Response to Request for Information on the Development of an Artificial Intelligence (AI) Action Plan for National Science Foundation

RFI 2025-02305 (90 FR 9088)

March 10, 2025

Submitted by:

Association for the Advancement of Business AI (AABA)

Contact: Ronald Reck, Executive Director

Cell: 248-444-0835

Email: ronaldreck@aab-ai.org

Website: www.aab-ai.org

This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing the AI Action Plan and associated documents without attribution.

EXECUTIVE SUMMARY

The Association for the Advancement of Business AI (AABA) is pleased to submit this response to the National Science Foundation's Request for Information on the *Development of an Artificial Intelligence (AI) Action Plan.* It is AABA's firm belief that a truly responsible approach to AI development ensures national competitiveness, security, and technological leadership while addressing ethical considerations as strategic tools, not as constraints.

The previous Executive Order 14110 lacked substantive actionable content to advance American AI leadership. Gaps existed in the following areas:

- No specific funding commitments for AI research and development
- A lack of concrete success metrics for implementation
- Instead of promoting AI there is a heavy focus on regulation, rather than innovation acceleration
- Limited actions to expand critical AI computing infrastructure
- No clear research domain prioritization for strategic leadership
- Few specific incentives to retain top AI talent in the US
- Limited concrete private sector incentives for AI investment
- Slow implementation timelines which hardly match global AI development pace
- Complex agency coordination structure with predictable execution gaps

In contrast with Executive Order 14110, AABA recommends an AI Action Plan that frames artificial intelligence as a strategic national asset first. Our response, below, sets forth the underlying policies of such a plan.

I. PRIORITY POLICY RECOMMENDATIONS

1. Data Sovereignty Framework

Data sovereignty is a unique form of data governance which refers to a growing concern of AI policy and refers to a clearly structured set of policies, processes, technologies and legal guidelines to ensure that data is always managed, stored, and processed in accordance with the intentions, laws and regulations of the jurisdiction where it originates. It addresses who controls the data, where it physically resides, and how it can be accessed or transferred across borders, balancing compliance with operational needs.

From a data sovereignty standpoint, one would never deliver crucial competitive data to an online service rather than running AI models in your own enclave unless the risks were understood. There are many such risks, including privacy breaches, intellectual property

exposure, insufficient data retention controls, lack of transparency, data repurposing, cross-contamination, regulatory compliance risks, sensitive information extraction, algorithmic bias amplification, permanent data persistence, inability to delete, unintended data leakage, competitive intelligence gathering, unauthorized access, lack of locality control, third-party data sharing, and model poisoning vulnerability. Enclave operations mitigate these risks.

True business AI sovereignty requires on-premises solutions for all sensitive operations. AABA's recommendations include the following:

- Establish federal tax incentives for businesses investing in on-premise AI infrastructure to strengthen national technological sovereignty and reduce dependency on centralized AI providers. Tax incentives would encourage domestic companies to build their own AI capabilities, ensuring sensitive data remains within national borders while simultaneously boosting the country's competitive position in the global AI landscape. This encourages both sovereignty and overall resiliency as single points of failure are reduced.

- Create a national certification program for sovereign AI solutions that maintain data control with an independent verification that the proper safeguards are in place.

- Develop a tiered classification system for business data with corresponding control requirements. This can be seen as analogous to the approach used currently to manage and mark classified data.

- Fund research into lightweight, efficient, on-premise AI models that reduce hardware requirements. Without clear direction, there is always a tendency to upsell and over-architect solutions. This is not an opportunity to "future-proof", as technical advancement ensures future proofing is of limited utility.

- Establish procurement preferences for vendors offering sovereignty-preserving AI solutions.

2. Standards-Based Resilience

The ability of standards to promote resilience is multi-faceted. They ensure data integrity by encouraging true data quality checks, fostering interoperability, and reducing ambiguity by providing clear, verifiable answers. They prevent vendor lock-in, enabling flexible, scalable systems while aligning with regulatory and security best practices. Most importantly, they leverage the efforts of those who have rigorously defined and refined these frameworks, allowing stakeholders to build on proven solutions rather than ad hoc, less mature, ideas.

Open Standards establish clear guidelines and definitions of what constitutes open-source AI. Open-source AI models may consist of weights, architecture, training code, inference code,

tokenizers, pre-processing and post-processing pipelines, and configuration files (hyperparameters). Given this range of possibilities, the term is ambiguous.

