

Secure AI for the Modern State Department

A Mission-Ready Platform by Bart & Associates

A Secure, IL5-Capable AI Platform to Accelerate the Mission

Bart & Associates has developed an AI platform on AWS GovCloud that automates critical workflows, delivering significant efficiency gains while ensuring total data sovereignty and FedRAMP-ready security.



Secure

Built for Impact Level 5 (IL5) on AWS GovCloud. All data remains within U.S. government boundaries, operated by U.S. citizens.



Efficient

Proven to reduce manual work by over 80% in high-stakes use cases, enabling faster and more accurate decisions.



Compliant

Designed to meet FedRAMP High, ITAR, and appropriations law requirements with complete, immutable audit trails.

Use Case 1: From Hours to Seconds with AI-Powered Export Control Compliance

The Challenge

State Department personnel spend hours manually researching hundreds of pages of ITAR and EAR regulations. This process is slow, error-prone, and creates bottlenecks in licensing decisions.

Our Solution

An AI-powered RAG system that provides instant, cited answers to natural language questions. Users can ask, *"Do I need a license to export thermal cameras to Mexico?"* and receive a precise response.

The Impact

- Reduces research time from hours to seconds.
- Provides answers with direct regulatory citations (e.g., ITAR § 121.1, Category XII).
- Displays confidence scores and allows source text verification.
- Creates a full audit trail for compliance.

Do I need a license to export thermal cameras to Mexico?



Generated Answer

Yes, a license is likely required. Thermal cameras are controlled under ITAR § 121.1, Category XII(c) as significant military equipment. Export to Mexico requires specific authorization from Directorate of Defense Trade Controls (DDTC).

CITATION: ITAR § 121.1, Category XII

CONFIDENCE: HIGH

Use Case 2: Automating Appropriations Law for Event Funding

The Challenge

Certifying officers must manually classify invoice line items against complex appropriations law (31 U.S.C. § 1301, § 1341), a high-risk and error-prone process.

Our Solution

An automated tool that analyzes event documents (invoices, seating charts) and applies a 6-step legal logic to allocate funding between EDCS, DP, and EOP accounts.

The Impact

- Reduces manual classification time by 80%.
- Ensures compliance and protects certifying officers from liability (per 31 U.S.C. § 3528).
- Automatically generates reimbursement memos and flags items for legal review.



The B&A Secure AI Foundation: The Engine Behind Our Solutions

The previous use cases are not standalone tools. They are applications built upon a reusable, secure, and scalable platform designed specifically for sensitive government AI workloads on AWS GovCloud.

**Export Control
Compliance**

Event Funding Tool

Future Use Cases

B&A Secure AI Foundation on AWS GovCloud (IL5)

A Fortress for Government Data: Security by Design



Network Security

- VPC with private subnets
- No public internet access for compute
- VPC endpoints & least-privilege security groups



Data Protection

- FIPS 140-2 validated encryption at rest (KMS)
- TLS 1.2+ encryption in transit
- Regular key rotation



Access Control

- IAM roles with least-privilege principles
- Mandatory MFA
- Service-to-service authentication, no long-term credentials



Audit & Compliance

- Immutable audit trails via AWS CloudTrail
- Logging of all API calls
- 5-year retention policy



