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

Paul F. Roysdon, Ph.D.

March 8, 2025

1 Introduction

Artificial Intelligence (AI) has emerged as a transformative general-purpose technology reshaping industries and national power. The United States, long a global leader in AI, now faces the imperative of a **national-scale effort** to sustain that leadership and harness AI across society. Realizing AI's full potential "requires the combined efforts of industry, academia, and government," as the Trump White House emphasized, to accelerate innovation for the benefit of the American people [1]. Indeed, the Trump Administration's official strategy recognized that **continued American leadership in AI is "of paramount importance to maintaining the economic and national security of the United States"** [1]. This paper argues that a coordinated national endeavor – spanning cutting-edge technical infrastructure, **broad economic adoption**, forward-looking **policy frameworks**, and **strategic applications** – is needed to develop AI systems and apply them in domains like intelligence analytics, event prediction, insider threat detection, cybersecurity, and critical infrastructure protection. Both government leadership and private-sector collaboration are essential to build an AI ecosystem that **secures America's future competitiveness and national security**.

2 Technical Implications: Infrastructure and Innovation

Keeping the U.S. at the forefront of AI requires massive investment in **AI infrastructure** – from high-performance computing and cloud resources to large-scale data and cutting-edge algorithms. Modern AI breakthroughs (e.g. training advanced Large Language Models [LLMs]) demand vast computational power and data; currently, this is a **major advantage held by tech giants**, whose resources often exceed those of academia or government labs [4]. Leading scientists have warned that the U.S. is "**unprepared to reap many of the economic and societal benefits offered by AI**" because our research infrastructure and funding have not kept pace with the rapid advances [4]. To close this gap, experts like Fei-Fei Li and John Etchemendy propose bold initiatives such as a **National Research Cloud** to provide researchers with shared high-performance computing and datasets [4]. Federal leadership can catalyze such infrastructure: early steps by Washington – including an AI R&D investment boost to nearly $1 billion in 2020 and an Executive Order updating federal AI research strategy – were encouraging but "not nearly enough" to meet the long-term challenge [4].

In addition to compute infrastructure, a national AI effort must support research into next-generation AI **models and algorithms**. Breakthroughs in areas like explainable AI, safe autonomy, and advanced machine learning will come from sustained R&D across government, universities, and industry. The **federal government's role is pivotal** in funding foundational research and setting standards: the 2019 American AI Initiative explicitly tasked agencies to facilitate AI R&D and develop technical standards for safe AI deployment [2]. This includes ensuring open datasets and testbeds are available to researchers and businesses [2]. By seeding ambitious projects (analogous to the Apollo program or the Human Genome Project), the U.S. can drive technological breakthroughs and train a new generation of AI scientists and engineers. The payoff is not only scientific leadership but also the tools to tackle national challenges with AI. For example, improving the **AI workforce** is part of the technical imperative: investments in STEM and computer science education are needed so that American talent can build and operate advanced AI systems [4]. In short, the U.S. must treat AI innovation as critical infrastructure – funding it, sharing it, and safeguarding it as a strategic resource.

3 Economic Implications: Competitiveness and Business Adoption

Economically, AI is poised to deliver enormous productivity gains and new capabilities across industries. Analysts estimate AI could contribute **trillions of dollars to the economy** in the coming decade. One study by PwC projects **$15.7 trillion in global economic gains by 2030** [10] due to AI, reflecting its potential to usher in an era of widespread prosperity [4]. Nations that lead in AI are expected to capture a disproportionate share of these benefits: **leading AI countries might gain 20-25% in additional net economic benefits**, versus only 5-15% for developing countries [4]. Simply put, **falling behind in AI will have "disastrous effects on a nation's prospects,"** hurting growth and competitiveness [4]. For the United States, this means a robust national AI strategy is not just about tech leadership but also about long-term economic vitality and middle-class jobs.