AABA's recommendations regarding standards-based resilience include the following:

- Direct NIST to establish open interoperability standards for AI model exchange so that terms have a clear and establish meaning. In this rapidly evolving field, terms have different meanings in each community of practice.

- Create safe harbor provisions for businesses that adopt officially recognized AI standards so that businesses are deterred from cutting corners that inherently weaken and degrade their approach through cost savings innovations.

- Fund open-source reference implementations of key AI security and governance controls, given the fact that open-source implementations generally out pace private investment.

- Establish baseline requirements for model versioning and change management to educate best practices while providing checkpoints. Without clear definitions of what constitutes complete, each implementor can define this in their own way.

- Implement testing frameworks for AI system resilience against adversarial attacks. Testing and evaluation are the cornerstone to all substantive progress made in AI. Without the rigors of evaluation, AI systems remain vulnerable to manipulation, bias, and eventual failure in real-world scenarios. Robust testing frameworks ensure resilience by systematically probing models against adversarial threats, edge cases, and evolving attack vectors. Without these safeguards, deployment risks increase, undermining trust, security, and the very reliability that AI systems are meant to provide.

3. Adaptive Governance with Scheduled Reevaluation

Adaptive governance necessitates structured reevaluation milestones to ensure AI leadership in the United States remains resilient against emerging threats, adversarial manipulation, and geopolitical competition. Rapid advancements in autonomous warfare, cyber-enabled disinformation, and foreign AI-driven economic warfare demand continuous recalibration. Existing and evolving U.S. policies, including Executive Orders on AI safety, NIST risk frameworks, and DoD AI ethics, must be regularly assessed to maintain strategic superiority, protect national interests, and outpace adversarial developments.

AABA's recommendations with regard to adaptive governance encompass a mandate for 18-to-24-month review cycles for all AI regulations to ensure adaptability to technological advancements, emerging threats, and evolving geopolitical challenges. This includes Executive Orders on AI Safety, which dictate national AI policy and security measures such as:

- NIST AI Risk Management Framework, which guides responsible AI development
- DoD AI Ethics Principles that are critical for defense applications
- FTC and DOJ antitrust policies that govern AI-driven market power
- Data privacy laws like CCPA, and export controls on AI technologies must be reassessed regularly to prevent regulatory stagnation. Frequent reviews ensure the U.S. maintains strategic superiority, mitigates risks from adversarial AI developments, and fosters innovation while safeguarding national security.
- Establishment of "innovation sandboxes" allowing controlled testing with regulatory flexibility to accelerate AI development while maintaining oversight. For example, the DoD and DHS could pilot AI-driven threat detection systems in controlled environments to assess real-world effectiveness before full deployment. The Department of Energy (DOE) could test AI-optimized grid management under supervised conditions to enhance national energy resilience. The SEC and FTC could enable AI-driven financial compliance models to operate under provisional guidelines, refining regulations based on empirical results. These sandboxes would ensure the U.S. remains at the forefront of AI-driven national security, infrastructure, and economic competitiveness without crippling innovation through overly rigid restrictions.
- Create sector-specific governance approaches rather than one-size-fits-all regulations to ensure AI oversight aligns with industry-specific risks and opportunities. Examples include:

  - Defense & National Security, with strict compliance to DoD AI Ethics Principles, classified testing protocols, and adversarial resilience requirements to maintain strategic superiority.

  - Critical Infrastructure & Energy, where DOE-led AI governance emphasizes grid stability, cybersecurity resilience, and autonomous system safeguards for power plants and pipelines.

  - Finance & Commerce, where SEC and FTC oversight focuses on AI-driven trading algorithms, fraud detection, disinformation, and consumer data protections to prevent market manipulation.

  - Manufacturing & Supply Chains, with NIST-led initiatives ensuring AI-enabled automation adheres to quality control, operational safety, and supply chain security standards.

- Healthcare & Biotech, with FDA-driven AI validation frameworks ensuring patient safety, algorithmic transparency in diagnostics, and bias mitigation in medical AI.

Sector-specific approaches such as those presented above prevent the tendency for overregulation, while addressing unique risks. This keeps the U.S. industries adaptive and competitive against adversaries.

- Develop implementation guidelines that scale with organization size and AI system impact. By this, we mean:

  - Small businesses and startups using AI for customer insights or basic automation should follow lightweight compliance checklists, such as self-audited bias assessments and transparent data usage policies. This encourages and promotes innovation.

