discovered or changes in status by providing a mutually agreed upon timeframe to resolve the issue and/or implement a compensating control.
4. Submit a procedure acceptable to the contracting officer to guide notification, reporting, and remediation of any change in status or flaws discovered by a Third-Party Assessment Organization (3PAO).

Pre-Contract Requirements

Proof of compliance with the required GovRAMP security status, or Security Snapshot, is necessary to complete due diligence. Depending on the sourcing methodology, what the proof is and the point when it must be furnished may vary. The clauses below must harmonize with the GovRAMP compliance clause utilized above.

The examples below describe the different times in the award process when due diligence may be completed.

Proof of Compliance at Time of Proposal

With some methods, proof of compliance with the required GovRAMP security status, or Security Snapshot, is necessary for the contracting officer to complete due diligence before proposals are scored. The most typical RFP methodology requires a responsiveness determination before proposals are evaluated and scored. The RFP requires proof of mandatory requirements such as proof of GovRAMP Authorization or attainment of Security Snapshot to be submitted with the proposal.

Vendor must submit one of the following at the time of proposal submission as requested by (Insert Organization Name):

1. Proof of current GovRAMP Authorized status in the form of a GovRAMP Letter
2. Proof of current GovRAMP Ready status in the form of a GovRAMP Letter
3. Proof of current GovRAMP Core status in the form of a GovRAMP Letter
4. Valid GovRAMP Security Snapshot Score and proof of enrollment in the GovRAMP Progressing Security Snapshot Program

Failure to submit the document(s) listed above at the time of proposal will result in a proposal being deemed non-responsive.

Proof of Compliance after Proposal Submission, but Prior to Contract Award

For other methods, proof of GovRAMP Compliance or Security Snapshot level may be delayed after evaluation but before contract execution.

Again, proof of compliance with the required GovRAMP security status, or Security Snapshot level is required for the contracting officer to complete due diligence, but in this case the proof is due before contracts are executed by the Contracting Officer. In these circumstances the solicitation (RFP for a single award, RFP for multiple awards, Challenge Procurement, etc.) may allow a maximum period of time for the Contracting Officer to accept the proof, or it may be left unspecified. This method allows prospective contractors more time to obtain compliance but should not be indefinite. This method can help stimulate competition in an immature market because it allows in process Authorizations and Snapshots to be completed.

Prospective contractors must submit one of the following in accordance with the requirements of the RFP when required by the Contracting Officer and before a final award may be executed.

1. Proof of current GovRAMP Authorized Status in the form of a GovRAMP Letter
2. Proof of current GovRAMP Ready Status in the form of a GovRAMP Letter
3. Proof of current GovRAMP Core Status in the form of a GovRAMP Letter
4. Valid State RAMP Security Score and proof of enrollment in GovRAMP Progressing Security Snapshot Program

Proof of Compliance Before Final Contract Execution

For other methods, including, but not limited to price agreements, umbrella contracts, indefinite quantity awards, work order contracts or cooperative proof of GovRAMP compliance may be delayed until final contracts are executed by the using agency. While award mechanisms may vary by organization, when the proof is required and who validates the proof must be specified in the solicitation document. The final validation can be made by the contracting officer in price agreements and similar award processes where the GovRAMP compliance and requirements are made part of the final award, or they may be differed to the using agencies to validate the proof of compliance and complete the due diligence for prequalification listings and cooperative procurement awards.

Delayed proof can maximize competition by allowing emerging technology solutions to obtain appropriate levels of compliance and allow awarded cloud service providers to improve their security compliance poster over time. This gives organizations more choices and better fits for cloud services needs over time.

Selected cloud product provider must submit one of the following in accordance with the requirements of the RFP when required before a final award may be executed.

1. Proof of current GovRAMP Authorized Status in the form of a GovRAMP Letter.
2. Proof of current GovRAMP Ready Status in the form of a GovRAMP Letter
3. Proof of current GovRAMP Core Status in the form of a GovRAMP Letter
4. Valid State RAMP Security Score and proof of enrollment in GovRAMP Progressing Security Snapshot Program.

