U.S. Department of Defense

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE FOR INDUSTRIAL BASE POLICY

Request for Information (RFI) on Defense Industrial Base (DIB) Adoption of Artificial Intelligence (AI)

Summary and Analysis Report

OFFICE OF THE ASSISTANT SECRETARY
OF DEFENSE FOR INDUSTRIAL BASE POLICY

2025

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Assistant Secretary of Defense's Office for Industrial Base Policy (IBP) is the principal advisor to the Under Secretary of Defense for Acquisition and Sustainment for developing Department of Defense (DoD) policies for the maintenance of the United States (U.S.) Defense Industrial Base (DIB). IBP works with domestic and international partners to forge and sustain a robust, secure, and resilient industrial base, enabling the warfighter, now and in the future.

IBP analyzes the health of the DIB to inform decisions to retire outdated platforms and prioritize the development of technologically advanced systems. By promoting a resilient supply chain, IBP ensures the DoD and the DIB are prepared to meet future mission demands.

The DoD recognizes Artificial Intelligence (AI)[1] as one of 14 critical technologies crucial for U.S. national security. Integrating AI into defense systems and processes is vital for maintaining a tactical advantage over adversaries. The DIB, responsible for developing and maintaining United States (U.S.) military systems, plays a critical role in this effort. Therefore, a top priority for both the DoD and IBP is empowering the DIB to adopt AI for defense applications. This priority aligns with strategic objectives outlined in national defense strategies, including the National Defense Industrial Strategy (NDIS).

To identify gaps in the DIB concerning AI adoption and potential policy enablers to address these gaps, IBP published a Request for Information (RFI) in the Federal Register on May 22, 2024, titled *Defense Industrial Base Adoption of Artificial Intelligence for Defense Applications.* The objective of the RFI was to gain insight into the public's perspective on the actions that the DoD can take to support the ongoing adoption of AI for defense applications. The RFI requested public feedback in the following areas related to the DIB's ability to adopt AI:

- Infrastructure and Supply Chain Resilience
- Workforce
- Innovation
- Acquisition, Policy, and Regulatory Environment

This report presents a summary and analysis of the responses received to the RFI. The statements and opinions presented in this document reflect the views of the respondents derived from RFI submissions and do not imply endorsement by the DoD.

The RFI respondents identified a wide range of opinions on potential barriers inhibiting adoption of AI for defense applications within the DIB. Respondents also provided recommendations to overcome those barriers and facilitate continued progress. Analysis revealed four main themes in recommendations from respondents:

1. **Infrastructure and Supply Chain Resilience:** The DoD should reduce reliance on foreign suppliers, particularly those posing a heightened risk of supply disruptions, such as China. DoD should reduce foreign reliance on critical components of AI infrastructure, including large data centers and advanced processors. This challenge could be alleviated by increasing investments in U.S. manufacturing capabilities to promote a more reliable and resilient supply chain for AI infrastructure, particularly for AI semiconductors. Relying on vulnerable supply

[1] In the context of this report, AI refers to *limited memory* applications which use historical data and pre-programmed information to make predictions and perform classification tasks.

chains supporting AI infrastructure will hinder the U.S.'s ability to expand AI adoption quickly and securely within defense applications.

2. **Workforce:** The DoD should collaborate with the broader AI community, including academia, industry, and other government partners to establish and expand training programs and curricula for both the current and future workforce. Workers should be adequately trained in data management, ethics, and responsible AI use. An inadequately trained workforce adversely impacts the DIB's ability to adopt and field AI-integrated defense systems.

3. **Innovation:** The DoD should develop frameworks and standards to facilitate data sharing, AI development, and system interoperability. These frameworks would encourage faster innovation cycles and wider adoption of AI capabilities for defense applications. Without these frameworks and standards, the DIB will continue to face challenges, such as complex intellectual property (IP) considerations and inconsistent data sharing standards, which hinder rapid and widespread innovation.

4. **Acquisition, Policy, and Regulatory Environment:** The DoD should simplify and expedite the acquisition process for emerging technologies and increasingly use expedited contracting pathways, such as Other Transaction Agreements (OTAs). Currently, acquisition processes present significant hurdles for smaller and non-traditional contractors due to their complexity, cost, and time to execute. Current acquisition processes could lead to missed opportunities in the AI field, resulting in delays or even outright failures to acquire critical technologies.

These recommendations aid the Department in understanding the barriers encountered and resources required by the DIB for continued integration of AI into defense applications. Additionally, the responses gathered in the RFI will inform IBP's AI DIB Roadmap, which will outline quick wins, mid-range goals, and long-range DIB considerations for AI-enabled defense applications.

INTRODUCTION AND BACKGROUND

The DoD understands the critical need to invest in the Defense Industrial Base's (DIB) capacity to integrate AI across the lifecycle of defense applications, from design to operations, maintenance, and support. This focus on a robust and modernized DIB, capable of adopting AI, aligns with national priorities to strengthen U.S. technological competitiveness, supply chain resilience, and economic and national security. Furthermore, it mirrors DoD priorities to restore the warrior ethos, rebuild the military, and reestablish deterrence. These DoD strategies and policies underscore the need for a strong and resilient DIB with the capacity to effectively leverage and integrate AI in defense applications.

The National Defense Industrial Strategy (NDIS) further underscores the importance of a robust supply chain. By ensuring supply chains are both responsive to demand and resilient against national security risks, the DoD can effectively leverage AI for a stronger defense posture.