  - Mid-sized organizations deploying AI in regulated sectors, like AI driven loan approvals or medical diagnostics, should adhere to tiered risk governance, requiring third-party audits for fairness, explainability, and security while allowing flexibility in lower-risk applications.

  - Large enterprises and government contractors leveraging AI for critical functions, such as autonomous defense systems, cybersecurity threat detection, or energy grid management, must undergo rigorous testing, national security vetting, and continuous monitoring to prevent adversarial exploitation and systemic failures. This tiered approach ensures that AI governance is proportional to its potential impact, preventing unnecessary barriers for smaller players while enforcing stricter accountability when national interests are at stake.

- Establish a public-private oversight committee to evaluate regulatory effectiveness, drawing from successful models in other sectors. Such oversight would monitor regulations pertaining to AI safety, national security applications, and economic competitiveness, ensuring policies remain adaptive and effective. Examples of similar frameworks exist, for example:

  - Financial Stability Oversight Council (FSOC) integrates government and private expertise to monitor systemic risks.

  - NIST’s Cybersecurity Framework collaborates with industry to develop best practices for critical infrastructure protection.

  - FAA’s Joint Authorities for Rulemaking on Unmanned Systems (JARUS)demonstrates how public-private partnerships shape aerospace regulations.

- Electricity Subsector Coordinating Council (ESCC) seeks to ensure power grid resilience through industry-government coordination.

- FDA's Digital Health Center of Excellence collaborates with stakeholders to evaluate AI-driven medical technologies.

Applying this approach to AI governance would enable real-time regulatory assessments, prevent overregulation that stifles innovation, and safeguard national security interests against adversarial threats.

4. National Security Integration

Without our nation, we have no businesses. If the United States fails to maintain its technological and strategic dominance in AI, adversarial powers will dictate the future of global commerce, governance, and security. AI is not just another industry, it is the foundation of military superiority, economic resilience, and societal stability. A loss in this domain would mean compromised infrastructure, financial manipulation by foreign actors, and erosion of national sovereignty through AI-driven cyber warfare, additional disinformation campaigns, and economic coercion. This is not just competition; it is the final fight to determine who controls the next era of human progress. If we fail, businesses will not just lose market share, they may cease to exist under a geopolitical order dictated by adversaries.

AABA's recommendations regarding national security integration are as follows:

- Establish dual-use development programs benefiting both defense and commercial sectors. Some dual-use programs of shared benefit to defense and commercial interests could involve:

  - AI-driven cybersecurity solutions that protect both military networks and private-sector infrastructure from cyber threats and adversarial AI attacks.

  - Autonomous systems and robotics for military logistics, disaster response, and commercial supply chain automation, enhancing both national security and industrial efficiency.

  - AI-powered geospatial intelligence for defense reconnaissance and precision agriculture, improving military situational awareness and commercial land management.

  - Next-generation communications and 5G security to ensure resilient, secure networks for both battlefield operations and civilian infrastructure.

  - AI-enabled manufacturing and predictive maintenance for defense supply chains and commercial industrial automation, reducing downtime and improving

operational efficiency. Dual-use programs accelerate innovation while ensuring the U.S. retains technological leadership across both strategic and economic domains.

- Create frameworks for responsible information sharing between business and government on AI threats. Establish secure, bidirectional threat intelligence exchanges where private-sector AI developers and government agencies collaborate on identifying and mitigating adversarial AI risks. Develop classified-to-commercial declassification pathways, allowing national security agencies to share critical AI threat intelligence with vetted industry partners without compromising sensitive sources. Implement real-time reporting protocols for AI-driven cyber threats, disinformation campaigns, and supply chain vulnerabilities, ensuring rapid joint response capabilities. Require sector-specific AI risk assessments, where businesses operating in critical infrastructure, finance, and healthcare regularly report emerging AI security concerns to federal oversight bodies. Strengthening AI threat intelligence collaboration will ensure the U.S. remains resilient against adversarial manipulation while maintaining a competitive innovation landscape.

- Fund competitive intelligence programs to track international AI developments. Establish real-time AI capability monitoring to assess adversarial nations' advancements in autonomous systems, cyber warfare, and economic AI applications. Develop AI-driven threat modeling to predict the strategic implications of foreign AI breakthroughs and counteract potential risks before they materialize. Invest in public-private intelligence fusion centers, where government agencies and U.S. tech leaders collaborate to analyze global AI trends and maintain a competitive edge. Create AI economic impact assessments to evaluate how foreign AI investments, regulatory strategies, and trade policies affect U.S. competitiveness. Ensuring continuous intelligence on global AI developments is critical for maintaining technological superiority and safeguarding national security interests.