Business analytics exemplifies how AI can drive economic innovation. Companies are increasingly deploying AI algorithms to analyze big data for insights – improving customer targeting, optimizing supply chains, and discovering efficiencies unreachable by manual analysis. AI systems can forecast market trends or consumer behavior (i.e. **event prediction** in commerce) with a speed and accuracy that give firms a competitive edge. Recent research even shows that combining multiple AI models can predict complex outcomes (like political or economic events) **on par with expert human forecasters**, offering faster and cheaper decision support for organizations [5]. As one scholar noted, AI-driven predictions are "changing how we think about forecasting entirely," enabling smarter business and policy planning [5]. However, not all firms have equal access to AI capabilities. This creates a gap between "AI haves and have-nots" [4]. A national effort can help **democratize AI for businesses**, for example through public-private partnerships that provide smaller companies and startups access to AI research, tools, and skilled talent. If only a few big tech firms dominate AI, the benefits will concentrate and many sectors may be left behind [4]. Thus, U.S. policymakers must promote broad AI adoption – via tax incentives, education, and dissemination of best practices – to ensure that every sector from manufacturing and agriculture to finance and healthcare can leverage AI. The economic promise of AI (higher productivity, new products and services, and even entirely new industries) will be fully realized only if we address implementation barriers and skill gaps across the business landscape [4].

4 Policy Implications: National Strategy and Public-Private Collaboration

Capitalizing on AI's potential requires forward-looking **policy and governance**. The United States needs a cohesive **national AI strategy** that coordinates efforts across federal agencies, state and local governments, academia, and industry. In 2019, President Trump launched the American AI Initiative, declaring it "the policy of the United States Government to sustain and enhance" U.S. scientific, technological and economic leadership in AI through a **coordinated federal strategy** [2]. This marked a starting point: it directed agencies to prioritize AI R&D, open up data resources, and foster international cooperation [2]. Likewise, the Trump Administration convened summits with industry to shape policy. As **CTO Michael Kratsios** explained at the White House AI Summit, "our free market approach to scientific discovery harnesses the combined strengths of government, industry, and academia" to advance AI for the nation's benefit [3]. This principle of **public-private collaboration** is central: **the U.S. government recognizes it must partner with tech companies and universities** rather than try to direct innovation alone. The 2018 AI Industry Summit, for instance, brought together over 100 senior officials, top academics, and business leaders, underscoring the "commitment of the Trump Administration to leverage AI across agency missions ... and enable American industry to continue to lead the world." [3] Key policy areas include **funding and incentives**, regulatory frameworks, and setting **ethical guidelines**.

On funding, government can stimulate AI research in areas with broad public benefit (such as AI for healthcare, climate, or security) that may be underinvested by the private sector. Strategically, experts have urged much larger federal investments – on the order of a new "Sputnik" moment. Tech leader Eric Schmidt argued that AI is now so vital to future power that "the United States needs a national strategy on artificial intelligence, just as it had one for the development of space technology during the Cold War." [9] This call echoes across the policy community: just as past generations built interstate highways and sent humans to the Moon, today's leaders must make AI a national mission. Congress has begun to respond (for example, authorizing a National AI Research Resource to broaden academic access to computing), but a more comprehensive strategy is still coalescing. In shaping this strategy, policymakers also have to address **governance and ethics** – ensuring AI systems align with American values of privacy, fairness, and transparency (**"AI with American Values," in President Trump's parlance** [1]). This includes updating legal and regulatory frameworks to accommodate AI in areas like autonomous vehicles, finance, or medicine, without stifling innovation. The U.S. can leverage its strengths – a vibrant private sector, top universities, and democratic institutions – to craft a model of AI development that is **responsible and accessible**, guarding against misuse (such as bias or threats to privacy) while pushing the frontiers of innovation [4]. In sum, sound policy and leadership will set the stage for America's AI trajectory, and that requires a partnership of government vision with industry agility.

5 Strategic Implications: AI and National Security

Perhaps the most compelling reason for a national-scale AI effort is to secure the United States' future in terms of **national security and global strategic leadership**. AI is widely seen as a game-changer in military and intelligence affairs – so much so that rivals frame it as an arms race. In early 2018, Russia's President Putin famously remarked that "whoever becomes the leader in [AI] will become the ruler of the world." World leaders recognize that AI will revolutionize military power, espionage, and defense. The U.S. National Security Strategy (2017) accordingly identified AI as a key technology, and **President Trump affirmed that AI advancement "enhance[s] our economic and national security"** [2]. The Defense Department has initiated programs to integrate AI, from battlefield decision support to autonomous systems. **Existing AI capabilities already offer significant national security benefits** – for example, today's machine learning can automate labor-intensive tasks like analyzing satellite imagery or detecting cyber intrusions, dramatically improving intelligence and defense operations [7]. An influential Harvard Belfer Center study argued that future progress in AI could be as transformative to warfare as the advent of nuclear weapons or aircraft, potentially "**a turning point in the use of automation in warfare**." It highlighted that AI will impact **military superiority, information dominance, and even economic superiority** in international competition [7].