Moreover, the Data, Analytics, and Artificial Intelligence Adoption Strategy[2] by the DoD's Chief Digital and Artificial Intelligence Office (CDAO) advocates for an approach to AI adoption that includes rapid research and development and seamless integration with allied nations and partners. This includes ensuring the allocation of resources essential for successful AI adoption. Specifically, CDAO's strategy identifies five AI-centric efforts:

- Strengthen governance and remove policy barriers;
- Deliver capabilities for enterprise and join warfighting impact;
- Improve foundational data management;
- Invest in interoperable, federated infrastructure;
- Advance the data, analytics, and AI community; and
- Expand digital talent management.

To gain additional insight on this pertinent topic, IBP sought public comments through a request for information (RFI) on how the DoD can enable the DIB to continue adopting AI for defense. The RFI consists of 13 questions (included in the Appendix) and received 48 responses. The responses are generally classified into the themes of ***barriers*** and ***recommendations***. This report examines barriers and recommendations through analysis of the four question areas: (1) infrastructure and supply chain resilience; (2) workforce; (3) innovation; and (4) the acquisition, policy, and regulatory environment.

Characterization of RFI Respondents

Analysis of the 48 RFI responses revealed a varied respondent pool. Enterprises and small businesses constituted the largest groups, accounting for 29% and 27% of responses, respectively. Associations contributed 17% of responses, followed by consulting firms (13%), private individuals (8%), and other respondent types (6%).[3]

---

[2] DoD Data, Analytics, and Artificial Intelligence Adoption Strategy

[3] Enterprise: legal entity possessing the right to conduct business on its own, for example to enter contracts, own property, incur liabilities and establish bank accounts. An enterprise may be a corporation, a quasi-corporation, a non-profit institution, or an unincorporated enterprise; Small Business: a company of relatively limited size, as measured by its revenue, number of employees, or both; Association: individuals or companies that share a common interest or work in the same industry; Consulting: entities providing funding or for-pay services to enterprises; Private Individual: members of the public who do not represent any organization in an official capacity; Assignment of respondents to each category was inferred based on the content of the submission.

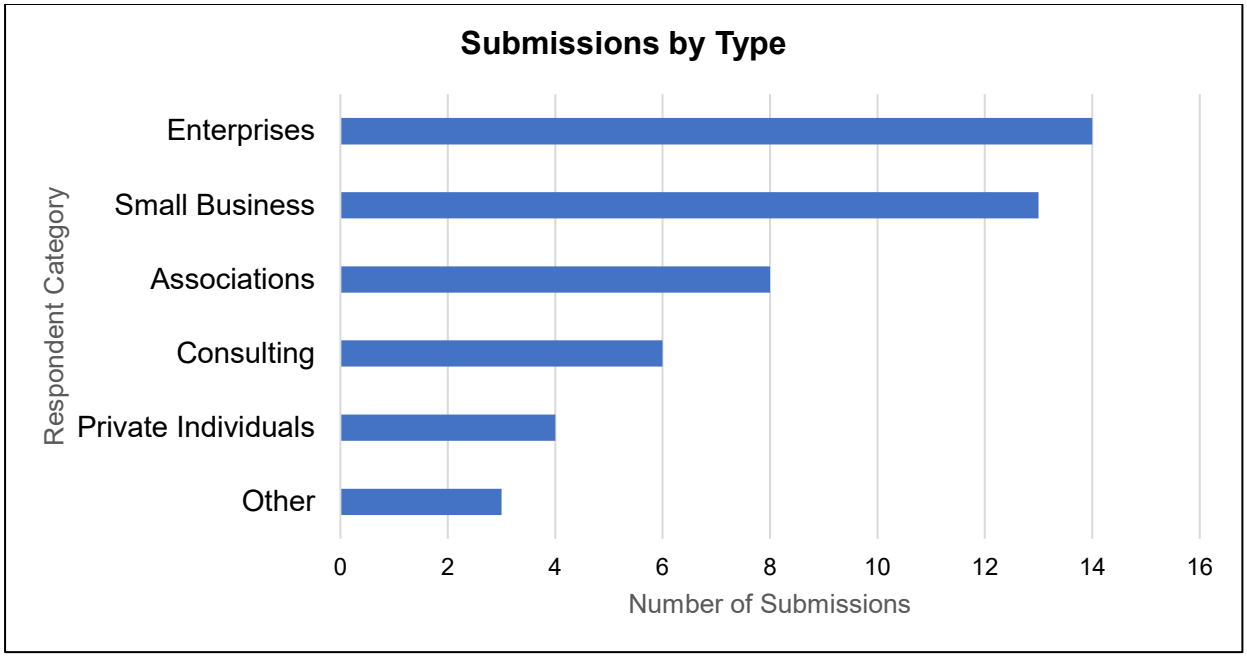

Figure 1: Number of Submissions by Respondent Type

Analysis of responses to individual RFI questions reveals that topics related to foundational investments (Question 1) and information sharing (Question 7) garnered the highest levels of engagement from stakeholders. Specifically, respondents were particularly interested in:

Question 1: Foundational Investments

What foundational investments in the DIB does the DoD need to make to support increased adoption of AI into defense systems (e.g., manufacturing considerations, standards, best practices, bill of materials, etc.)? What foundational investments (e.g., standards, best practices, bills of materials, etc.) already exist within the DIB for defense systems that incorporate AI?