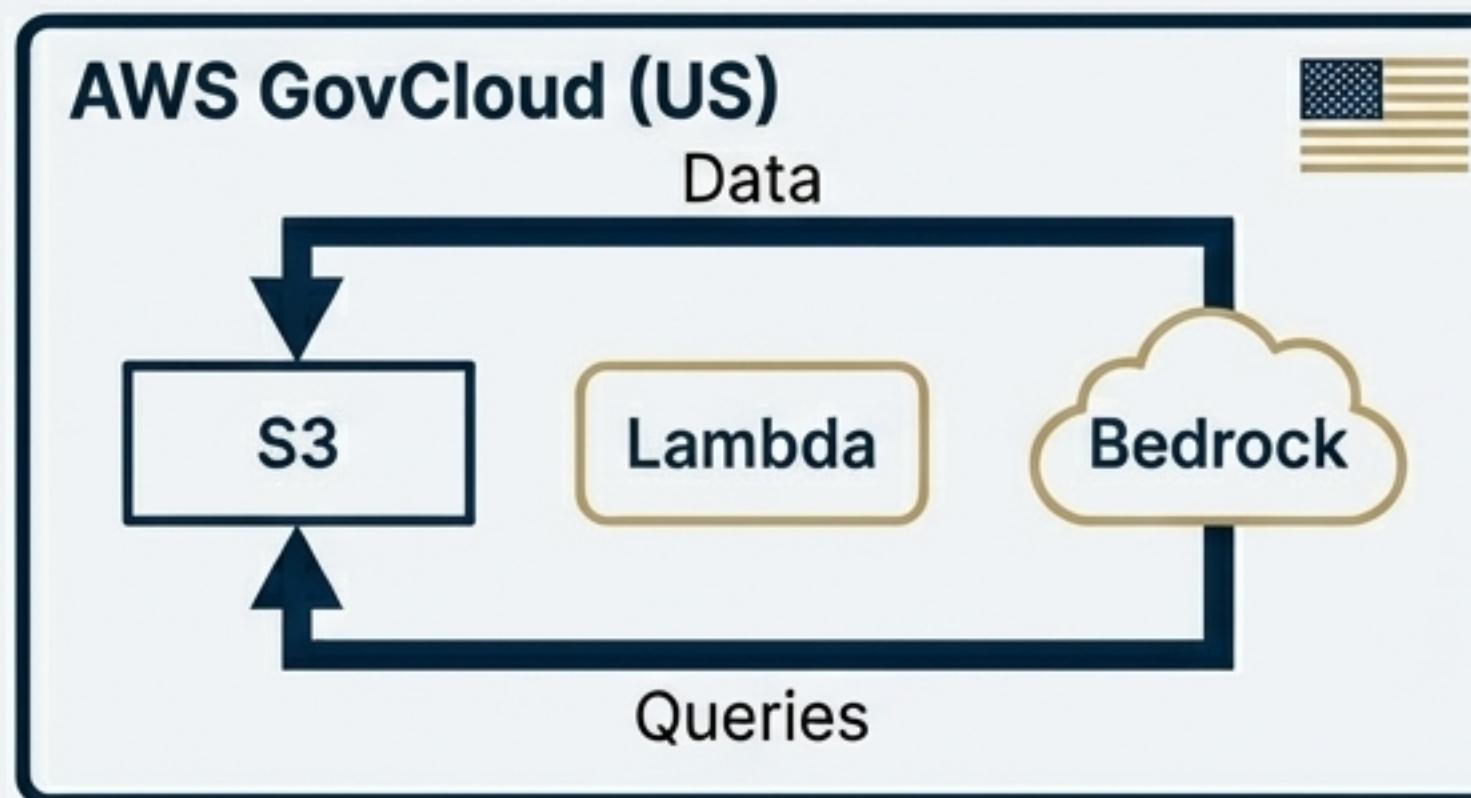
AI Security

- LLM operations via AWS Bedrock (data never leaves AWS)
- Prompt injection protection & output validation
- No data sent to public AI services