Critically, America's strategic competitors are mounting their own national AI drives.

- **China**, for instance, announced a national AI strategy in 2017 declaring AI a "major strategic opportunity" and outlining plans to achieve world-leading status by 2030 [9]. Beijing has invested heavily in AI research, startups, and military applications, aiming to leverage its huge data resources and talent pool.

- **Russia** is likewise pursuing AI for military use (from autonomous drones to AI-guided missiles) [9].

Allies and adversaries alike see AI as foundational to future security. In this context, maintaining U.S. leadership in AI is a strategic necessity to avoid being eclipsed technologically. American officials and experts increasingly describe the situation as a **race** not just for economic gain but for safeguarding the free world's values and security [9]. As retired General John Allen warned, the U.S. must do more to "get and stay ahead" in AI, lest we wake up to find the balance of power tilted to authoritarian regimes [9].

Beyond military competition, AI is vital for **domestic security and critical infrastructure protection**. AI tools can dramatically strengthen cybersecurity by identifying network intrusions and malware faster than human analysts. In fact, **AI-driven anomaly detection is already used by critical infrastructure** providers to flag malicious cyber activities in power grids, financial systems, and other vital networks [8]. These capabilities help defend against state-sponsored hackers and cyber criminals targeting U.S. infrastructure. At the same time, as sectors like energy and transportation adopt AI for automation and optimization, we must manage new risks (e.g. vulnerabilities in AI systems themselves) [8]. Another area of growing concern is **insider threats** – malicious actors within an organization who steal data or sabotage systems. Such threats are notoriously hard to detect, but machine learning models can analyze user behavior logs to spot anomalies that might indicate an insider attack. Research confirms that "insider threats pose a critical challenge" to organizations and that AI-based detection systems, while promising, need further development to reliably catch these subtle threats [6]. By investing in AI solutions for cybersecurity, **NSA** can better **protect government and industry networks from espionage and disruption**. Likewise, AI can aid in **predictive intelligence** for national security – analyzing vast streams of data (social media, economic indicators, etc.) to **predict events** such as political instability, terrorist activity, or pandemic outbreaks. For instance, ensemble models of multiple AI systems have shown success in forecasting geopolitical events and could augment human analysts in agencies like the **CIA** [5]. In short, from the Pentagon to critical infrastructure operators, deploying AI is becoming essential to stay ahead of threats. A national AI effort focused on security would ensure that law enforcement, intelligence, and defense communities have access to the best AI tools and expertise to keep America safe. As **President Trump's administration declared, advancing AI is "of paramount importance" to America's national security** [1] – it underpins our military edge, cyber defenses, and resilience against emergent threats.

6 AI Necessity in the Intelligence Community

Artificial Intelligence is transforming the nature of intelligence itself. The exponential growth of data, the increasing speed and complexity of threats, and the rise of strategic competitors leveraging AI at scale demand a fundamental rethinking of how the Intelligence Community (IC) collects, analyzes, and delivers insight. This is not an incremental shift it is a foundational transformation. The IC must not simply adapt to AI; it must lead in shaping and securely deploying it in support of U.S. national interests.

As the integrator and strategic coordinator of U.S. intelligence, the Office of the Director of National Intelligence (ODNI) has a central role to play. ODNI must ensure the IC both harnesses and secures artificial intelligence at every level of mission execution from collection to analysis to strategic warning. The rapid development of frontier AI large-scale, general-purpose models capable of multi-domain reasoning introduces both operational opportunity and strategic risk. ODNIs leadership is essential to responsibly accelerating AI adoption while safeguarding national security equities.

Frontier AI is reshaping the strategic landscape. These models trained on trillions of tokens and comprising hundreds of billions of parameters now approach general-purpose reasoning and are increasingly relevant to core intelligence workflows: translation, summarization, imagery analysis, cyber defense, and open-source exploitation. Their power lies not just in speed, but in their ability to operate across modalities and adapt to new contexts.

Critically, the IC cannot outsource its future AI capabilities. The models that will matter most will not come from commercial tools designed for consumer use. They will emerge from systems trained on sovereign data, hosted in secure environments, and tailored to intelligence missions. Ensuring access to such models requires owning and operating the infrastructure compute, data pipelines, and model governance that enables them.

Why This Matters Now: China's national AI strategy explicitly prioritizes sovereign compute and end-to-end model development. Peer and near-peer nations including the UK, UAE, and South Korea are investing heavily in national-scale datacenters to reduce reliance on U.S.-based cloud providers. If the United States is to remain the global leader in intelligence and innovation, it must not only lead in algorithms and research it must also ensure strategic control over the infrastructure that makes them operational.

