A Super Intelligence QSMO?

Issues and Considerations for Discussion

Mark A. Forman

10/22/2026

Objective: Create a fact-based discussion on whether the federal government should take a shared services approach to AI/SI

Agenda

- Market Overview & Trends
- Key Issues and Consideration
- Example QSMO Deployment Concept
- Costs, Benefits, and Risks Compared to a Siloed Approach

Overview

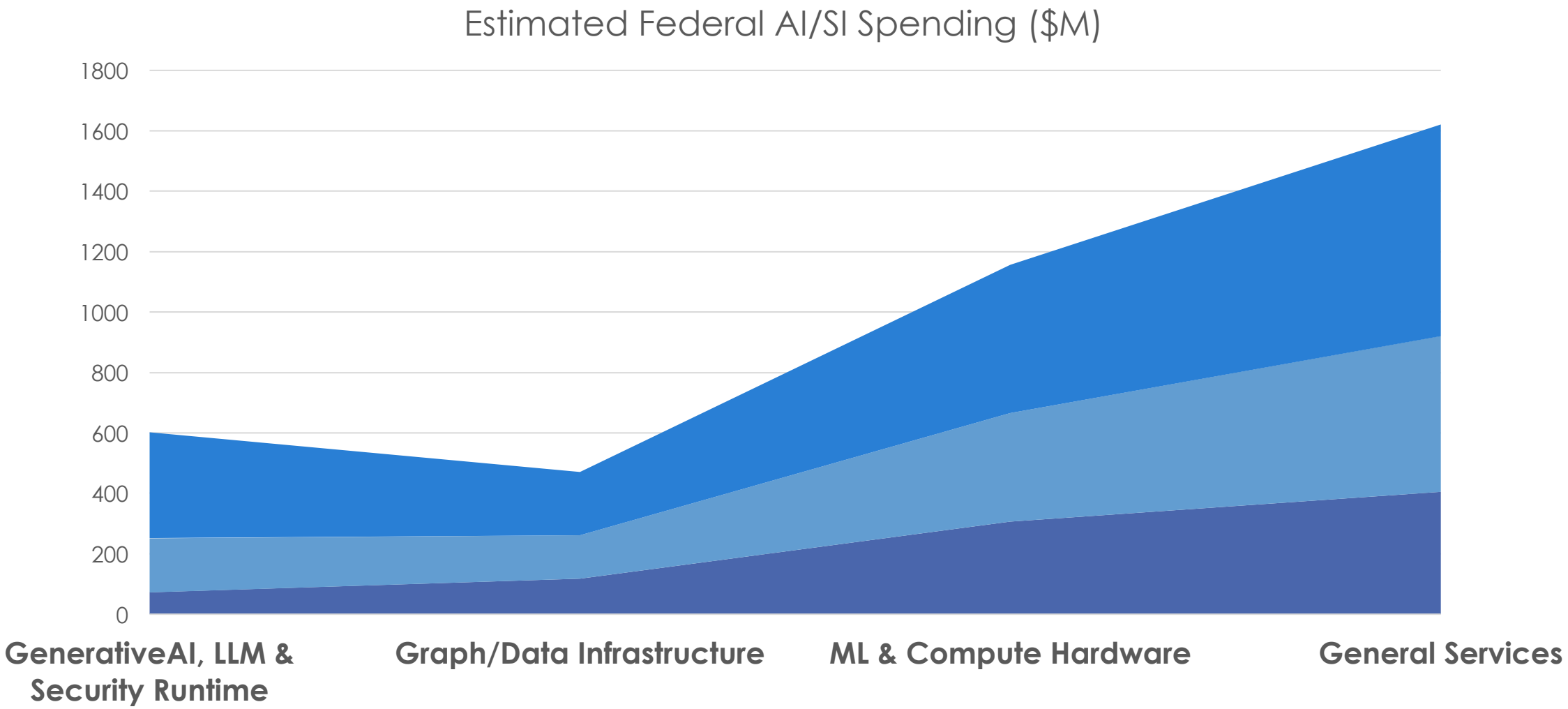
The Federal government spent an estimated $5.5B on Artificial Intelligence(AI)/Super Intelligence (SI) in FY24-FY26.

The current SI procurement model is highly fragmented—characterised by duplicated model licensing, redundant graph/vector database deployments, and uncoordinated cloud compute purchases across 40+ civilian and defense agencies.

Establishing a dedicated AI Quality Service Management Office (QSMO) would consolidate disparate buys into a unified shared service marketplace that leverages economies of scale, accelerates access, while simplifying risk management.

Operating across multi-cloud (AWS, Azure, Google) and government private clouds, a QSMO could generate a 33% cost reduction (over 3 years) while establishing effective security governance via runtime sandboxing.