Question 7: Information Sharing

How can the DoD promote information-sharing and collaboration among government agencies, defense contractors, and research institutions to enhance data availability, collective knowledge, capabilities, and defense innovation in AI adoption into defense systems?

The high response rate to these questions underscores the significance of foundational investments and robust information sharing mechanisms as key priorities for the DIB across all sectors. Stakeholders are prominently seeking clarity and direction from the DoD on these critical aspects of AI adoption. The below figure shows the number of responses to each RFI question from broken

down by respondent category. Questions 1 and 7 received the highest number of responses.

Category	Question	Number of Responses						
		All Types	*Enterprises*	*Small Business*	*Associations*	*Consulting Firms*	*Private Individuals*	*Other*
Infrastructure and Supply Chain Resilience	1	35	10	8	6	6	2	3
	2	26	11	7	4	2	1	1
	3	16	8	4	2	1	0	1
Workforce	4	22	8	6	4	3	0	1
	5	21	8	5	5	1	1	1
Innovation	6	20	8	4	4	2	1	1
	7	34	10	8	5	5	3	3
	8	19	7	2	5	3	0	2
Acquisition, Policy, & Regulatory Environment	9	18	7	4	5	1	0	1
	10	12	7	0	2	2	0	1
	11	14	8	1	3	1	0	1
	12	19	7	4	4	2	1	1
	13	21	7	5	3	3	2	1

Figure 2. Number of Question Responses by Respondent Type

BARRIERS TO ADOPTION OF ARTIFICIAL INTELLIGENCE IN DEFENSE APPLICATIONS

Introduction

The RFI revealed a range of barriers hindering AI adoption within the DIB. To provide a structured analysis, respondent feedback was organized into four key categories:

1. Infrastructure and Supply Chain Resilience
2. Workforce
3. Innovation
4. Acquisition, Policy, and Regulatory Environment

Within each category, overarching themes emerged from the responses. This report delves into each theme, providing further context and elaboration through specific respondent comments.

Infrastructure and Supply Chain Resilience Barriers

The supply chain for supporting infrastructure (e.g., microelectronics) needs to be resilient and readily available for DIB participants to support AI development and adoption. According to respondents, an overreliance on foreign suppliers was identified as a significant barrier. Many inputs, such as microelectronics, state-of-the-art fabrication equipment, and rare earth elements in the upstream value chain, are heavily sourced from foreign suppliers. This reliance on foreign suppliers increases vulnerabilities and the likelihood of disruptions, such as counterfeit goods, natural disasters, and foreign influence. RFI responses focused more specifically on AI's technical development as an underlying barrier.

In several instances, respondents stated that high research and development (R&D) costs and lengthy quality control cycles hinder the speed of adoption. Another development barrier that inhibits the AI supply chain is the production rate of microelectronics. Microelectronics are the cornerstone for AI, but production must be scaled up in time to meet the rapidly growing demand, including the need for graphics processing units (GPUs).

Supply chain vulnerabilities, particularly in the face of IP theft and cyberattacks, present significant barriers to AI adoption within the DIB. The data-intensive nature of AI systems, often involving sensitive information, creates a lucrative target for malicious actors.

Key concerns from respondents include:

- **Data Breaches:** Loss of sensitive data through IP theft can compromise algorithms, training data, and undermine competitive advantage.
- **Operational Disruptions:** Cyberattacks targeting supply chain infrastructure can disrupt the flow of essential data, hindering AI system development and deployment.
- **Compromised Security Measures:** Successful attacks can expose vulnerabilities in existing security protocols, leaving AI systems susceptible to manipulation or exploitation.

Addressing these vulnerabilities is paramount for building a resilient and trustworthy AI ecosystem within the DIB.

Workforce Barriers

Adoption of AI into defense applications by the DIB requires a skilled and readily available workforce. Respondents stated that to adequately address any workforce gaps, there must be an increased focus on upskilling and reskilling the existing workforce.

Key concerns from respondents include:

- **Training and Upskilling:** Most of those surveyed concurred that a sufficiently staffed and trained AI workforce needs investment, participation, and knowledge sharing in AI-focused educational programming across government, industry, and academia. Notably, the AI industry's understaffed workforce is partially due to a lack of AI-specific training within the DoD and inadequate STEM education. Respondents state that the U.S. faces a continuous shortage of students pursuing degrees related to STEM. Responses suggest that establishing public-private partnerships that bring together academia, industry experts, and government partners will improve collaboration and increase sponsorship of R&D initiatives and the exchange of ideas.

Respondents state that the DoD must consider developing targeted talent acquisition and retention strategies to secure top talent in AI and related fields. Additionally, recommendations urge the DoD to expand opportunities for professional growth, including training, and mentorship.

Innovation Barriers

The RFI highlighted significant innovation barriers within the DIB, particularly related to data accessibility, intellectual property concerns, and lack of interoperability.

Key concerns from respondents include:

- **Data Silos Hindering Collaboration:** Respondents consistently pointed to decentralized and isolated data repositories as a major obstacle. These silos impede collaboration, making it difficult to identify existing capabilities and pursue joint initiatives. While a centralized data source could mitigate this, respondents acknowledged the heightened risk of cyberattacks and the reliance on third-party trust.