7 AI Roadmap for the Nation

To meet the extraordinary scale of AI demand, the Executive Office of the President (EOP) must establish a **sustained, whole-of-government coordination mechanism** that extends beyond traditional national security bodies. In addition to the National Security Council (NSC), National Economic Council (NEC), Office of Science and Technology Policy (OSTP), and Office of Management and Budget (OMB), the **Domestic Policy Council (DPC)** must be elevated as a core partner. Although the DPC typically focuses on domestic welfare issues, its leadership will be indispensable for **modernizing the power grid and accelerating next-generation energy infrastructure** – two prerequisites for high-capacity AI compute and data centers.

No single federal agency can underwrite or direct the vast energy build-out required to fuel exascale-class AI systems. Congress, state public utility commissions, and local permitting authorities collectively control transmission rights, siting approvals, and cost-recovery models for utilities. As such, the DPC should lead an integrated task force charged with:

- **Aligning Regulatory Incentives**: Coordinate federal and state regulators to harmonize permitting timelines, streamline interconnection standards, and incentivize utilities to prioritize capacity upgrades that directly support AI data-center campuses.
- **Modernizing Permitting Processes**: Build on the recent Executive Order on permitting reform by creating a permanent "AI Infrastructure Permitting Council" within the DPC – empowered to fast-track critical-path approvals, resolve cross-jurisdictional disputes, and establish uniform environmental and reliability standards.
- **Shaping Financial Incentives**: Work with OMB and NEC to design federal grant-and-loan programs that de-risk private capital investment in grid modernization, including conditional tax credits for utilities that commit to providing high-density, low-latency power to AI facilities.
- **Syncing Policy and Infrastructure Timelines**: Institute a rolling, multi-year roadmap – approved by the EOP councils – to ensure that energy-sector rulemakings, budget appropriations, and regional grid upgrades occur in lockstep with AI infrastructure deployments planned by DoD, the Intelligence Community, and research institutions.

By embedding the DPC at the heart of this cross-agency effort, the EOP can convene the full spectrum of federal, state, and local stakeholders. This convening power – coupled with clear incentives and streamlined processes – will transform permitting from a bottleneck into a strategic enabler, ensuring that Americas AI ambitions are matched by the resilient, high-capacity electric grid they require.

Below is a high-level, step-by-step roadmap to turn the national AI vision into reality, organized into four pillars: Governance, Infrastructure & R&D, Workforce & Ecosystem, Policy & Security.

7.1 Governance & Coordination

- **Establish a National AI Council**

- Charter a White House-level AI Council (or elevate NSCAI's successor) to set strategy, align agencies, and monitor progress.
- Mandate representation from OMB, OSTP, DoD, DHS, Commerce, DoC-NIST, and key private-sector/academic stakeholders [11].

- **Define Clear Goals and Metrics**
  - Set quantifiable targets (e.g., doubling federal AI R&D funding by 2027, provisioning 5 exaflops of public compute capacity, training 50,000 AI specialists).
  - Track both technical outcomes (model performance, open-source releases) and adoption metrics (SME AI usage rates).

7.2 Infrastructure & R&D

- **Launch a National AI Research Cloud**
  - Build on the "National Research Cloud" concept to provide affordable, secure access to HPC, GPUs/TPUs, and large-scale datasets for universities, startups, and agencies [4].
  - Co-invest with major cloud providers under clear terms for data privacy and open-access tiers.
- **Fund Foundational AI Research**
  - Increase NSF, DARPA, DOE, and NIH AI budgets; specifically target explainable AI, robustness, safe autonomy, and cybersecurity applications.
  - Create multi-institution "AI Grand Challenge" grants (*à la* the Human Genome Project) to tackle problems in event prediction, anomaly detection, and critical-infrastructure resilience.
- **Open Data & Benchmark Platforms**
  - Mandate that all federally funded AI projects publish data, code, and benchmarks on a centralized portal.
  - Sponsor annual "AI Open Data Challenge" prizes to stimulate novel applications in business analytics and security.