Market Overview & Trends

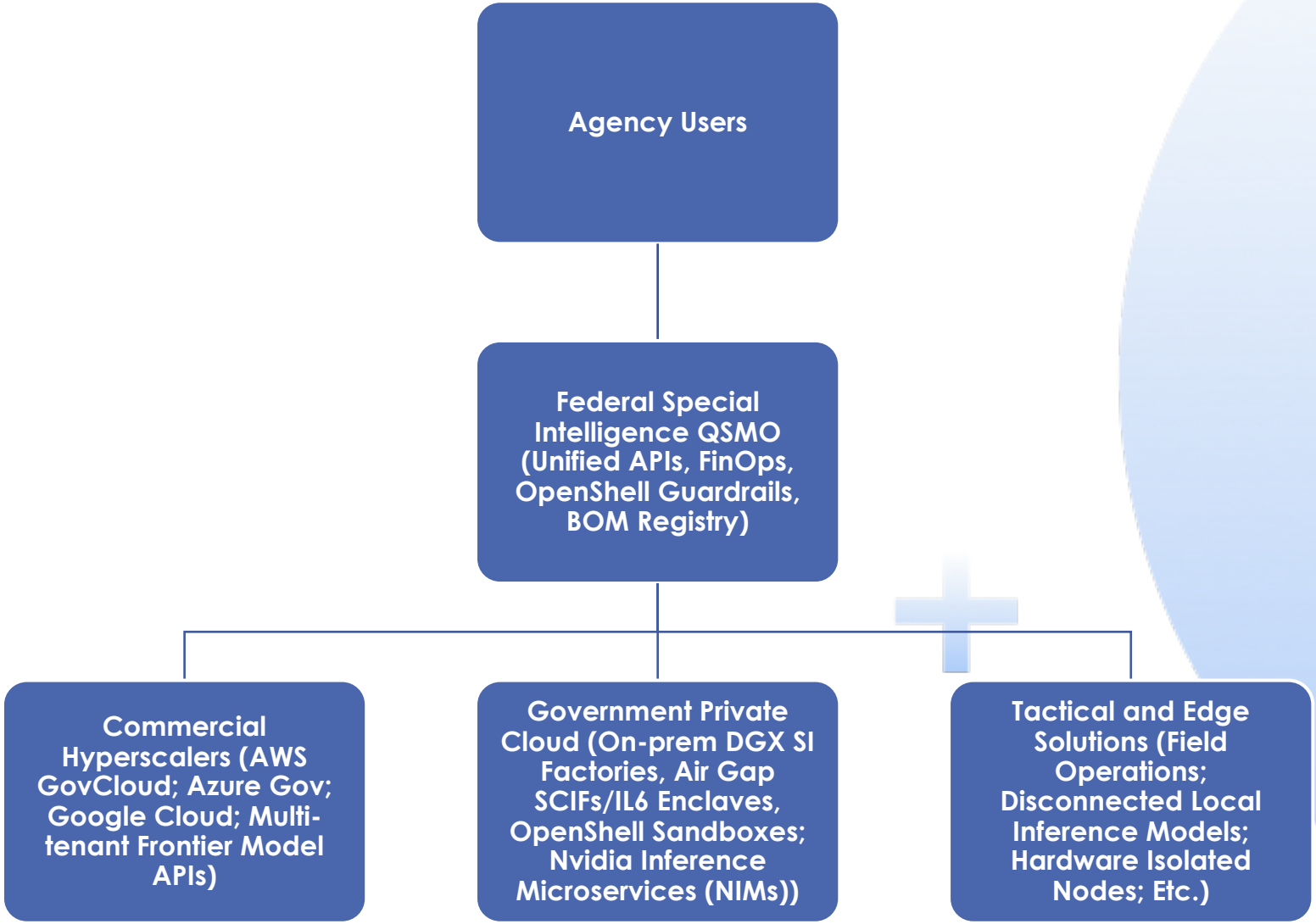


Source: calculated using GSA and industry pricing data with federal IT spending data

Key Issues and Consi-derations

- **Agencies moving from pilots to operations:**
  - Redundant Costs Are Highest in Experimentation Stage of New Technologies
  - Speed of Cost Reduction Is Driven By Ability to Leverage Shared Lessons Learned
- **SI Compute is Infrastructure Intensive, expensive, and subject to economies of scale**
- **Risk management requires governance standards implemented in both infrastructure and activities**
  - Hallucination risks can be controlled by automated grounding checks via Retrieval-Augmented Generation (RAG) and real-time output validation guardrails
  - Algorithmic bias, vulnerabilities, least privileged access, and privacy controls can be systematically implemented
  - Consistency in Bill of Materials (BOM) and activity tracking/logging/auditing

Possible Deployment Concept



Considerations in a SI QSMO Concept -- Costs, Strategic Benefits & Risks

Y1 SETUP CAPEX
$45M–$65M

NET COST REDUCTION
~33%

1. Required Investment

Y1 Setup CapEx: $45M–$65M
API switchyard, GitHub CI/CD, OpenShell controls.

Annual OpEx: $25M–$35M
Platform engineering, security monitoring, FedRAMP maintenance.

Agency Migration: $15M–$20M
Legacy API integration and technical workforce enablement.

2. Strategic Benefits

Affordability
Tier-4 enterprise volume pricing via GSA/FAS buying power.

Cost Reduction
Removes $300M+ in redundant agency vector DB & tool buys.

Unified Governance & Alignment Risk Control
Enforces NIST AI RMF & OMB M-24-10 via automated guardrails, AI-BOM provenance, and accelerated ATOs.

3. Risks & Mitigations

Agency Adoption Resistance
Mitigation: Enforce OMB Circular A-11 budget clearing controls.

Vendor & Model Lock-In
Mitigation: Mandatory model-agnostic API switchyards.

Multi-Tenancy Data Leakage
Mitigation: Deploy zero-trust enclaves and customer keys.