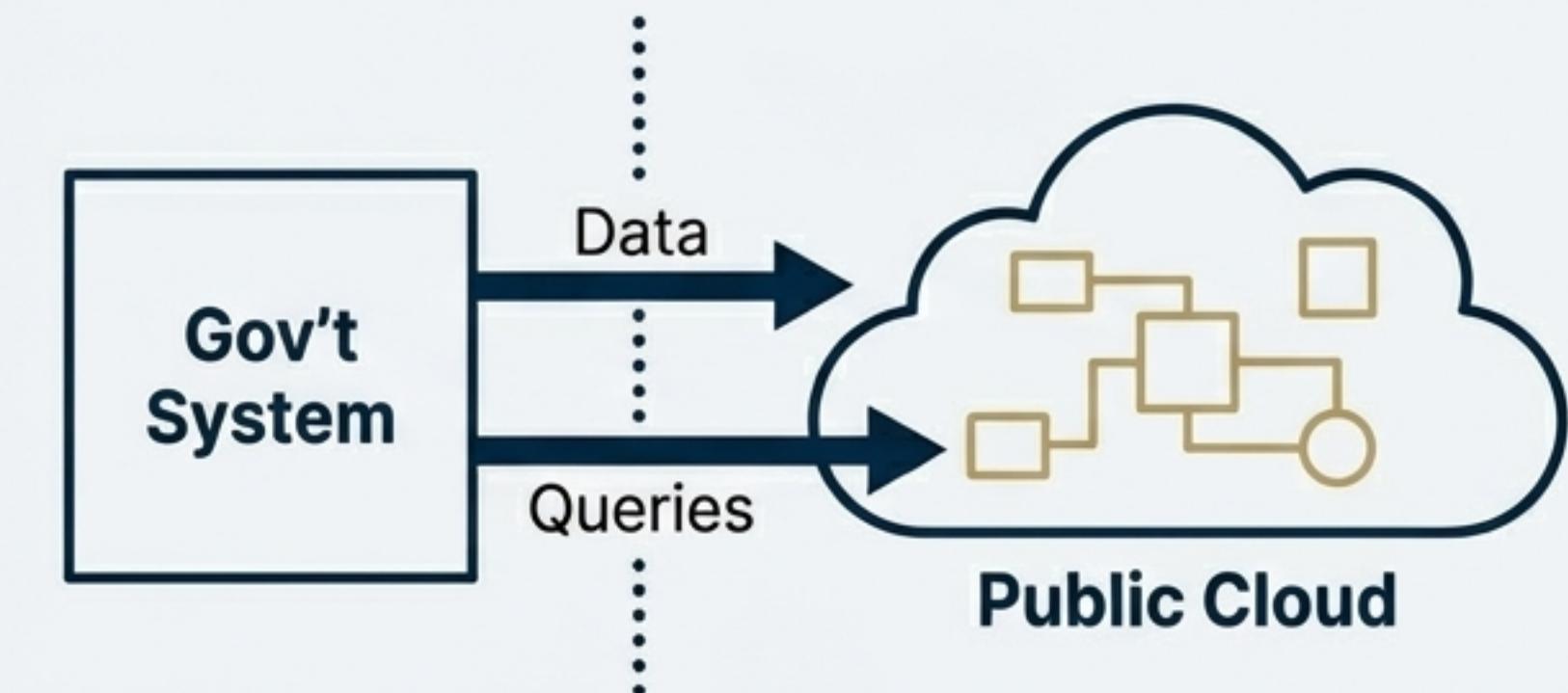
True Data Sovereignty is Non-Negotiable

All data, from documents to queries, remains within U.S. government boundaries, physically and logically separated from **commercial cloud regions** and **operated by U.S. citizens on U.S. soil**.

B&A Secure AI Foundation



Public AI APIs (ChatGPT, Public Claude API, etc.)



- ✓ Data remains within AWS GovCloud boundary.
- ✓ Operated by vetted U.S. citizens.
- ✓ ITAR and FedRAMP compliant environment.
- ✓ Data is never used for third-party model training.

- ✗ Data leaves the government boundary.
- ✗ Data may be processed in commercial regions globally.
- ✗ Not inherently ITAR or IL5 compliant.
- ✗ Data usage policies can be ambiguous.

Built with Best-in-Class, Enterprise-Grade Technology

AI & Machine Learning Layer



AWS Bedrock

For LLM access (Claude 3 Sonnet/Opus) and semantic embeddings (Amazon Titan).
A FedRAMP authorized service.



Amazon OpenSearch Service

For k-NN vector search and hybrid search capabilities.

Infrastructure & Data Layer



AWS Lambda

For serverless, auto-scaling compute within a VPC.



Amazon S3

For secure, encrypted document storage.



Amazon API Gateway

For secure API access with IAM authentication.



CloudWatch & CloudTrail

For comprehensive monitoring and auditing.

Our Competitive Edge: Purpose-Built for Government



True Data Sovereignty: All data and operations remain within AWS GovCloud.



FedRAMP Ready & IL5 Capable: Built from the ground up to meet FedRAMP High and support CUI and ITAR data.



No Vendor Lock-In: Architecture uses open standards and can be adapted.



Scalable & Extensible: Designed as a platform to host many future AI solutions.



Complete Audit Trail: Every query, response, and system action is logged for compliance and oversight.

Meeting Rigorous Compliance and Governance Mandates



Regulatory Compliance

Federal Requirements

- Adheres to FedRAMP High baseline, FISMA, NIST 800-53 security controls, and FIPS 140-2 cryptography.

Department-Specific

- Built for ITAR compliance, understands Appropriations Law (31 U.S.C.), and adheres to State Department security and records retention policies.