7.3 Workforce & Ecosystem

- **Scale AI Education and Training**
  - Expand federal scholarships and fellowships in AI, machine learning, and data science (including a "Digital Service Academy" for government AI talent).
  - Fund nationwide boot camps, community-college certificates, and online courses targeted at upskilling the current IT workforce.
- **SME Accelerator Programs**

  - Create regional AI “innovation hubs” that pair small and medium enterprises with AI experts, offering subsidized consulting, data-science residencies, and shared infrastructure.
  - Offer tax credits or matching grants for SMEs that adopt AI solutions in analytics, cybersecurity, or predictive maintenance.
- **Industry-Academia Consortia**
  - Seed joint labs (e.g., AI for Security, AI for Infrastructure) in leading research universities, with rotating industry-staff placements and funded PhD fellowships.

7.4 Policy, Ethics & National Security

- **Enact a Comprehensive AI Policy Framework**
  - Update the American AI Initiative into a binding National AI Strategy, codifying safeguards around privacy, bias, and algorithmic transparency (Executive Order 2019).
  - Direct NIST to accelerate development of AI Risk Management guidelines and sector-specific standards (e.g., for finance, healthcare, energy).
- **Integrate AI into National Security Doctrine**
  - Stand up an AI Integration Office within the DoD and DHS to deploy AI for intelligence analysis, autonomous systems, and cyber defense (NSCI emphasis).
  - Launch classified “AI for Defense” testbeds and wargames to stress-test algorithms under real-world scenarios.
  - Coordinate with FBI and CISA on deploying AI-driven insider-threat and anomaly-detection systems across federal and critical-infrastructure networks.
- **Foster International Partnerships**
  - Work with allies (e.g., Five Eyes, EU) to harmonize AI standards, share threat intelligence, and co-fund joint R&D projects.
  - Lead in setting global norms for responsible AI, leveraging U.S. strengths in democratic governance and rule of law.

By following these steps – anchored in strong governance, shared infrastructure, talent development, and robust policy – the United States can marshal a truly national AI effort that drives economic growth, secures critical systems, and sustains America’s leadership on the world stage.

8 AI Roadmap for the IC

Below is a set of concrete, Intelligence Community-focused recommendations, organized into five domains. Together, these steps will help agencies marshal the IC’s unique elements of power, deploy the necessary infrastructure, leverage frontier AI models and data-analytics partners, and architect secure multi-cloud environments with leading vendors.

8.1 Elements of Power: Mission, Authority, and Talent

- **Clarify Mission Priorities**
  - Establish a community-wide AI White Board under ODNI to codify high-priority use-cases (e.g., strategic warning, anomaly detection in signals intelligence, rapid geospatial analysis).
  - Assign "use-case owners" in each agency (CIA, NSA, NGA, DIA, etc.) to own requirements, performance metrics, and fielding timelines for their mission areas.
- **Governance & Authority**
  - Empower the IC Chief Data and AI Officer (CDAO) Council to set binding policies on model evaluation, security accreditation, and data-sharing standards.
  - Leverage existing authorities (e.g., 50 U.S.C. § 3036 for ODNI, CNCI directives for NSA) to mandate participation in shared AI initiatives.
- **Talent & Culture**
  - Expand rotational programs with industry and academia – e.g., assign intelligence officers to six-month "AI exchange" fellowships at labs like Google Research, OpenAI, or Meta's FAIR labs.
  - Stand up a permanent IC AI Academy for continuous upskilling in ML engineering, MLOps, and AI ethics, leveraging online curricula from entities like Scale AI, MIT, and Stanford's Center for AI Safety.

8.2 Infrastructure: Data Centers, Compute & Storage

- **Tiered AI Data Centers**
  - Tier 1: At Fort Meade, build a 200 MW HPC campus with exascale-class GPU/TPU clusters dedicated to foundational research and classified model training.
  - Tier 2: Regional "Edge AI Pods" co-located at mission hubs (e.g., Omaha for NGA, Colorado Springs for DIA) equipped with 10-20 petaflops of inference capacity and fast Non-Volatile Memory Express (NVMe) storage.
  - Tier 3: Field-deployable ruggedized AI appliances (e.g., NVIDIA Jetson-class modules) for deployed SIGINT/IMINT teams in austere environments.
- **Scalable Storage Fabric**
  - Implement a unified, high-throughput Object Storage layer (S3-compatible) with at least 100 PB of capacity and sub-millisecond metadata latency, protected by end-to-end encryption and zero-trust ingress controls.
  - Utilize Write Once Read Many (WORM)-capable tiers for long-term archival of vetted train-

ing datasets, and fast-cache tiers (all-flash) for active model development.

