RGS
Rancher Government Solutions

White Paper

Delivering AI Securely and Confidently in Government Environments

How Federal Agencies Can Adopt Generative AI Without Compromising Data Integrity, Control, or Compliance

Table of Contents

Executive Summary

U.S. government agencies are rapidly exploring generative AI (GenAI) to enhance decision-making, battlefield advantage, mission efficiency, and constituent services. But many overlook the significant risks associated with using public or SaaS-based AI models, especially when handling sensitive, proprietary, or classified data.

This paper outlines how government organizations can adopt GenAI securely, compliantly, and under full agency control by leveraging Rancher Government Solutions' hardened, enterprise open-source platform built for federal requirements. It covers:

- The risks of using SaaS-based AI tools with mission data
- Shadow AI and unmanaged LLM usage across government teams
- Compliance imperatives: STIG, FIPS 140-3, CIS, and Executive Order 14028
- Why government agencies require air-gapped, extensible, and zero-trust AI infrastructure
- How Rancher Government supports secure, mission-aligned AI adoption

The Problem: Shadow AI, SaaS Exposure, and a Lack of Control

SaaS-based AI platforms are popular because of ease of use—but they offer little to no assurance of security, compliance, or data sovereignty. For federal agencies, that's a mission risk. Public LLMs often retain and reuse input data to train commercial models, and U.S. adversaries are exploiting these blind spots.

A 2023 report from Cyberhaven found that 11% of pasted information into SaaS-based AI tools contained sensitive data. Unauthorized, unmanaged use—known as shadow AI—amplifies this risk across government networks and workloads.

For federal programs handling law enforcement, defense, intelligence, or civilian services, this is unacceptable.

The Government AI Stack: Fragmented and Incomplete

Federal agencies exploring AI today often face three suboptimal choices:

- **Public SaaS Tools:** Unverified, uncontrolled, and potentially insecure
- **Upstream Open Source Projects**: Flexible but lack the required certifications (FIPS, STIG) and enterprise support
- **Commercial Enterprise AI Solutions:** May offer security but restrict flexibility, lock in vendors, or lack air-gapped deployability

None of these options meet the standards of a zero-trust, compliant, and mission-ready AI deployment model.

The Solution: Secure, Flexible AI with RGS

Rancher Government Solutions delivers a secure-by-design, open-source AI platform tailored for federal needs. Built on the hardened Kubernetes stack (RKE2) and delivered through Rancher Government Carbide, RGS offers a platform that:

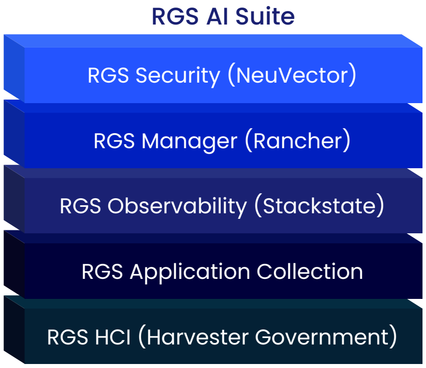
- Is 100% U.S.-citizen staffed
- Authorized to perform within the DoD and IC communities (CAGE Code 8GLZ3)
- Designed to deliver enterprise open source innovation, flexibility and choice
- Is validated through STIGs, CIS Benchmarks, and FIPS 140-3
- Enables on-prem, hybrid, cloud, or air-gapped AI deployment

- Enforces supply chain integrity via SBOMs, SLSA Level 3, and signed artifacts
- Supports data control and zero trust architecture as default

This approach empowers agencies to build and deploy GenAI workloads confidently, without handing their data to third-party clouds or exposing mission-critical code to foreign models.

Secure Infrastructure for AI and Edge Workloads

Artificial intelligence doesn't operate in a vacuum — it relies on secure, scalable, and resilient infrastructure. That's where the RGS AI Suite, the secure by design Cloud Native Infrastructure platform from Rancher Government Solutions, becomes critical. The RGS AI Suite stands apart through its curated stack of open source AI/ML tools, integrated GPU telemetry, and modular architecture designed to simplify GenAI deployment. Optimized for hybrid, edge, and disconnected environments, RGS AI Suite creates a trusted compute fabric for mission-critical AI — all while meeting Zero Trust and federal compliance standards.