Adding to the challenge, even accessing unclassified data can be cumbersome, often involving lengthy approval processes. This delay significantly hampers AI development, as highlighted by one respondent: ″AI development often requires access to large datasets, which may be proprietary or classified. Ensuring appropriate data rights and usage permissions can be complex.″

For classified data, stringent security clearance requirements further exacerbate delays. Background checks can take months, excluding subject matter experts and slowing down project timelines. Respondents emphasized that this siloed approach, prevalent across intelligence and law enforcement agencies, significantly hinders progress in AI development.

- **Intellectual Property Creating Uncertainty:** Concerns surrounding IP ownership emerged as a significant barrier to data sharing and innovation. Respondents criticized what many termed the ″traditional view″ of IP within the DIB, arguing that it primarily benefits the public sector and fails to consider the needs of private industry stakeholders.

The government's frequent pursuit of full IP control, while intended to prevent vendor lock-in, discourages private investment and innovation. As one respondent noted, transferring IP rights to the public sector could drive companies out of business, weakening the DIB as a whole. This reluctance

to share IP, coupled with a lack of trust within the industry, creates an environment of uncertainty and inhibits collaboration.

- **Interoperability as an Enabler for a Competitive Landscape:** A lack of interoperability emerged as another critical concern. Respondents emphasized that interoperable systems are essential to prevent market dominance by a few providers with proprietary technologies. This open approach fosters competition and flexibility, driving innovation and cost-effectiveness. As respondents highlighted, interoperability benefits both the government and industry by ensuring access to the most advanced technologies at the best value.

To foster a truly innovative AI network within the DIB, addressing these data, IP, and interoperability challenges is paramount to AI adoption.

Acquisition, Policy, and Regulatory Environment Barriers

The RFI responses revealed significant concerns about the current acquisition, policy, and regulatory environment, which respondents perceive as a major impediment to AI adoption within the DIB.

Key concerns from respondents include:

- **Cumbersome Acquisition Processes:** Respondents overwhelmingly cited complex and lengthy government acquisition processes as a major barrier, particularly for small businesses lacking the resources to navigate the intricate contracting landscape. The current system, respondents viewed as burdened by extensive regulations, leans towards AI vendors with existing access to data and resources, making it challenging for non-traditional contractors to break into the DoD AI market.
- **Budgetary Constraints and Inadequate Contract Vehicles:** Respondents cite the lack of adequate funding and inflexible contracting mechanisms further hinder AI adoption. Respondents emphasized that while the demand for AI capabilities is increasing, budgetary constraints within program offices often fail to keep pace with the resources required for testing, validation, and deployment.

Additionally, current contract vehicles and billing structures lack the flexibility to effectively procure consumption-based AI solutions and services, a stark contrast to the dynamic pricing models prevalent in the free market. This rigidity contributes to inefficient acquisition processes, hindering the timely, and scalable delivery of AI capabilities.

- **Regulations Pacing with AI Advancements:** Respondents stressed the need for regulatory updates to keep up with the rapid evolution of AI technology. The Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) were specifically identified as requiring revisions to address the unique aspects of AI procurement, testing, and deployment.

Existing safety and certification standards, often not designed with AI in mind, further prolong the regulatory process. This lag creates uncertainty for developers and hinders the timely deployment of AI solutions.

- **International Collaboration and Export Controls:** Several respondents highlighted the unintended consequences of stringent export controls on AI technology. These restrictions, while intended to protect national security, can limit international collaboration and stifle innovation by preventing the sharing of knowledge and resources with allies.

In conclusion, respondents emphasized the need for a more agile, adaptable, and globally-minded approach to acquisition, policy, and regulation within the AI domain. Addressing these barriers is crucial to fostering a more dynamic and competitive DIB capable of delivering cutting-edge AI capabilities for national defense.

Discussion

Respondents overwhelmingly pointed to **acquisition, policy, and regulatory environments as the most significant barriers to AI adoption in defense applications** (Figure 3). These barriers were highlighted by 47 out of 48 responses. Infrastructure and supply chain issues were also identified as a major obstacle by a significant majority (71% or 34 respondents).

While respondents often cited multiple barriers, suggesting these challenges are widespread across categories, the consistent emphasis on specific themes like supply chain bottlenecks and hiring difficulties reveal **clear gaps hindering AI adoption within the DIB**. The DoD needs to prioritize AI adoption to leverage the skills of future generations and ensure forward progress. Notably, a 2023 survey of 14,000 workers conducted by Salesforce highlighted that 28% were already using generative AI in the workplace, with that number expected to grow.[4] This strong consensus on existing barriers provides the DoD with valuable insight and a clear direction for its efforts to prepare for AI's growing importance in the DIB. A wider variety of RFI responses might have indicated differing viewpoints on the best path towards AI integration, but the shared concerns highlight the need to address these fundamental roadblocks.

