StateRAMP (dba GovRAMP)
AI Security Task Force Charter

I. Background

StateRAMP (dba GovRAMP) has worked with its governing committees to adopt NIST-based minimum requirements for cybersecurity in cloud products with a consistent validation process, allowing providers to benefit from a "verify once, serve many" model and allowing public sector users the ability to more efficiently and proactively manage compliance and risk ongoing throughout the contract lifecycle.

With the increasing use of generative AI in cloud products and across the public sector, it is crucial to implement appropriate cybersecurity measures for these AI-integrated solutions (SaaS, PaaS, IaaS). State and local governments are well-positioned to lead this effort by establishing a common set of security standards for AI in cloud products.

II. Purpose

GovRAMP leadership advocates for applying best practices in cybersecurity.

Rather than creating a separate set of standards to evaluate the cybersecurity of cloud products with generative AI, the Task Force will evaluate how to leverage already established NIST cloud security standards and explore whether any additional requirements are necessary.

III. Scope

The Task Force will aggregate best practices recommendations for cybersecurity and trustworthiness as it relates to the use of generative AI in third party cloud products.

Regarding cybersecurity, the scope includes a review of the GovRAMP Security Program to make recommendations for updates to address the security implications of generative AI in cloud products. Recommendations for the GovRAMP Security Program are anticipated to be iterative in nature. That is because GovRAMP's governance and security framework supports an iterative approach, allowing for updates on an annual basis or more frequently, if necessary. This framework enables GovRAMP, along with its advisors and committees, to make incremental adjustments with the assurance that modifications can be made over time as additional information and usage patterns emerge.

Regarding trustworthiness, the Task Force will compile or point to existing recommendations for best practices that can be deployed by public entities when evaluating the use of cloud products with generative AI.

III. Mission

The GovRAMP AI Executive Council will serve as the advisory body for the AI Security Task Force and will work with GovRAMP Staff to direct activities to help meet the objectives of this Charter.

The AI Executive Council will consist of no more than eight (8) members that include a mix of State CIOs and State CISOs.

The AI Security Task Force will be comprised of volunteers from GovRAMP public and private sectors members. The GovRAMP Appeals Committee will provide technical support as needed.

The AI Executive Council will review recommendations from the Task Force and have responsibility for presenting final recommendations to the Standards and Technical Committee and Board for adoption.

IV. Objectives

The Task Force objectives are as follows:

1. **Security Considerations and Risks** – Identify the cybersecurity risks related to the use of Generative AI technologies consistent with the NIST AI Risk Management Framework and NIST 800-53 Rev. 5. Identify gaps and opportunities for improved risk management in the GovRAMP Security Program.

2. **Evaluating Trustworthiness** – Identify risk management frameworks for approaching the trustworthiness of AI systems, such as those as established by the National Institute for Standards and Technology (AI Risk Management Framework, NIST AI RMF Playbook). Make recommendations for best practices/resources for trustworthiness in third party risk management.

V. Strategy

The Task Force will leverage subject matter expertise of Task Force members, GovRAMP Appeals Committee members, GovRAMP Staff and Program Management Office, as well as third party organizations and GovRAMP strategic partners to complete the objectives of the Charter. GovRAMP strategic partners and other organizations include but are not limited to: NASCIO, GovAI Coalition, NASPO, NACO, and the Center for Digital Government.

VI. Responsibilities

The responsibilities of the Task Force are as follows:

1. **Active Participation / Confidentiality**–Task force members are encouraged to have consistent meeting attendance and serve as active participants at meetings, completing any necessary assignments and providing timely feedback to the Executive Council on work products.

2. **Leadership** – The Executive Council will direct the activities of the Task Force and Staff for the purpose of achieving its goals under the Charter.

3. **Working Meetings and Assignments** – Staff will have the responsibility of coordinating work and preparing relevant documentation for meetings.

4. **Executive Leadership Stakeholders and Final Presentation** – The Executive Council will provide an executive presentation to the Board and Standards & Technical Committee on the Task Force findings and recommendations.

VII. Deliverables

The key deliverables include:

1. **GovRAMP Security Program Enhancements –** Recommend enhancements to the GovRAMP Security Program to address cybersecurity of cloud products with generative AI.

2. **Best Practices for AI in Cloud Products Report** – Produce a policy report that includes the following:
    a. **Security, Compliance, and Privacy Controls** – Identify relevant NIST information security and privacy controls that are involved with the responsible use of Generative AI technologies in accordance with best practices; any current federal/state regulatory data compliance requirements that mandate the use of specific controls should be included.
    b. **Trustworthiness Guidance** – Provide recommendations for evaluating trustworthiness of AI in cloud products.

VII. Stakeholders

Task Force may involve input from stakeholders as necessary, including, but not limited to:

1. **Staff** – Executive management, including the support of the GovRAMP Program Management Office (PMO), will provide guidance and support to ensure the fulfillment of this Charter.

2. **AI Executive Council** - The AI Executive Council will direct the Task Force activities and consist of no more than eight (8) members that include a mix of State CIOs and State CISOs.

3. **Task Force** – The AI Security Task Force will be comprised of volunteers from GovRAMP public and private sectors members.

4. **GovRAMP Appeals Committee**– The GovRAMP Appeals Committee is comprised of technical leaders and will work closely with the PMO technical staff to provide necessary subject matter expertise.

5. **Partners/Organizations** – Strategic partners and other related organizations may assist the Task Force, providing guidance and feedback to support the mission described in this Charter.

IX. Authority / Meeting Structure

The Task Force is an ad hoc committee formed by the GovRAMP Board of Directors as a 2025 Strategic Initiative. Meetings will be held virtually.

XI. References

Refer to GovRAMP Resources:

- GovRAMP Security Assessment Framework
- Rev. 5 Templates and Resources - GovRAMP
- Task Force Webpage

XII. Document Information

Initial Issue Date:	March 20, 2025
Point of Contacts:	Leah McGrath, Executive Director, GovRAMP
	Fred Brittain, Executive Advisor to GovRAMP / PMO
Approved By:	AI Executive Council