RGS AI Suite
RGS Security (NeuVector)
RGS Manager (Rancher)
RGS Observability (Stackstate)
RGS Application Collection
RGS HCI (Harvester Government)

Why RGS AI Matters

- **Unified Stack for VMs + Containers:** The RGS Suite bridges legacy virtual machines and modern AI/ML containerized workloads within a single, manageable platform—eliminating silos and accelerating AI adoption across hybrid environments.
- **Edge and Tactical Support:** The RGS AI runs on commodity hardware and supports disconnected, low-footprint edge deployments—ideal for DoD, IC, and field-intelligence scenarios requiring air-gapped LLM inference or secure data pre-processing at the tactical edge.
- **Kubernetes-Native by Design:** Built with Kubernetes at its core, the RGS AI integrates Rancher and RKE2 to orchestrate AI workloads, GPU pools, and secure storage from a centralized control plane, providing consistent management from cloud to edge.
- **Zero Trust Security for AI Pipelines:** The RGS AI delivers full-lifecycle container security—ensuring containerized AI workloads remain protected from build to runtime, even in classified or disconnected environments.
- **Built for Observability and Compliance:** RGS Observability tools deliver real-time performance metrics and anomaly detection across the stack, while maintaining alignment with government compliance mandates including STIG, FIPS, and CNSSI 1253. Special integrations for monitoring provide granular usage metrics to optimize GPU resource utilization.

- **Optimized for Inference and Training at the Edge:** With support for GPU passthrough, secure storage, and hardened networking, the RGS AI enables both AI inference and fine-tuning in forward-operating environments—without compromising control or mission assurance inference and even fine-tuning models in forward-operating environments — without compromising control or compliance.

Bottom Line: RGS enables agencies to run secure, compliant AI workloads not just in the cloud or on-prem, but anywhere the mission requires — from Sensitive Compartmented Information Facilities (SCIFs) to warfighters at the tactical edge. RGS AI is the infrastructure foundation for that vision.

RGS AI Platform Benefits

Capability	**RGS AI Platform Advantage**
Control Over Data	Run GenAI workloads within your agency's boundaries — no public training, no data leaks
Security-First Architecture	FIPS-validated modules, STIG compliance, secure-by-default container runtimes
Air-Gap Friendly	Deploy in disconnected environments for classified and sensitive use cases
Open Source, No Lock-in	Flexibility to use multiple LLMs and extend your stack without commercial limitations
Mission-Focused	Built by a cleared, U.S.-based team experienced with defense, IC, and civilian programs
Compliance Ready	Designed for Executive Order 14028, CISA S ecure-by-Design, and ATO pathways
Variable Workloads	Allows you to run VMs and Containers side by side

Use Cases for Government AI with RGS

- **DoD Tactical Edge AI:** Deploy containerized and/or VM based LLMs in disconnected environments using RKE2 + Carbide and RGS HCI (Harvester Government)
- **Intelligence Data Summarization:** Ingest, process, and interpret structured/ unstructured data privately

- **Civilian Agency Workflow Automation:** Accelerate Freedom of Information Act (FOIA), citizen response, or document intake securely
- **Cyber Threat Modeling and Detection:** Use AI safely within the cybersecurity kill chain
- **Law Enforcement Facial or Pattern Recognition:** Run LLM inference models in compliance with CJIS and other mandates

Application Enablement, Secured

RGS's secure container stack is already trusted and accelerating missions across the DoD, IC and Civilian agencies. That same infrastructure now supports secure, extensible AI enablement. Through Rancher Government Carbide, our product and solution benefits from:

- Embedded SBOMs
- Vulnerability scanning and attestations
- Continuous compliance checks
- STIGATRON (STIG validation at runtime)
- Offline documentation and edge deployment capability

This is not SaaS AI. This is sovereign AI, built for government mission needs.

Conclusion

The future of secure government operations depends on the ability to harness AI without compromising trust, security, or compliance. RGS provides the hardened, flexible, US based, infrastructure and services to deliver just that. No foreign-owned data centers or personnel. No black-box SaaS tools. Just enterprise open source innovation and choice, secured and tailored for US Government priorities.

It's your mission. It should be your infrastructure. And it must be your data.

Learn More

Visit www.ranchergovernment.com or contact us at info@ranchergovernment.com.

RGS
Rancher Government Solutions

Rancher Government Solutions (RGS) is a fully independent, wholly owned subsidiary of SUSE S.A., operating with a specialized focus on serving U.S. government agencies and their partners. RGS has a DCSA approved, FOCI-mitigated (Foreign Ownership, Control, or Influence) proxy structure, ensuring full operational independence from its parent company. This structure enables RGS to comply with U.S. government security, compliance, and regulatory requirements, including those related to classified and sensitive workloads. All RGS products, services, and engagements are tailored to meet federal cybersecurity and operational mandates, ensuring trusted, mission-ready solutions for U.S. government customers.

For more information, contact RGS at:
844-RGS-7779

Rancher Government Solutions
1900 Reston Metro Plaza, Suite 600
Reston, VA 20190
USA

www.ranchergovernment.com

Commercial and Government Entity
(CAGE) Code: 8GLZ3