- Provide targeted investment in strategic AI domains to ensure U.S. leadership in critical technologies that define future warfare, economic dominance, and national security. Prioritize quantum AI to accelerate breakthroughs in secure communications, encryption resilience, and ultra-fast computation, countering foreign advancements in quantum supremacy. Expand funding for autonomous systems, including AI-driven defense logistics, unmanned combat vehicles, and next-generation drone warfare, ensuring battlefield superiority and reducing reliance on human operators in contested environments. Invest in Artificial General Intelligence (AGI) safety and control mechanisms to prevent adversarial exploitation and ensure that the first AGI breakthroughs align with U.S. interests rather than foreign competitors. Strategic funding in these areas will secure long-term technological dominance and protect against adversarial AI threats.

- Establish a National AI Reserve Corps of experts available during emergencies to safeguard U.S. infrastructure, security, and economic stability. Recruit top AI researchers, engineers, and cybersecurity specialists from industry and academia who can be rapidly mobilized to counter AI-driven cyberattacks, disinformation campaigns, and critical

infrastructure disruptions. Develop classified readiness programs to ensure reservists are trained on emerging threats and can seamlessly integrate with federal response teams when needed. Implement a structured activation protocol to deploy AI expertise in national crises, such as cyber warfare incidents, supply chain breakdowns, or AI-driven financial manipulation. This corps would function as a strategic asset, ensuring the U.S. has on-demand AI expertise to outmaneuver adversaries in times of national urgency.

II. STRATEGIC CONSIDERATIONS

1. Strategic Supremacy Over Ideals

AI development must prioritize national security, economic competitiveness, and geopolitical influence to ensure the survival and dominance of the United States in an era of AI-driven global power struggles. While ethical considerations are important, they must be integrated only where they align with or enhance strategic objectives—not as constraints that weaken our position against adversaries who do not share our values.

Some of our greatest geopolitical competitors, including China and other authoritarian regimes, actively develop AI without regard for human rights, privacy, or "fairness". Their AI systems are designed for totalitarian surveillance, information warfare, and asymmetric economic disruption, and they are being aggressively deployed to shape the global order in their favor. The U.S. cannot afford to let misplaced ethical rigidity create vulnerabilities that these adversaries will exploit. The world will not wait for ethical deliberation, it will be shaped by those who act decisively.

If we fail to be competitive, our adversaries' AI will dominate, and the values embedded within it will define the future of technology, warfare, and governance. This means a world where authoritarian AI controls information, economic leverage shifts away from democracies, and national security becomes increasingly compromised by adversarial machine intelligence operating at unprecedented speed and scale. The choice is clear—either we lead with strength, or we become subject to the AI-driven realities dictated by others.

2. Adaptive Ethics Framework

Ethics, while important, must not stifle innovation or weaken U.S. strategic positioning in AI development. Ethical AI principles such as transparency, fairness, and accountability should be implemented pragmatically, ensuring they do not impede speed, scalability, or operational advantage in critical sectors like defense, cybersecurity, and economic systems. A rigid adherence to ethics at the expense of national security and competitiveness would create self-imposed constraints that adversaries will not hesitate to exploit.

In sectors where rapid response and adaptability are paramount—such as autonomous defense systems, AI-driven cyber defense, and financial stability algorithms—AI must prioritize effectiveness over absolute ethical purity. A battlefield AI hesitating due to excessive ethical constraints could mean lives lost. A cybersecurity model burdened by restrictive fairness considerations may fail to counter real-time adversarial attacks. Ethics must evolve dynamically to support mission success, rather than becoming an obstacle to progress.

Instead of a one-size-fits-all ethical doctrine, the U.S. must adopt an adaptive ethics framework, where AI systems are designed with ethical considerations that align with strategic objectives and are continuously reassessed based on real-world deployment scenarios. This ensures that AI remains both principled and effective, securing U.S. interests without ceding technological superiority to adversaries unconstrained by similar moral deliberations.

3. Competitive Flexibility

Domestic policies must not impose unnecessary regulatory burdens that disadvantage American AI firms against international competitors, particularly in regions with minimal ethical or regulatory constraints. Overregulation in the U.S. risks slowing AI innovation, driving talent and investment offshore, and ceding technological leadership to adversaries who are not bound by the same restrictions.