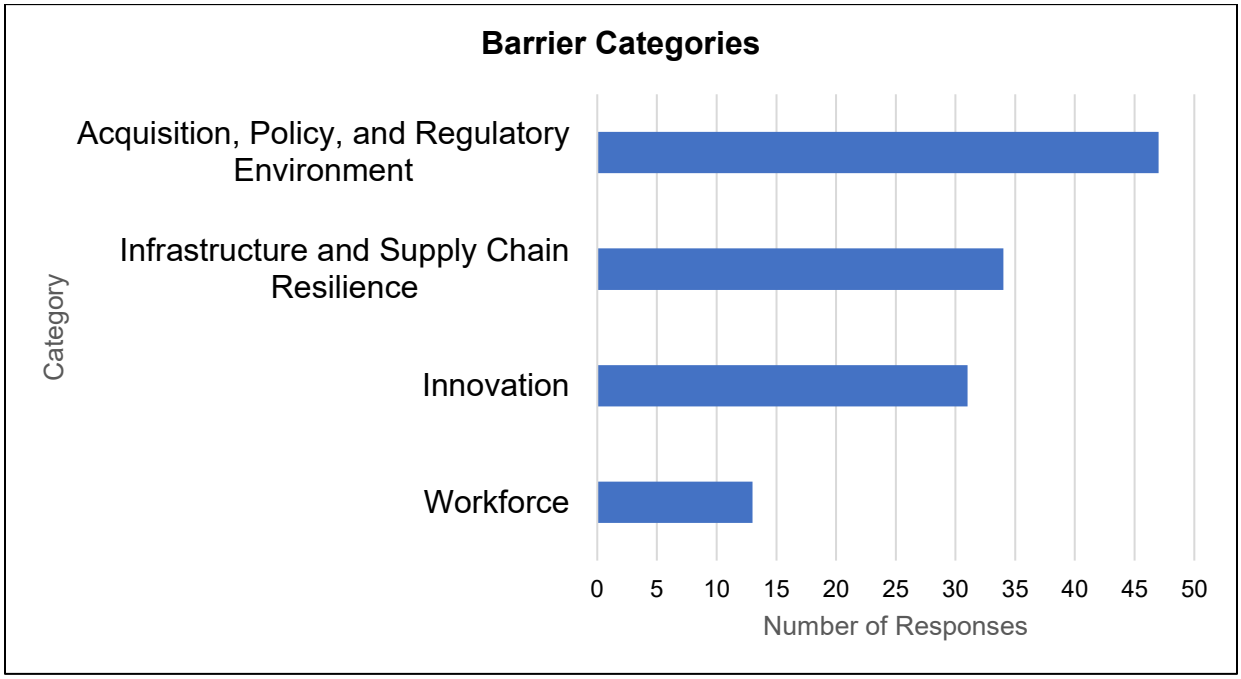

Figure 3. Barrier Categories

[4] Salesforce - More than Half of Generative AI Adopters Use Unapproved Tools at Work

RECOMMENDATIONS FOR ADOPTION OF AI IN DEFENSE APPLICATIONS

Introduction

Respondents offered a range of comprehensive recommendations to address barriers to the adoption of AI in defense applications. These responses were subsequently categorized into Infrastructure and Supply Chain Resilience, Workforce, Innovation, and Acquisition, Policy, and Regulatory Environment. Selected recommendations identified by the respondents within each of the categories are described below.

Infrastructure and Supply Chain Resilience Recommendations

- **Risk Management:** Respondents indicated that an initial step to securing the AI supply chain is to **develop a comprehensive risk management framework to identify** and mitigate potential supply chain disruptions, particularly critical AI components. The framework should include a means to vary suppliers and establish redundant supply chains to ensure continuity.

- **Supply Chain Mapping:** Respondents strongly recommended utilizing AI to bolster supply chain resilience in two key ways:

    - *Real-time Visibility and Risk Management*:
        - Implement AI-powered systems to track goods and materials in real-time, allowing for proactive identification of bottlenecks, route optimization, and timely delivery.
        - Utilize AI for continuous monitoring and forecasting of potential disruptions within the supply chain, enhancing preparedness and minimizing disruptions.
        - Automate repetitive tasks like data entry using AI, freeing up human resources to focus on strategic planning and decision-making.
        - Leverage AI's superior pattern recognition capabilities to identify counterfeit products and adapt to demand surges caused by external factors.
    - *Enhanced Traceability and Security*:
        - Develop and implement comprehensive supply chain mapping and traceability systems, ensuring a secure and transparent chain of custody for all AI algorithm development activities.
        - Document all inputs and origins of development efforts, enabling full transparency and understanding of the DoD's AI algorithm supply chain.

By implementing these measures, the DoD can create a more robust and secure supply chain, mitigating risks through increased visibility, proactive risk management, and improved traceability.

- **Enhanced Support and Collaboration:** Lastly, respondents suggest supporting industries in the AI value chain by offering subsidies or creating public-private partnerships. This recommendation aims to enhance supply chain resilience by providing financial support for AI infrastructure across value chain tiers, ensuring they are robust enough to withstand disruptions and keep pace with AI growth.

Workforce Recommendations

- **Education and Upskilling:**
  - Respondents advocate for **updating educational curricula to include AI and related fields** and providing opportunities for lifelong adaptation to technology changes. **DoD could partner with industry to offer AI** related online courses, bootcamps, and training initiatives developed with universities and industry leaders.
  - AI workforce development and education should focus on technologies such as data analysis, programming, and AI ethics.
  - Respondents recommend that the DoD establish and **strengthen public-private partnerships with academic institutions**, and small businesses which would facilitate collaborative R&D. The DoD should prioritize these institutions to identify best practices to reskill and upskill current employees and train new employees. Respondents believe that non-defense experts, especially those who work on commercial AI models, can provide valuable insight on advances and current trends in AI development, reducing the time it takes for the DoD to implement advanced techniques and capabilities.
- **Recruitment:** Respondents recommend that the DoD attract new talent by creating greater career opportunities and pathways for advancement in AI fields. Furthermore, respondents suggest that the DoD can also support the DIB by creating a larger community of researchers on the forefront of this emerging field, similarly to the efforts it supported in developing a workforce for nuclear energy projects in the 1950s and aerospace projects in the 1960s.