Resellers

Applicability to Resellers: Any Contractor acting as a software reseller under this Contract must ensure that any cloud products—subject to the conditions outlined in <insert organization cloud policy> —and made available to, sold to, or distributed to the State, comply with applicable GovRAMP and/or FedRAMP security requirements. This obligation extends to software developed or owned by third parties. The original software owner or developer must meet the standards outlined in NIST Special Publication 800-53 Revision 5, in accordance with <insert cloud policy and specific requirement>. If the cloud product is participating in the GovRAMP program, the product owner must provide the State with access to the following artifacts, including but not limited to: continuous monitoring data, monthly progress reports, quarterly Snapshot scores, Third-Party Assessment Organization (3PAO) audits, risk assessments, vulnerability assessments, and penetration tests.

Contractor Responsibility: The reseller is responsible for ensuring that the software owner complies with these requirements for the duration of the contract. Failure to ensure compliance may result in contract reevaluation, liquidated damages, or termination.

Exception Policy

<Organization Name> - Exceptions

The requirements of this policy are the default standards for <insert affected agencies and/or entities> that are responsible to the <insert appropriate lead agency>, as well as any other entities that utilize the organization's systems, network, or other IT infrastructure. They are intended to protect the data of these different entities and the technology resources that are used to store, process, and transmit it. The minimum security level matrices that are discussed in this policy are based on generally accepted industry standards that cloud providers should be familiar with and amenable to.

a. This exception process applies to all contracts subject to the requirements established under <refer to policy requiring security assessments for cloud>.

b. All exceptions are considered policy deviations and may be granted in accordance with applicable law by the CISO or designee. Administrative, physical, or technical requirements may indicate the need for exemption under this Policy, for specific matters. Considerations for exemptions may include but are not limited to:

    a. Contracts where the contract value is under $X; or,

    b. The contract lifecycle is lesser than or equal to X; and

    c. Contracts where CISO or designee has determined either that the risk is low or that the State accepts the risk presented by Policy deviation; and

    d. Contracts where the contractor only does business within the <insert region covered>; and

    e. Contractor meets the State of X's criteria for small business designation as defined by <insert code/statute/policy>.

    Such exceptions must be documented in accordance with Section D below.

c. Exceptions may not be granted for service providers that have experienced a material breach within the last (12) months.

d. Depending on where the data falls in the matrix and following an appropriate risk assessment, the CISO or designee, can acknowledge and/or escalate exception requests and may require the cloud service provider to:

    a. Complete a GovRAMP Core assessment in lieu of GovRAMP Authorized and maintain Core status for the duration of the contract; or

    b. Enroll in the GovRAMP Progressing Snapshot program in lieu of GovRAMP Core; or

    c. At CISO or designee's sole discretion, complete either an annual single GovRAMP Snapshot or work with <organization Office of Technology> to directly assess the security controls included in the then current GovRAMP Snapshot on at least an annual basis.

e. **Exception Process**: Prior to an exception request being submitted to <organization Office of Technology> , it must be approved by the highest-ranking authority at the covered entity (executive director, commissioner, agency head, etc.), who must acknowledge that he or she has reviewed the modifications and believes an exception is warranted because the benefits to the covered entity's business and mission are judged to outweigh any associated security risks. Requests for exceptions must use the appropriate form and be approved by the <organization Office of Technology> , prior to submission. Exception requests must be submitted by the requesting agency via <organization Office of Technology> electronic form, which is available by request at <insert applicable link or email>. At a minimum, the request must document the following:

    1. A description of the cloud offering in question including how it will enable the covered entity to serve our constituents, cost of the product/service, and whether sensitive data and/or critical infrastructure is involved and the volume thereof;

    2. A description of precisely how the requirements should be modified and why it believes the modifications are warranted under the circumstances.

f. All exceptions must be documented in accordance with this Policy. Exceptions are valid for 12 months and may be renewed by reapplying via the process outlined above.