Data Governance

Classification Handling

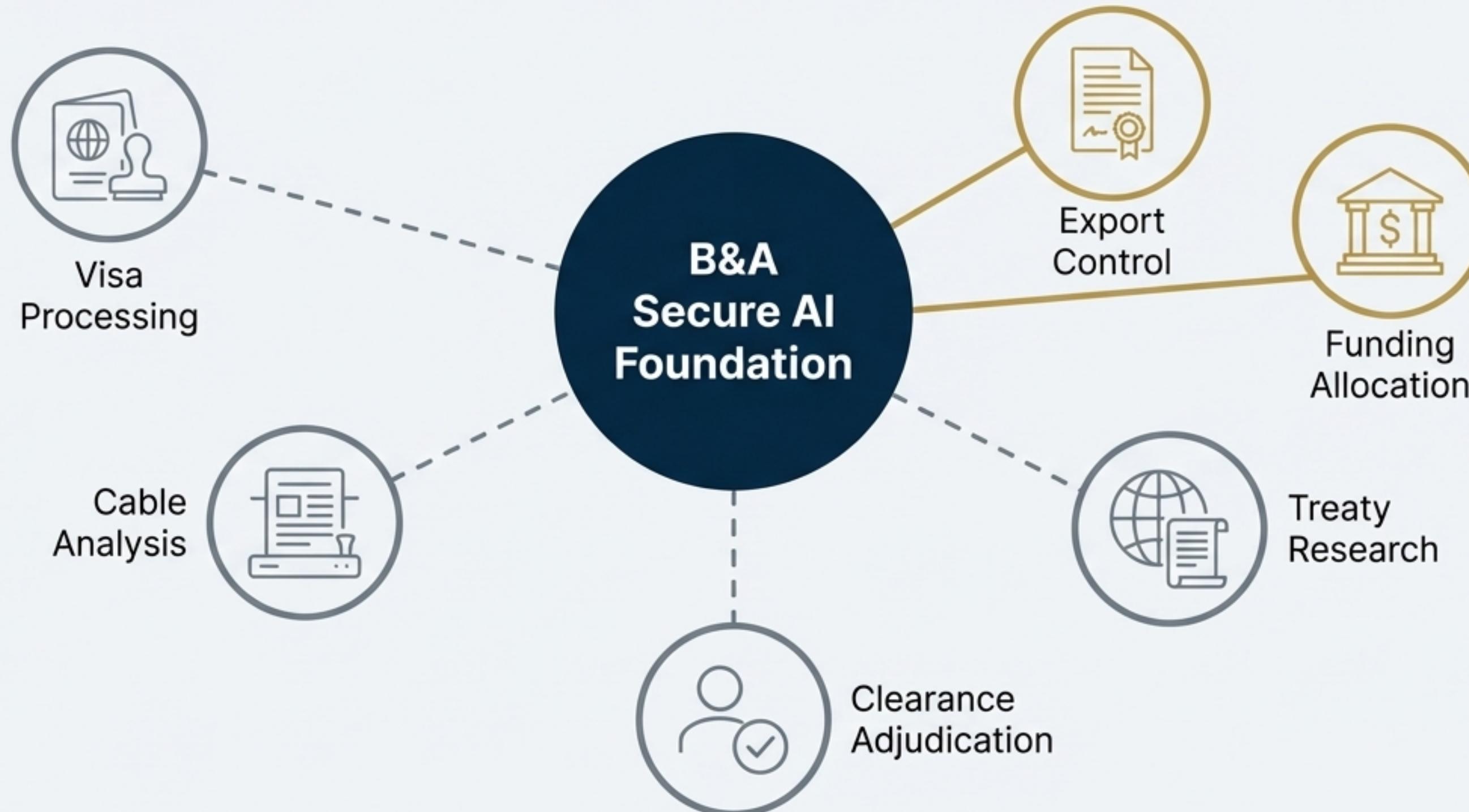
- Designed for Controlled Unclassified Information (CUI), ITAR-controlled technical data, and Sensitive But Unclassified (SBU).

Data Lifecycle

- Automated data retention policies, secure deletion protocols, and version control for audit trails.

A Platform for the Future of State Department Operations

The Secure AI Foundation is a strategic asset that reduces costs and accelerates the deployment of new capabilities across the Department.



Smart, Scalable, and Cost-Efficient by Design

Serverless Architecture Benefits

- Pay only for actual usage—no idle infrastructure costs.
- Automatically scales to meet demand.
- Reduced operational overhead for your team.

