PUBLIC SUBMISSION

Received: May 29, 2025
Tracking No. mb9-igoe-tid1
Comments Due: May 28, 2025 **Submission Type:** API

Docket: NSF-2025-OGC-0001
NITRD_FRDOC_0001

Comment On: NSF-2025-OGC-0001-0001
Request for Information: Development of a 2025 National Artificial Intelligence Research and Development Strategic Plan

Document: NSF-2025-OGC-0001-DRAFT-0189
Comment on FR Doc # 2025-07332

Submitter Information

Organization: Legion Intelligence

General Comment

See attached file(s)

Attachments

Legion_Aligning_AI_RD_Strategy_to_US_National_Security

Aligning AI R&D Strategy to U.S. National Security

Emerging in response to an acute need to bring Generative AI to the national security community, Legion is a secure and private enterprise Generative AI platform that empowers teams to do their best work. Founded in 2022, Legion aims to transform knowledge management and mission critical workflows at scale in both the public and private sectors. To learn more please visit www.legionintel.com.

Introduction

Legion agrees that the U.S. needs an updated National Artificial Intelligence (AI) Research & Development (R&D) Strategic Plan in order to strengthen our country's position as the global leader in AI and enhance our economic competitiveness and national security posture. To that end, Legion proposes modernizing "Strategy 8: Expand Public-Private Partnerships to Accelerate Advances in AI" and adding two new AI R&D strategies, "Strategy 10: Agentic AI for Defense & Security" and "Strategy 11: AI Innovation Ecosystem Development." These changes will provide a structured approach for integrating advanced AI agents into critical defense operations, ensure sustained technological leadership, and mitigate risks associated with proprietary model concentration. Doing so is paramount with the current intensification of the U.S.-China AI arms race, which threatens America's position as the global leader in AI technology.

The sections that follow detail each of these revisions in turn.

Expanding Public-Private Partnerships for National Security

To comprehensively address the evolving geopolitical and AI national security landscape, key areas of the current strategy should be rewritten to focus on explicitly integrating national security priorities, addressing critical infrastructure needs, and streamlining pathways for operational deployment.

Enhancing Strategic Alignment with National Security Objectives

As global competition intensifies, particularly with nations actively integrating AI into military and intelligence frameworks, the United States must adopt a more explicitly security-centric approach within public-private partnerships. The existing strategy language emphasizes partnerships largely from an economic growth and innovation perspective. While these goals

remain important, the strategy must more explicitly recognize the vital role of AI in national security.

The revised strategy should highlight the imperative of aligning commercial AI advancements with strategic defense needs. This alignment would encourage private-sector AI developers and technology companies to more directly collaborate with national security agencies. A clear, shared understanding of defense imperatives would guide partnerships toward capabilities that directly enhance national security, such as cybersecurity, logistics automation, and predictive intelligence systems.

Operational Deployment and Transitioning AI into Mission-Critical Environments

In today's hyper-competitive AI ecosystem, the lack of pathways for transitioning AI into real-world, mission-critical environments ensures a loss against geopolitical competitors. This strategy should emphasize clear mechanisms to facilitate seamless integration of AI technologies into operational systems within defense and national security contexts. Addressing operational deployment explicitly would streamline adoption processes, significantly reducing bureaucratic obstacles and accelerating the integration of mature AI technologies into critical defense missions.

The development and widespread adoption of experimental AI pilots in national security applications have demonstrated the practical capabilities and limitations of AI. However, these pilots remain mostly isolated from direct operational systems and real-time data flows. Moving beyond experimental phases toward integrated, operationally relevant deployments necessitates clear policy guidance and oversight frameworks. Revised language in Strategy 8 should therefore explicitly outline best practices for deploying AI tools safely and effectively in sensitive operational contexts.

Strategy 10: Agentic AI for Defense & Security

When the current AI & RD Strategy was last edited in 2023, the concept of "agentic AI" was in its infancy. Though the editors at the time engaged with the topic of Human-AI Collaboration in Strategy 2, the field has matured to the point that the market speaks of AI in terms of its level of agentic capability.