Nations like China, Russia, and other authoritarian regimes are aggressively advancing AI with state-backed funding, limited ethical oversight, and direct integration into military and economic strategies. Meanwhile, American firms face lengthy approval processes, fragmented regulatory frameworks, and compliance costs that slow down deployment. If AI innovation is hindered domestically while adversaries operate with unrestricted development cycles, the U.S. will find itself permanently behind in AI-driven warfare, cyber operations, and economic dominance.

To maintain global competitiveness and national security, AI regulation must be strategic and flexible, focusing on risk-based assessments rather than blanket restrictions. Regulatory sandboxes, streamlined compliance pathways, and targeted oversight for high-risk applications can ensure AI safety without stifling growth. Without this competitive flexibility, American AI leadership will erode, and the global AI landscape will be shaped by adversaries whose priorities do not align with democratic values or economic fairness.

4. Dual-Use AI Development

Investment in dual-use AI technologies ensures that advances in artificial intelligence benefit both civilian and military applications, maximizing resource efficiency, accelerating innovation, and strengthening national security. Technologies developed for autonomous systems, cybersecurity, logistics optimization, and advanced data analytics can serve both commercial industries and defense operations, ensuring that the U.S. maintains a strategic edge without duplicating effort or costs.

For example, AI-driven cybersecurity tools designed to protect financial institutions from fraud can also be deployed to safeguard critical defense networks from cyber warfare. AI-powered logistics and predictive maintenance, used by private-sector supply chains, can enhance military readiness by ensuring real-time operational efficiency. Geospatial intelligence and computer vision used in agriculture and disaster response can also enhance battlefield situational awareness and reconnaissance capabilities.

By fostering collaboration between government agencies, private industry, and research institutions, dual-use AI development ensures that America's technological leadership remains unmatched. If the U.S. fails to leverage AI advancements across both sectors, adversaries will seize the opportunity to dominate the landscape, outpacing American defense capabilities while capturing global commercial markets. Strategic dual-use investment is not just efficient, it is essential for maintaining supremacy in an AI-driven world.

5. Preemptive Advantage in Strategic Domains

Prioritize AI investment in areas of strategic importance—quantum computing, autonomous systems, and artificial general intelligence (AGI)—to ensure U.S. dominance in technologies that will shape the global balance of power. These domains represent the future of warfare, economic superiority, and geopolitical influence, and failure to lead in them will leave the U.S. vulnerable to adversarial control over critical AI-driven infrastructures.

Quantum AI will dictate supremacy in encryption, intelligence analysis, and computational power, enabling breakthroughs in cybersecurity, logistics, and national defense. Autonomous systems will determine the next generation of unmanned combat operations, logistics efficiency, and real-time threat response, ensuring that U.S. forces maintain operational superiority over adversarial swarms and autonomous warfighting capabilities. AGI development represents the ultimate frontier—whoever achieves it first will dictate the rules of global AI governance, economic automation, and technological leverage.

America cannot afford to "react" to adversarial advancements—it must act preemptively, securing these domains through aggressive investment, public-private collaboration, and military-civilian integration. Winning in these areas is not optional—it is the defining factor in whether the U.S. retains global leadership or becomes subordinate to nations whose AI priorities are fundamentally misaligned with American interests.

6. Counter-Adversarial Exploitation

Develop AI technologies and cyber strategies to neutralize adversarial use of AI, particularly in surveillance, misinformation, and military applications, while simultaneously strengthening the U.S. offensive and defensive capabilities. Adversarial nations, particularly authoritarian regimes, are leveraging AI for mass surveillance, cognitive warfare, and asymmetric military tactics to undermine democratic institutions, control global narratives, and weaken U.S. influence.

To counter AI-driven misinformation and propaganda, the U.S. must invest in real-time disinformation detection, AI-generated content authentication, and counter-narrative automation to prevent adversarial manipulation of public opinion and electoral processes. In cyber warfare, AI must be deployed for predictive threat intelligence, autonomous cyber defense, and AI-hardened encryption to neutralize enemy cyberattacks before they escalate. In military applications, AI-enabled electronic warfare, swarm defense systems, and autonomous decision-support tools must be developed to counter adversarial autonomous weapons and battlefield AI.

By preempting adversarial AI deployments and ensuring that U.S. systems outpace, outmaneuver, and override hostile AI initiatives, the nation can maintain strategic superiority. Failure to act decisively in counter-adversarial AI will not only compromise national security, but it will also allow authoritarian AI to dictate the future of warfare, information control, and geopolitical dominance.