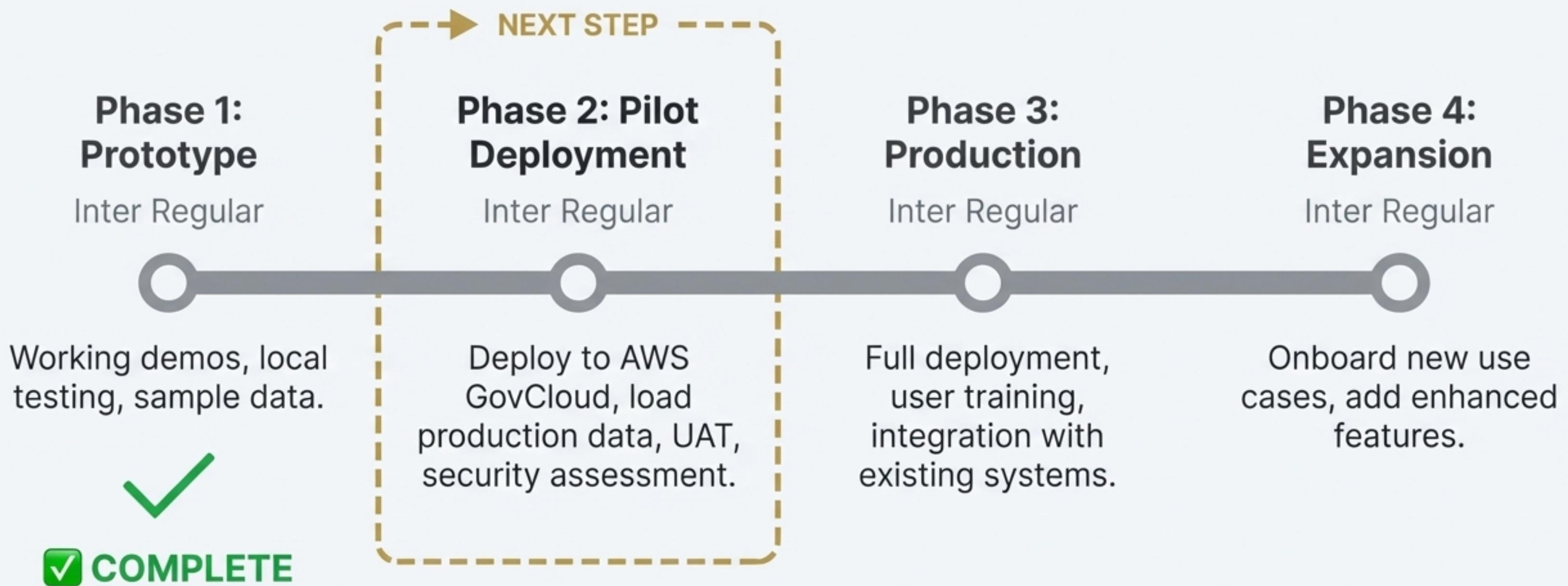
Estimated Monthly Costs (per use case)

Deployment Size	Estimated Cost
Small (1,000 queries/mo)	~\$500
Medium (10,000 queries/mo)	~\$850
Large (100,000 queries/mo)	~\$3,500

Compelling Return on Investment

This investment delivers significant returns by reducing manual work by **80%+**, eliminating costly errors, and accelerating mission-critical decision-making.

Our Phased Approach to Deployment



The New Paradigm for Government AI

The B&A Secure AI Foundation is purpose-built for the unique requirements of the **U.S. Department of State**, delivering on the promise of AI with the security and compliance government missions demand.

-  **Security:** IL5-capable infrastructure with FedRAMP-ready controls.
-  **Compliance:** Meets federal and department-specific mandates.
-  **Efficiency:** Reduces manual work by 80%+ while improving accuracy.
-  **Scalability:** A platform ready to host future AI use cases.
-  **Data Sovereignty:** All data remains within U.S. government boundaries.

Next Steps & Discussion

Bart & Associates

Secure AI Solutions

contact@bart-associates.com

(202) 555-0182

www.bart-associates.com

Specialized Contacts

For Technical Questions

[Name of Technical Contact]

Lead Solutions Architect

tech-contact@bart-associates.com

For Security & Compliance

[Name of Security Contact]

Chief Information Security Officer

security-contact@bart-associates.com