Innovation Recommendations

Respondents consistently emphasized the critical importance of data integrity and security for trustworthy AI in defense. They strongly recommend robust data governance policies, secure access controls, and privacy-preserving technologies throughout the entire innovation cycle.

Specifically, respondents highlighted the value of Privacy-Enhancing Technologies (PETs) to safeguard sensitive information. By keeping data encrypted even during processing, PETs prevent unauthorized access and data breaches, effectively protecting critical defense information from adversarial threats. This focus on data security underscores its essential role in building reliable and trustworthy AI systems for defense applications.

- **Data Integrity:** To maintain the quality and integrity of data used in AI systems, respondents suggested implementing measures such as **continuous monitoring and validation** to protect against data poisoning. Additionally, it was emphasized that raw data and algorithms remain protected throughout their lifecycle.
- **Infrastructure Investment:** Another recommendation suggested that the DoD **utilize newly constructed data centers** designed to increase security, efficiency, and operational flexibility. These data centers would consolidate defense-related data and assets into a secure environment, specifically serving U.S. Federal Government interests. This infrastructure would not only protect sensitive data but also improve the efficiency of data processing and storage, ultimately promoting more effective AI development and deployment.
- **Data for Training:** Additionally, respondents recommended the **use of synthetic data and robust simulation-to-real transfer techniques** as a strategy to address the challenges of data scarcity and the complexities of collecting real-world data. These techniques allow for the

generation of realistic training data that can be used to develop and test AI models in environments that closely mimic real-world scenarios.

- **Intellectual Property Rights:** Respondents emphasized the importance of protecting intellectual property (IP) rights. AI is at a crossroads with developers from sectors including government, industry, and research centers. Eventually, ownership of such material will have to be established, especially as small businesses attempt to enter the sector and collaborate alongside large enterprises. Respondents recommended that **transparent IP rules and regulations** be promoted to encourage enhanced collaboration amongst stakeholders. Responses also stressed that government guidance doesn't require developers to publicize trade secrets and that there be direct guidance to prevent accidental leaks within the government. To firmly establish such policies, respondents recommend that the DoD publish clear IP policies for industry partners in place of the byzantine structure in place.

- **Centralized Data Sharing:** The DoD's current state of information sharing is decentralized, restricting opportunities for increased productivity. One suggestion proposed **implementing centralized data sharing** through "…a comprehensive, user-friendly database that aggregates and correlates data from all DoD services, project management offices, laboratories, and other relevant government organizations. This database should include details on ongoing projects, programs, test reports, standing contracts, and authorities to operate." Such a platform would also encourage the use of interoperable standards to promote data integration from various sources, which is key for supporting collaboration across sectors. Additionally, respondents emphasized that AI can substantially improve information-sharing by enabling the integration of data from multiple sources, generating a unified perspective of information across various systems and organizations.

- **Interoperability Standards:** Respondents also recommended that the DoD establish **interoperability and data transfer standards** to ensure that hardware and software are compatible across different platforms. Such mandates would ensure that AI developers are not locked into a single vendor's network, thereby promoting a heathier and innovative competitive landscape.

- **AI Development Framework:** Finally, respondents stated that standardization should be at the forefront of AI infrastructure implementation, thus enabling products to be more easily shared across the DoD. This would include implementing a common and singular AI development framework and toolkit to simplify adoption. **Consistent and secure model deployment environments with standardized protocols** would support simplified sharing of AI models across the public and private sector to support innovation cycles. Further, one set of validation and testing protocols would ensure reliability, security, and performance across sectors, while also serving as a conduit to trusted AI.

Acquisition, Policy, and Regulatory Environment Recommendations

Respondents identified significant opportunities for AI to revolutionize key aspects of the DIB, including acquisition, supply chain management, regulatory streamlining, and information sharing.

- **Acquisition Automation:** A respondent recommended that AI be used to **automate standard and intricate acquisition tasks,** such as requirements development, budget planning, proposal evaluations, and contract administration, thereby accelerating the timeline of these processes. AI offers rapid and accurate planning of program strategies, thus ensuring the

most efficient pathways are selected for delivering material solutions and close operational gaps identified in requirements documents.

- **Regulatory Updates:** The recommendations for regulatory compliance are to ensure that the deployment of AI technologies adheres to existing laws and regulations while also adapting to new challenges posed by AI. These recommendations are to **update regulatory frameworks** that can effectively address the unique risks and opportunities associated with AI, such as data privacy, contamination in AI algorithms, and the ethical implications of autonomous systems. Respondents also call for **clear guidelines from the DoD** that can help companies navigate the regulatory landscape and ensure that their AI implementations are compliant.

- **Proactive Regulation:** A recurring theme among respondent recommendations is the appeal for regulatory bodies to adapt a proactive approach to AI regulation, as opposed to a reactive one. This involves anticipating potential issues and developing regulations that can address them before they become problematic. Some recommendations advocate for stringent regulations to prevent any misuse of AI, while others suggest a **more flexible approach that promotes innovation at speed** while still ensuring safety and compliance. The balance between fostering innovation and ensuring compliance is a recurring theme, with different recommendations suggesting varying levels of regulatory oversight.