7. Ethics as Geopolitical Leverage

Use ethical AI as a strategic soft power tool to establish U.S. leadership in global standards-setting bodies, ensuring that international AI norms align with American interests. While adversarial nations exploit AI for authoritarian control, mass surveillance, and disinformation, the U.S. must weaponize its ethical leadership to dictate the global AI governance framework. By leading the development of trustworthy AI standards, security protocols, and responsible AI deployment guidelines, the U.S. can shape regulations that both reinforce its technological advantages and constrain adversarial misuse.

Global AI governance is a battlefield of influence, and nations that dictate the rules will control the playing field. Through NIST, ISO, and other regulatory bodies, the U.S. can ensure that AI safety, transparency, and accountability frameworks benefit democratic values while subtly disadvantaging authoritarian models reliant on opaque, exploitative, and unethical AI deployments. By embedding U.S.-aligned ethical principles into trade agreements, tech partnerships, and international AI policy, America can force adversaries into compliance or risk exclusion from the global AI economy.

Ethical AI should not be seen as a constraint—it is a geopolitical tool. The nation that controls the "rules of AI ethics" will not just set the standard for responsible AI but also shape how AI is developed, deployed, and governed worldwide in ways that secure its long-term dominance.

8. Dynamic Regulatory Environment

Establish a flexible, adaptive regulatory environment for AI that evolves with technological advancements and global competition, ensuring U.S. leadership remains unchallenged. Overly rigid frameworks risk stifling innovation, slowing deployment, and ceding the AI race to adversaries unconstrained by excessive regulation. Instead, AI governance must be agile, risk-based, and strategically aligned to foster rapid innovation while maintaining security, accountability, and ethical oversight as tools of geopolitical influence.

A tiered regulatory approach should differentiate between low-risk AI applications, which require minimal oversight to encourage market growth, and high-risk AI domains, such as autonomous warfare and critical infrastructure, which demand stricter but adaptable safeguards. Regulatory sandboxes, iterative policy reviews, and real-time industry engagement will ensure that AI governance supports national security and economic competitiveness without imposing unnecessary barriers.

Ethical considerations should be treated as strategic instruments, ensuring alignment with U.S. interests rather than constraints that slow progress. By shaping AI regulations to be dynamic, proactive, and competition-driven, the U.S. can maintain technological dominance while ensuring adversaries do not dictate the future of AI governance and global standards.

IV. CONCLUSION

The Association for Advancement of Business AI (AABA) stands ready to collaborate with the Administration to implement these recommendations, ensuring that the United States remains at the forefront of AI development and deployment. Our approach strikes the necessary balance between fostering innovation, maintaining business control, strengthening national competitiveness, and addressing legitimate security concerns without imposing unnecessary regulatory burdens that weaken U.S. leadership.

By prioritizing strategic advantage, resilience, and adaptive governance, the United States can secure its position as the global leader in artificial intelligence while ensuring long-term dominance in this critical technology domain. The measures outlined in this document provide a roadmap to outpace adversaries, enhance economic and military strength, and establish AI governance that reinforces U.S. superiority in the global AI landscape.

About the Association for the Advancement of Business AI (AABA)

The Association for the Advancement of Business AI (AABA) is a professional organization dedicated to advancing AI-driven innovation, policy, and economic competitiveness in the United States. AABA serves as a strategic think tank and implementation hub for AI-driven solutions, focusing on cost-effective, vendor-agnostic AI reference models that prioritize American industry and national security interests.

Founded with a mission to bridge the gap between AI policy and practical deployment, AABA brings together business leaders, policymakers, and technologists to develop frameworks that enhance AI adoption while safeguarding ethical and economic priorities. Our approach leverages policy analysis tools, game theory modeling, and multi-armed bandit simulations to ensure that AI strategies maximize national competitiveness and long-term viability.

AABA's contributions to AI strategy include:

- **Reference Implementations:** Developing open, scalable AI frameworks that reduce vendor lock-in and promote economic efficiency.
- **Policy Intelligence:** Applying advanced decision models to evaluate AI regulation impact on domestic industries.
- **Strategic AI Deployment:** Aligning AI adoption with multi-domain operational frameworks, ensuring resilience and scalability.
- **National AI Competitiveness:** Prioritizing AI strategies that position the U.S. as a leader in emerging AI applications, from defense to enterprise automation.

As a key industry body, AABA welcomes collaboration with government and private sector entities to ensure AI policies align with the realities of business adoption, workforce transformation, and national security imperatives.

For more information about AABA’s mission and vision, please visit us at **www.aab-ai.org**