National-Scale AI: Building U.S. Infrastructure, Innovation, and Security

Paul F. Roysdon, Ph.D.

September 8, 2025

1 Executive Summary

The rapid evolution of Artificial Intelligence (AI) presents both an unprecedented opportunity and an urgent imperative for U.S. national security. This document outlines a comprehensive, Intelligence Community-focused blueprint to harness AI's transformative power – securing America's strategic advantage, protecting critical infrastructure, and accelerating decision-cycle dominance.

1. **AI as a Core IC Capability**
   AI is reshaping every phase of intelligence: collection, processing, analysis, and strategic warning. Frontier models now approach general-purpose reasoning – enabling automated translation, imagery interpretation, anomaly detection in signals, and rapid open-source exploitation. To maintain sovereign control, the IC must own and operate the compute platforms, data pipelines, and governance frameworks that underpin these capabilities, rather than rely solely on commercial tools.

2. **Governance & Accountability**
   A clear, tiered governance structure is essential:

   - Model Oversight under the IC Chief AI Officer (CAIO) Council, supported by interagency working groups, to approve architectures, convene Model Review Boards, and maintain a certified-model registry.
   - Data Stewardship under the IC Chief Data Officer and Data Council to set classification, access controls, retention policies, and operate a federated metadata catalog.
   - Networks & Infrastructure under the IC Chief Information Officer to design and manage HPC campuses, regional edge pods, and secure multi-cloud fabrics with zero-trust networking and vendor-neutral storage.

3. **Sovereign Infrastructure Deployment**
   A tiered data-center strategy will deliver resilience and scale:

   - Tier 1: Exascale-class HPC clusters (e.g., Fort Meade) for classified model training.
   - Tier 2: Regional edge pods at mission hubs (e.g., NGA, DIA) with petaflops of inference capacity.

   - Tier 3: Ruggedized field appliances for deployed SIGINT/IMINT teams. All tiers share a high-throughput, encrypted object-store fabric (>100 PB), sub-millisecond metadata, and federated learning interconnects over the IC ITE backbone.

4. **Strategic Industry Partnerships**
   To access the latest foundation models and expertise:

   - Negotiate secure-enclave licenses with companies like Google, Microsoft, and Meta for model customization.

   - Embed joint "AI Research Hubs" alongside companies like DeepMind, OpenAI, and FAIR to co-develop explainability, robustness, and adversarial defenses.

   - Partner with companies like Palantir and Scale AI for data-lakehouse orchestration and rapid, high-quality dataset annotation pipelines.

5. **Accelerated Acquisition & DevSecOps**
   Streamlined procurement and continuous security are vital:

   - Adopt modular, performance-based contracts and expand Other Transaction Authorities for rapid AI prototyping.

   - Form a cross-agency "AI Tiger Team" to compress reviews into 30-day sprints and issue "AI Acquisition Passports" for pre-cleared vendors.

   - Transition to a continuous ATO model with DevSecOps pipelines and tiered assurance levels aligned to mission criticality.

By integrating robust governance, sovereign infrastructure, strategic partnerships, and agile acquisition, the Intelligence Community can fully leverage AI to outpace adversaries, secure critical systems, and deliver timely, actionable intelligence. This national-scale AI effort is essential to preserve American leadership and protect our democracy in an increasingly contested global landscape.