- **Flexible Contracting Vehicles:** Respondents provided many recommendations to improve acquisition processes, streamline policies, and modernize the regulatory environment to promote the development and deployment of AI solutions. It was recommended that the DoD utilize flexible acquisition contracting pathways more frequently, such as government-wide information technology acquisition contracts, OTAs, Small Business Innovation Research (SBIR), and Commercial Solutions Openings (CSOs) to increase acquisition of AI capabilities. Respondents recommended that the DoD collaborate with international partners to reevaluate and modernize acquisition processes and regulations. This collaboration would aim to facilitate and expand the adoption of AI technologies on an international scale.

- **Rapid Development Pathways:** Given the dynamic and evolving AI operating environment, respondents recommend that the DoD develop regulatory frameworks to support the rapid development, testing, and deployment of AI systems while ensuring compliance with safety and ethical standards. To accelerate the certification and deployment of new AI technologies, respondents recommended the establishment of DoD-led *sandboxes.* These controlled environments would allow for the testing and validation of AI systems under streamlined regulations.

- **Security & Regulatory Compliance:** To enhance security compliance, the DoD should utilize AI to streamline the Federal Risk and Authorization Management Program (FedRAMP) authorization process. By using automated tools for evaluation and risk identification, the process can be more efficient. For example, AI can be used in tools to enable true continuous monitoring, reporting, and threat mitigation thus enhancing cybersecurity across the enterprise. For regulatory compliance, AI can continuously monitor regulatory requirements and ensure that all processes and products comply with relevant standards. This includes tracking changes in regulations and updating compliance protocols accordingly.

Discussion

Supply chain resilience emerged as a dominant theme in respondent recommendations, with over half emphasizing its importance. Specifically, 37 (77%) responses directly addressed infrastructure and supply chain concerns. Workforce development also featured prominently, mentioned in nearly half of the responses. This contrasts with the barriers section, where workforce issues were less frequently cited.

Acquisition, policy, and regulatory matters received comparatively less attention, with only 14 mentions. Echoing the barriers section, recommendations in these areas centered around key actions for the DoD, such as promoting secure and shareable AI training data and streamlining contracting to attract non-traditional suppliers.

Overall, the recommendations provide a valuable roadmap for the DoD, outlining concrete steps to advance AI adoption and innovation within the DIB.

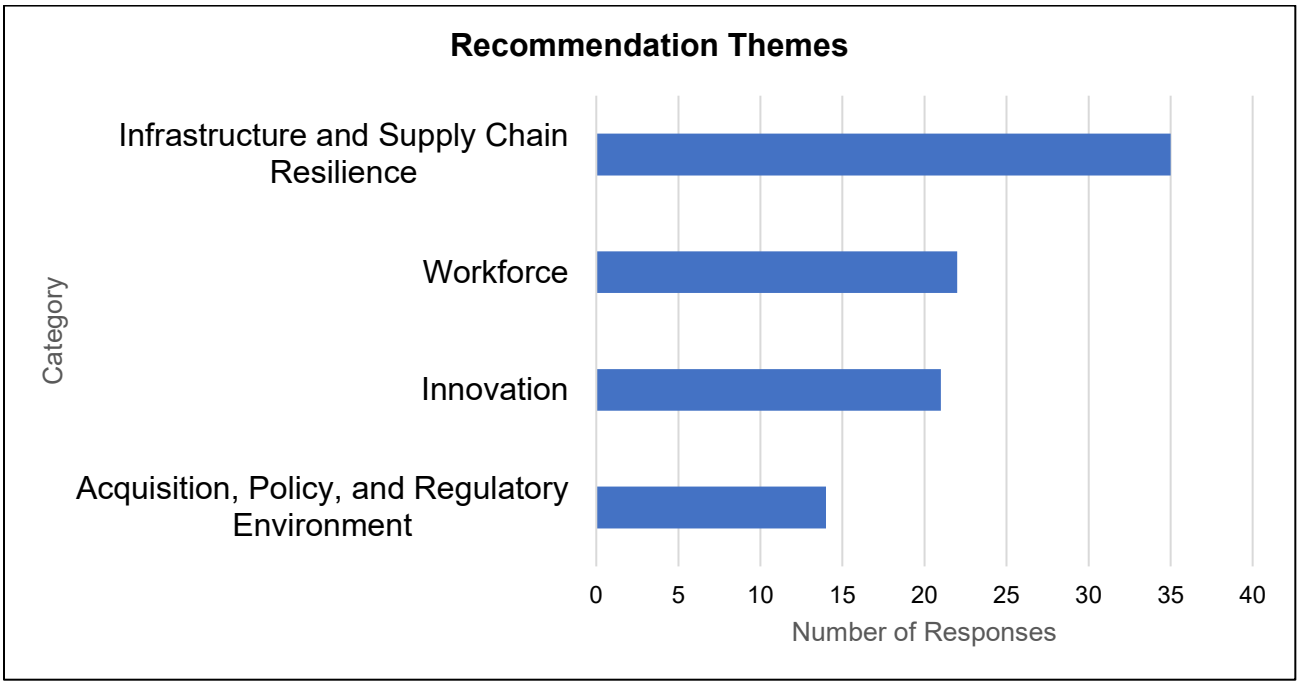

Figure 4. Recommendation Themes

CONCLUSION

As artificial intelligence evolves rapidly, it is inevitable that AI will be incorporated not only into defense applications but also into defense suppliers' daily operations. The RFI feedback illuminated key areas for action to accelerate AI innovation in defense. Respondents consistently emphasized the need for robust frameworks and standards to facilitate data sharing, streamline AI development, and ensure system interoperability. These measures would pave the way for faster innovation cycles and wider adoption of AI capabilities across defense applications.