Agentic Capability Definitions

The current discourse around “agentic” AI is mired in marketing jargon with no clear agreed upon definition for what an “agent” actually is. In order to level-set, Legion uses the following as a foundational measure of agentic capability levels:

- L0 – Retrieval & Rule-Based Automation
    - Simple scripts performing predefined tasks without learning. Examples: keyword searches, form-filling bots. Limited but common in government.
- L1 – Assisted Intelligence (Basic Responder)
    - Basic AI responding to prompts without planning. Examples: FAQ chatbots, email drafting assistants. Enhances productivity, relies on human oversight.
- L2 – Tool-Using Agent (Actor)
    - AI utilizing tools and APIs for data interactions in single-turn tasks. Example: image retrieval or confirming logistics. Limited adaptability, human-corrected.
- L3 – Autonomous Workflow Agent (Operator)
    - Autonomously manages multi-step tasks, iteratively plans and executes actions towards defined goals. Examples: automated IT diagnostics, intelligence triage. Requires human oversight occasionally.
- L4 – Fully Autonomous Agent (Explorer)
    - Independently initiates tasks, dynamically adapts plans without explicit prompts. Examples: continuous cyber-defense monitoring, dynamic operational planning. Significant oversight and policy challenges remain.
- L5 – Designer Agent (Inventor)
    - Hypothetical human-level AI that independently sets goals, invents solutions, and self-improves. Conceivable for strategic military planning or diplomacy. Currently theoretical, no existing deployments.

Agentic AI for Defense & Security

The proposed "Agentic AI for Defense & Security" strategy should clearly articulate the integration of AI agents into defense operations, reflecting an understanding of the nuanced stages of agentic AI maturity (L0-L5). The strategy should emphasize thoughtful deployment, ensuring these AI systems act as force multipliers rather than replacements for human operators. It should explicitly address three critical areas:

1. **Integration and Accessibility:** Ensure mission critical networks have sufficient infrastructure and policy frameworks to securely incorporate advanced AI models. This

means prioritizing the bridging of gaps between cutting-edge generative AI technologies and mission critical operational data. Developing clear, secure pathways for operationalizing L2 and L3 AI agents into intelligence workflows and logistics systems will accelerate mission effectiveness.

2. **Policy and Oversight Mechanisms:** Develop robust, flexible governance frameworks to guide AI agent deployment, including role-based permissions, comprehensive auditing, and continuous red-teaming to build trust. Agentic AI use in sensitive scenarios must have guardrails that prevent unauthorized data access and minimize operational risk, maintaining a human-in-the-loop structure especially in high-stakes decisions.
3. **Scalable Compute Infrastructure:** Establish a national strategic compute reserve dedicated to supporting mission critical AI workloads, ensuring that the high-performance computing resources required by LLMs are reliably available. Investment in this infrastructure is crucial to maintain technological parity or superiority over adversaries.

Legion believes that agentic AI will dramatically reshape the operational landscape in the short to medium term. Thoughtful integration of agentic AI can significantly enhance strategic decision-making, mission readiness, and operational responsiveness, solidifying U.S. technological leadership and safeguarding national security interests.

Strategy 11: AI Innovation Ecosystem Development

Legion sees the evolving global AI competition as a new Cold War, where victory is defined not merely by defensive containment but by proactive, innovation-led growth. AI's transformative potential parallels historical innovations like electrification, promising wide-ranging societal and economic benefits if guided by a thoughtful and comprehensive national strategy to develop an AI innovation ecosystem.

Open-Source Innovation and Accessibility

Legion believes that an updated strategy for open-source AI development is needed to ensure a strong AI innovation ecosystem. The current market sees a strong concentration of both innovation and market power amongst a handful of model providers in a way that was not clear when the AI R&D Strategy was last revised in 2023.

The new strategy should push to avoid concentration risks associated with proprietary models. The U.S. government should facilitate open-source model development and public-private collaboration, encouraging incumbent model providers to emulate Meta's successful pivot to open-sourcing LLMs for national security use, similar to Meta with Llama 4.

The new strategy should also support foundational AI research. Ensuring that this foundational research remains accessible by startups and other small/medium businesses will drive domestic competition in the AI market and bring better capabilities to national security customers. This strategy should help develop standards to secure open-source models against adversarial exploitation while promoting transparency and widespread innovation.

Conclusion

The accelerating U.S.–China AI arms race requires immediate and strategic action to safeguard America's technological leadership and national security. Legion's proposals to modernize the National AI R&D Strategic Plan are crucial responses to the evolving geopolitical realities. By explicitly aligning public-private partnerships with national security objectives, facilitating seamless operational deployment, and clearly defining pathways for agentic AI integration, the U.S. can significantly strengthen its defense capabilities and strategic preparedness. Additionally, fostering a robust AI innovation ecosystem through open-source initiatives and foundational research ensures sustainable competitive advantage, fostering resilience against adversaries. Implementing these strategic recommendations will position the U.S. not merely to compete but to decisively lead in the global AI arena, securing both its technological edge and national security interests well into the future.

Respectfully submitted,
Legion Intelligence, Federal Team

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 2025 National AI R&D Strategic Plan and associated documents without attribution.