- **Networking & Interconnect**
  - Deploy 400 GbE spine-leaf fabrics inside data centers, with dedicated dark-fiber links to mission partners (e.g., DOE labs, academia) under the Trusted Internet Connection (TIC 3.0) framework.
  - Implement AI "data highways" over the Intelligence Community Information Technology Enterprise (IC ITE) backbone for rapid dataset distribution and federated learning.

8.3 Frontier Models & Big Tech Collaboration

- **Model Licensing & Customization**
  - Negotiate enterprise licenses or strategic partnerships with companies like Google (Vertex AI), Microsoft (Azure OpenAI Service), and Meta (Llama-based models) to access their latest foundation models under strict security enclaves.
  - Co-develop IC-tuned variants: e.g., fine-tuned GPT-4-class models for targeting analysis or maritime traffic forecasting, trained on declassified datasets watermark-tagged for provenance.
- **Joint Research Labs**
  - Establish in-agency "AI Research Hubs" in Silicon Valley and the DC area, embedded alongside teams like Google DeepMind, OpenAI, and Meta FAIR teams. These hubs would host joint scientists working on explainability, robustness, and adversarial defense methodologies.
- **Federated & Private Model Sharing**
  - Build a closed federated learning framework allowing secure model updates across agencies without raw data exchange. Leverage Intel SGX or AMD SEV for confidential multiparty model aggregation.

8.4 Data Analytics Partners & Ecosystem

- **Bespoke Data Integration**
  - Deploy tools like Palantir Gotham or Foundry as the IC's "data lakehouse" front-end: automate data ingestion, transformation, and low-latency search across classified and unclassified repositories.
  - Contract companies like Scale AI for bespoke labeling pipelines – rapidly annotate satellite imagery, SOC logs, or social-media streams at scale – then feed high-quality training sets into IC-owned model lifecycles.
- **Specialized Analytics Toolchains**
  - Integrate both open-source frameworks (e.g., Apache Airflow, Kubeflow, JupyterLab) and

  commercial CI/CD pipelines to move models from prototype to production under full audit.

  - Leverage commercial analytics startups (e.g., Databricks, DataRobot) via GSA schedules to accelerate use-case development while maintaining FedRAMP Moderate/High compliance.

8.5 Cloud Vendors & Secure Multi-Cloud Strategy

- **FedRAMP High Enclaves**
  - Ingest unclassified and secret-collaboration workloads into FedRAMP High environments like AWS GovCloud, Azure Government, and Google Cloud Platform's US Government regions.
  - Use vendor-provided confidential VMs (e.g., Azure Confidential Computing, GCP Confidential VMs) to protect workloads against insider and hypervisor threats.
- **Multi-Cloud Orchestration**
  - Adopt a service-mesh approach (e.g., Istio on Anthos, Azure Arc) for workload portability, encryption-in-transit, and consistent policy enforcement across clouds.
  - Leverage tools like Terraform or Crossplane to define Infrastructure as Code (IaC) modules that ensure repeatable, compliant deployments of AI clusters and data pipelines.
- **Vendor-Neutral Data Fabrics**
  - Implement a unified Data Fabric layer (e.g., NetApp Cloud Volumes) that spans on-premise and multiple cloud providers – ensuring data sovereignty, global namespace, and automated policy-based tiering.
  - Partner with vendors to embed Key Management Service (KMS) integration (e.g., AWS KMS, Azure Key Vault, Cloud KMS) for centralized key management under HSM protections, with auditable logs in SIEM tools (e.g., Splunk, IBM QRadar).

8.6 Pillar Ownership & Accountability

Model Development & Oversight

- *Ownership*: IC Chief AI Officer (IC CAIO) in conjunction with the CAIO Council, supported by interagency AI Working Groups.
- *Responsibilities*:
  - Approve model architectures, training pipelines, and performance metrics.
  - Convene Model Review Boards (security, ethics, mission SMEs) to certify each release.
  - Maintain a centralized registry of all approved AI models, versions, and associated risk assessments.

Data Governance & Stewardship

- *Ownership*: IC Chief Data Officer (IC CDO) in conjunction with the IC CDO Council.
- *Responsibilities*:
  - Define data classification schemes, access controls, and retention policies for AI datasets.
  - Standardize Data Use Agreements, provenance tagging, and audit protocols to ensure integrity and compliance.
  - Operate a federated metadata catalog to enable discovery, sharing, and reuse of mission-critical data assets under a unified trust framework.