Liquidated Damages

Guidance:

Liquidated damages provisions are common in contracts to pre-determine the amount of compensation one party must pay if they breach the contract. When deploying terms of this nature, there are some key considerations you must take into account:

1. **Reasonableness:** The amount specified must be a reasonable estimate of the anticipated or actual harm caused by a breach. If the amount is unreasonably large, it may be deemed unenforceable as a penalty. Take the time to think about what the costs would be to your organization to ensure protection of your data if the CSP isn't in compliance with your security requirements. These could be costs associated with performing your own checks on their system, administrative costs associated with regular check-ins and status calls, costs associated with increases in your cyber insurance coverage, or even the costs of deploying overlap between their service and another service that is in full compliance with your security standards. By thinking through and documenting these costs in advance, you will be able to show that the damages you are requesting are reasonable and not punitive.

2. **Clear and Specific:** The provision must be clearly stated in the contract, specifying the conditions under which liquidated damages will be applied and the exact amount or formula for calculating the damages.

3. **Not a Penalty:** Liquidated damages should not serve as a penalty. They are intended to compensate for anticipated or actual harm caused by the breach, not to punish the breaching party.

4. **Mutual Agreement:** Both parties must agree to the liquidated damages provision at the time of contract formation. This agreement should be documented in the contract using a provision similar to those below.

5. **Enforceability:** Courts will enforce liquidated damages provisions if they meet the criteria of reasonableness and are not punitive. However, if the actual damages are significantly different from the liquidated amount, the provision may be challenged.

6. **Context-Specific:** The appropriateness of liquidated damages can vary depending on the context of the contract. You want to ensure you are able to demonstrate anticipated harm or actual harm caused by failure to comply with a contract provision that gives rise to a liquidated damages clause.

Review the provisions below and determine which one best meets your needs within your organization. Speak with your legal counsel as they may have a provision they prefer or that is used frequently within your organization already (ex. provisions within your construction contracts). Discuss with them the work you have done to determine reasonable damages and incorporate that into your selected clause and resulting contract. Save whatever information you used to establish this amount so you have it should it be necessary later in a dispute.

Sample Clauses:

General Liquidated Damages Clause:
If the Contractor fails to meet the security requirements specified in this contract within the time allowed or fails to maintain the security status outlined in the contract throughout the contract's duration, the Contractor shall pay to the [Organization Name] liquidated damages in the amount of $X per day for each day of delay or lapse. These damages are intended to compensate the [Organization Name] for the loss and inconvenience caused by the delay or lapse and are not intended as a penalty.

Tiered Liquidated Damages Clause:
In the event the Contractor does not meet the security requirements outlined in this contract within the specified time or fails to maintain the security status outlined in the contract throughout the contract's duration, the Contractor shall be liable for liquidated damages as follows:

a. $X per day for the first 30 days of delay or subsequent non-compliance.

b. $Y per day for the next 30 days of delay or subsequent non-compliance.

c. $Z per day for any delay beyond 60 days or subsequent non-compliance.

These amounts are agreed upon as a reasonable estimate of the damages the [Organization Name] will incur due to the delay or non-compliance.

Performance-Based Liquidated Damages Clause:
Should the Contractor fail to achieve the required security standards by the deadline specified in this contract or fails to maintain the security status outlined in the contract throughout the contract's duration, the Contractor agrees to pay liquidated damages calculated as follows:

a. $X for each security breach or incident that occurs due to non-compliance.

b. $Y for each day the security requirements remain unmet.

These liquidated damages are intended to cover the administrative costs and potential risks associated with the delay or lapse in meeting security requirements.

Cumulative Liquidated Damages Clause:
If the Contractor does not fulfill the security requirements within the agreed timeframe, or fails to maintain the security status outlined in the contract throughout the contract's duration, the Contractor shall pay liquidated damages to the [Organization Name]. The damages shall be calculated at a rate of $X per day of non-compliance, cumulative up to a maximum of $Y. This provision is intended to ensure timely compliance and mitigate potential risks to the [Organization Name].


GovRAMP


NASPO
National Association of
State Procurement Officials