NASPO ValuePoint Cloud Solutions
Risk Assessment and GovRAMP Requirements Guide
for Participating Entities and Purchasing Entities

Participating Entities and Purchasing Entities have multiple options to gain assurance that their Cloud Solutions service provider has required security and privacy controls in place. Standards may include, but are not limited to, one or more of the following: a) GovRAMP authorization; b) FedRAMP authorization; c) review of control documentation by internal staff or a third-party assessment organization; d) the service provider's third-party attestation (*e.g.*, SOC 2 Type 2 audit); and e) self-assessment by the service provider. This guide is provided for informational purposes to assist Participating Entities and Purchasing Entities with assessing organizational risk and impact levels and identifying the corresponding GovRAMP status(es) appropriate for their needs.

Participating Entities and Purchasing Entities are encouraged to require their service providers to monitor security controls, assess them on a regular basis, and demonstrate that the security posture of their cloud service offering is continuously acceptable to the Participating Entity or Purchasing Entity, as applicable, throughout the life of the contract. It is further recommended that these entities require the use of independent verification processes, including review by third-party assessment organizations ("3PAOs"), for initial and continuous monitoring, especially where medium and high-risk information systems and data are concerned, and where internal staff may lack sufficient knowledge, experience, or time to effectively perform security and privacy control reviews or audits.

a. Level of Risk. The three primary levels of risk pertaining to data are described below. Before a Participating Addendum is executed or an Order is placed, the Participating Entity or Purchasing Entity should assess the type and level of risk the solution(s) may pose to the entity's data:

i. **Low** – Limited Impact: Loss would have minor adverse effect on operations or assets.
ii. **Moderate** – Serious Impact: Could cause significant operational disruption or loss of sensitive but unclassified data.
iii. **High** – Severe and Catastrophic Impact: Compromise could threaten security, public safety, or critical infrastructure.

Below is a brief list of questions to help a Participating Entity or Purchasing Entity assess general risk level and GovRAMP's risk level classification.

Data Process/Risk	Yes/No	Level of Risk
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?	Yes	Low
Will the vendor process, transmit, and/or store personally identifiable information (PII) as defined by the U.S. Department of Labor (DOL)?	Yes	Moderate
Will the vendor process, transmit, and/or store protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA)?	Yes	Moderate
Will the vendor process, transmit, and/or store payment card industry (PCI) data as defined by the PCI Security Standards Council (PCI SSC)?	Yes	Moderate
Will the vendor process, transmit, and/or store criminal justice information (CJI) data as defined by FBI CJIS division?	Yes	Moderate

Will the loss or unavailability of the data processed, transmitted, and/or stored by the service provider disrupt government operations?	Yes	Moderate
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?	Yes	Moderate

b. GovRAMP Requirements. GovRAMP uses the following statuses to describe the current security posture of a specific product or service:

- **Authorized Status:** Authorized, also referred to as full authorization, is the highest verification level which shows that a product has a proven and complete security package that has been reviewed by a Third-Party Assessing Organization ("3PAO") to ensure compliance with the NITS 800-53 required controls by impact level. The GovRAMP Project Management Office ("PMO") provides independent validation and verification of the security package which is then reviewed by the Sponsoring body before full approval is granted. These products participate in monthly continuous monitoring. Contractor must provide proof of current GovRAMP Authorized Status for the applicable Product(s) and Service(s) in the form of a GovRAMP Letter. A Participating Entity or a Purchasing Entity may also require supplementation of this status with an overlay (e.g., CJIS overlay). If an overlay is required in a Participating Addendum or Order, Contractor must provide proof of its compliance with the applicable requirements in the form of a GovRAMP Letter.

- **Provisionally Authorized Status:** A product meets the Authorization requirements, but one or more of the following is true: one of the product's interconnected technologies is not GovRAMP or FedRAMP Authorized and/or during the PMO review, it is identified that one or more deficiencies exists that the PMO and Sponsoring Body agree could reasonably be remediated through the issuance of a Plan of Action and Milestone entry and that those deficiencies do not materially affect the overall security posture of the product. These products also participate in monthly continuous monitoring. Contractor must provide proof of current GovRAMP Provisionally Authorized Status for the applicable Product(s) and Service(s) in the form of a GovRAMP Letter.

- **Ready Status:** A Ready status indicates that the product meets GovRAMP's Minimum Mandatory Requirements and most critical controls, with an annual readiness assessment completed by a 3PAO, along with monthly continuous monitoring requirements. Contractor must provide proof of current GovRAMP Ready Status for the applicable Product(s) and Service(s) in the form of a GovRAMP Letter.

- **Core Status:** 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, along with quarterly continuous monitoring. Contractor must provide proof of current GovRAMP Core Status for the applicable Product(s) and Service(s) in the form of a GovRAMP Letter.

- **Progressing Snapshot Program:** The GovRAMP Progressing Security Snapshot Program is an ongoing security maturity assessment for cloud products based on the

40 most impactful NIST 800-53 Rev. 5 controls as determined by the MITRE ATT&CK® Framework. The Progressing Security Snapshot Program helps service providers begin their cybersecurity journey while offering governments an initial level of insight into the risk maturity of suppliers' cloud products on an ongoing basis. Snapshots are completed on a quarterly basis to show governments and Providers where the product is on its cyber maturity journey. Contractor must provide proof of enrollment in the form of a GovRAMP letter and the most recent Snapshot score letter for the applicable Product(s) and Service(s) and must submit ongoing verification of progress until a verified status is achieved.

Participating Entities and Purchasing Entities have multiple options for applying GovRAMP requirements to some or all of a Contractor's offerings, including matrices identifying specific Products or Services required to meet one or more standards; setting a minimum status for all Products or Services, with more stringent requirements able to be identified in specific Orders; and requiring a status based on the type(s) of data being processed (*e.g.*, unregulated data vs. regulated data).

Once an entity has identified applicable risk levels in accordance with (a) above, Participating Entities and Purchasing Entities using GovRAMP for security verification are encouraged to refer to the GovRAMP-NASPO Procurement Cloud Security Resource Tool, or reach out to GovRAMP, for guidance on how to select the GovRAMP status(es) that are appropriate for their needs and align with their entity's policies.