Networks & Infrastructure

- *Ownership*: IC Chief Information Officer (IC CIO).
- *Responsibilities*:
  - Architect and oversee tiered AI data centers (HPC campuses, edge pods, field appliances) and high-throughput storage fabrics.
  - Implement zero-trust networking, multi-cloud orchestration, and secure interconnects across all data center tiers.
  - Manage vendor-neutral data fabrics, key-management integrations, and continuous monitoring to ensure performance, resilience, and compliance.

By delineating these three pillarsmodels under the CAIO Council, data under the IC CDO/Data Council, and networks under the IC CIOthe Intelligence Community gains a clear governance structure, streamlined policy levers, and precise accountability for each foundational element of its AI enterprise.

8.7 Summary

By executing these tailored steps – grounded in the IC's authorities and missions – agencies will gain:

- **Strategic Advantage**: Faster, more accurate intelligence through frontier AI
- **Resilience**: Hardened infrastructure and multi-cloud redundancy
- **Collaboration**: Deep partnerships with big tech and analytics firms
- **Security**: Zero-trust controls, confidential computing, and auditability

This blueprint positions the Intelligence Community to lead in applying AI for national security, safeguarding American interests in an era defined by data and algorithms.

9 Streamlining IC Acquisitions & Partnerships

Below are targeted strategies to streamline and accelerate the U.S. government's acquisition of AI technologies by cutting through statutory, regulatory, and policy "red tape" while still preserving accountability and security:

9.1 Establish an AI-Specific Rapid-Acquisition Pathway

- **Create a Dedicated AI Authority**. Amend the Federal Acquisition Regulation (FAR) to include an “AI Rapid-Fielding” subpart that mirrors Other Transaction Authority (OTA) flexibility but is tailored to AI’s iterative development cycles.
- **Sunset Reviews**. Build in automatic “sunset” clauses so pilot AI contracts expire or require renewal after 18-24 months, ensuring continual reassessment rather than open-ended commitments.

9.2 Broaden Use of Other Transaction Authorities (OTAs)

- **Lower Delegation Thresholds**. Increase the dollar thresholds delegated to program-office directors to award OTAs for AI prototypes (e.g., raise from $100 million to $250 million), reducing the need for lengthy senior-level approvals.
- **Pre-Approved Consortium Agreements**. Stand up pre-negotiated “AI Consortium OTAs” with vetted industry and academic partners (e.g., Google, Palantir, Scale AI) so that agencies can spin up new S&T efforts in days rather than months.

9.3 Streamline Data-Access and Classification Rules

- **Sensitive But Unclassified (SBU) Information Sandbox**. Carve out a “SBU-AI Sandbox” designation that allows vetted teams to work on sensitive datasets in a secured enclave without full Special Access Program or Controlled Access Program procedures.
- **Fast-Track Data Use Agreements**. Standardize and accelerate inter-agency and agency-to-industry data-sharing templates (e.g., MDTAs) with pre-approved cybersecurity and privacy clauses.

9.4 Adopt Agile-Friendly Contracting Structures

- **Modular “Plug-and-Play” Contracts**. Break large AI programs into small, self-contained “modules” (data ingestion, model training, deployment) with separate performance milestones, so each can be competed or updated independently.
- **Performance-Based Payments**. Shift from “cost plus” to outcome-driven payment lines (“pay for accuracy,” “pay for latency”) to incentivize rapid iteration and real-world performance.

9.5 Empower an AI Acquisition “Tiger Team”

- **Cross-Agency SWAT Team**. Assemble a standing rapid-acquisition task force drawn from GSAs 18F, DoDs DIU, DHSs Silicon Valley Innovation Program, and OMBs OFPP to shepherd AI proposals through legal, budgetary, and security reviews in a consolidated 30-day sprint.

- **One-Stop "Acquisition Passport."** Issue an "AI Acquisition Passport" that pre-clears technologies, security controls, and legal waivers so cleared vendors can deploy updates without repeating background checks and compliance audits project-by-project.

9.6 Modernize Security & Privacy Assessments

- **Adaptive Risk Framework**. Replace static Authority-to-Operate (ATO) processes with a "continuous ATO" model: security and privacy controls are assessed automatically via DevSecOps pipelines, with real-time dashboards to the Authorizing Official.
- **Tiered Assurance Levels**. Define Assurance Levels (ALs) for AI systems – AL1 (low-risk R&D), AL2 (pilot deployment), AL3 (mission-critical)each with a tailored, much lighter compliance checklist for AL1 and AL2.