Addressing the workforce gap is crucial. Respondents stressed the importance of strengthening collaboration between academia, industry, and government partners to develop comprehensive training programs and curricula for both current and future workforces. This collaborative approach would ensure a robust talent pipeline capable of meeting the surging demand for AI expertise.

Furthermore, respondents urged for more agile acquisition policies and processes to enable flexible pathways for acquiring innovative solutions, particularly from non-traditional suppliers.

Finally, the need for secure and resilient supply chains underpinning critical AI infrastructure was underscored. Respondents emphasized the urgency of sustained government investment in manufacturing capabilities, including advanced AI chip manufacturing. The DoD aims to establish a robust and accessible AI infrastructure. This can be achieved by leveraging AI's potential to boost production flexibility, improve efficiency, cut costs, and accelerate time-to-market.

APPENDIX

RFI Questions

The RFI posed 13 questions designed to gather comprehensive insights across four critical categories:

- Infrastructure and Supply Chain Resilience
- Workforce
- Innovation
- Acquisition, Policy, and Regulatory Environment

The RFI questions are outlined below. The complete AI RFI, including detailed context and instructions, is available on the Federal Register.

Infrastructure and Supply Chain Resilience

- What foundational investments in the DIB does the DoD need to make to support increased adoption of AI into defense systems (e.g., manufacturing considerations, standards, best practices, bill of materials, etc.)? What foundational investments (e.g., standards, best practices, bills of materials, etc.) already exist within the DIB for defense systems that incorporate AI?

- Are there specific vulnerabilities in the current and future supply chain that the DoD needs to address to support defense systems that incorporate AI?

- Are there specific sectors/subindustries within the DIB that face significant challenges in developing and applying AI to defense systems? If so, which sectors/subindustries are impacted, and what challenges do the sectors/subindustries face?

Workforce

- How can the DoD support the involvement of non-traditional defense contractors and small businesses in the design, development, testing, and deployment of AI technologies for defense applications?

- How can the DoD support and create effective partnerships with the DIB that will ensure that the DoD and DIB workforce is adequately trained, skilled, and sized to partner effectively?

Innovation

- Are there specific intellectual property considerations or challenges related to the development of AI-enabled defense systems that impact the DIB? If so, how can the DoD address these issues to promote innovation?

- How can the DoD promote information-sharing and collaboration among government agencies, defense contractors, and research institutions to enhance data availability, collective knowledge, capabilities, and defense innovation in AI adoption into defense systems?

- What measures can the DoD take to assess and mitigate the risks associated with potential adversarial exploitation of AI technologies within the DIB for developmental and operational defense systems?

Acquisition, Policy, & Regulatory Environment

- Please identify statutory, regulatory, or other policy barriers to the DIB's design, development, testing, and provision of AI-enabled defense systems in a manner consistent with DoD's approach to Responsible AI.[5]

- Please identify examples of DoD programs, strategies, policies, or initiatives that have provided effective support to the DIB in transitioning AI for defense applications. What made these programs, strategies, policies, or initiatives successful?

- What DoD financing and acquisition mechanisms can help facilitate or incentivize the DIB to continue to invest in AI technologies for defense applications?

- What are the primary barriers that the DoD needs to address in the next five to ten years to enable the DIB to adopt AI for defense applications?

- In what ways can AI support or enhance acquisitions, supply chain management, regulatory compliance, and information-sharing in the DIB?

Exemplar Programs

Respondents highlighted several successful DoD programs and policies already in place that could serve as model programs for wider implementation.

Defense Innovation Unit (DIU): DIU works with commercial AI companies to rapidly prototype and deploy AI solutions for defense needs. They have also developed Responsible AI (RAI) guidelines. DIU's RAI Guidelines aim to provide a clear, efficient process of inquiry for personnel involved in AI system development (e.g., program managers, commercial vendors, or government partners) to achieve the following goals:

1. Ensure that the DoD's Ethical Principles for AI are integrated into the planning, development, and deployment phases of the technical lifecycle;

2. Effectively examine, test, and validate that all programs and prototypes align with DoD's Ethical Principles for AI; and

3. Leverage a process that is reliable, replicable, and scalable across a variety of programs.

Chief Digital and Artificial Intelligence Office (CDAO): Leads strategic planning, coordinates AI projects, and fosters collaboration across the Department of Defense. CDAO provides enterprise tools for responsible AI development, invests in data management and workforce training, and has established a collaborative AI development environment that could support DIB investment more broadly. CDAO's Responsible AI Toolkit is a set of assessments and tools for improving the alignment of AI projects toward RAI best practices and the DoD AI Ethical Principles, while capitalizing on opportunities for innovation. Using the RAI Toolkit allows the DIB to demonstrate the

[5] The Reliable Artificial Intelligence (RAI) Toolkit

incorporation of traceability and assurance concepts throughout their development cycle. Additionally, CDAO oversees Tradewinds, an AI marketplace designed to streamline the procurement process, making it easier for the DoD to acquire cutting-edge AI solutions from industry partners.