9.7 Reform Budget & Appropriation Timing

- **Multi-Year Rapid Funds**. Combine R&D and procurement lines into a single "AI Innovation Fund" with multi-year appropriations, allowing agencies to hopscotch fiscal-year constraints for proof-of-concepts.
- **Reprogramming Flexibility**. Increase "reprogramming" thresholds specifically for AI within defense and homeland-security budgets, so money can shift from legacy programs into new AI pilots without waiting for annual appropriations.

9.8 Leverage Pre-Certified Technology Catalogs

- **GSA AI "QuickShip" Schedule**. Expand GSAs IT Schedule 70 with an AI "QuickShip" track: pre-certified AI tools and vendors that meet baseline security, performance, and ethical-AI criteria, available for immediate "off-the-shelf" purchase.
- **Continuous Vendor Vetting**. Use automated scorecards (via FedRAMP Connect or CDM dashboards) to keep the catalog up to date – adding innovations from Amazon AWS, Microsoft Azure, Oracle Cloud, and Google Cloud as soon as they pass minimal risk checks.

By embedding these reforms into law and policy – updating the FAR, harnessing OTAs, standing up cross-agency rapid teams, and adopting continuous security models – the **federal government can cut months (or even years) off its AI acquisition cycle**. The result: faster deployment of cutting-edge AI for mission-critical use cases, from predictive analytics and cybersecurity to insider-threat detection and critical-infrastructure protection.

10 Conclusion

In conclusion, the United States must undertake a comprehensive national-scale initiative on AI – one that builds the **technical infrastructure** for innovation, drives **economic adoption** across all sectors, establishes enlightened **policies**, and **advances strategic applications for security**. This effort cannot be government alone, nor market alone: it requires a true collaboration of public and private sectors, leveraging the strengths of each. The Trump Administration's steps – from launching a federal AI strategy to affirming that industry, academia, and government must work in concert – set the stage for this collaboration [1, 3]. Going forward, U.S. leaders should treat AI with the urgency and ambition of a national mission. The stakes are enormous: economically, AI promises new prosperity if we guide it wisely, and "**falling behind will have disastrous effects**" [4]; strategically, AI will help decide the winners of the 21st century in both commerce and conflict. As a nation, investing in AI is investing in our future security and prosperity. By building robust AI infrastructure, fostering innovation with American values, and uniting public and private efforts, the U.S. can continue to lead the world in AI – **to the benefit of our economy, our society, and our national security** [1, 3].

11 Acknowledgments

Special thanks to Dr. Alli Curran and Dr. Tom Pike for their valuable comments and additions.

12 Note on References

While there are many research papers that span these topics, this article emphasized papers with the following metrics:

- ✓ High Citation Counts - Many references have 1,000+ citations, ensuring they are widely accepted and influential in the AI, Cyber, Policy, Economics, and National Security research community.
- ✓ Top AI, Cyber, Policy, Economics, and National Security Institutions - Includes research from Stanford, CSET, GWU, and Harvard.
- ✓ Authors with High h-Index - leading AI researchers such as Fei-Fei Li (h-index: 150+).

References

[1] Trump, Donald J. "Artificial Intelligence for the American People." Trump White House Archives, 2018

[2] Executive Office of the President. Executive Order on Maintaining American Leadership in Artificial Intelligence. White House, 11 Feb. 2019

[3] White House Office of Science and Technology Policy. Summary of the 2018 White House Summit on Artificial Intelligence for American Industry, 10 May 2018

[4] Li, Fei-Fei, and John Etchemendy. "We Need a National Vision for AI." Stanford HAI News, 2020

[5] Murray, Seb. “Can AI Predict the Future?” Knowledge@Wharton, 14 Jan. 2025

[6] Bin Sarhan, Bushra, and Najwa Altwaijry. “Insider Threat Detection Using Machine Learning Approach.” Applied Sciences, vol. 13, no. 1, 2023

[7] Allen, Greg, and Taniel Chan. Artificial Intelligence and National Security. Belfer Center, Harvard Kennedy School, July 2017

[8] Rattray, Greg, et al. Securing Critical Infrastructure in the Age of AI. Center for Security and Emerging Technology, Oct. 2024

[9] Winegar, Lt. Col. Michael, et al. “Artificial Intelligence, International Competition, and the Balance of Power.” Texas National Security Review, vol. 1, no. 3, May 2018

[10] PricewaterhouseCoopers. Global Artificial Intelligence Study: Exploiting the AI Revolution. PwC, 2017

[11] National Security Commission on Artificial Intelligence. Final Report, 1 Mar. 2021.